

# 天行应用系统安全审计系统

## Topwalk-VAS

### 产品简介

拓尔思天行网安信息技术股份有限公司

# 天行应用系统安全审计系统 (Topwalk-VAS)

## 产品背景

天行应用系统安全审计系统通过网络侦听方式监视远程用户对查看/下载监控视频，控制摄像头方位等操作，对通过网络进行的操作行为进行审计和记录。

本系统通过旁路方式侦听网络中视频传输协议的数据包，通过信息还原和协议分析，可分析出对监控摄像头访问，操作等行为，并能得到终端用户的登录信息，如登录的机器IP地址，MAC地址，及其登录的用户名等。

用户可以通过管理界面进行规则设置，以记录有用的摄像头操作信息。用户可指定需监视的终端的IP地址，可指定需要重点监控的摄像头，可指定特定的操作信息，还可以通过操作类型和关键字对一些敏感的行为进行报警。用户可以设置各种规则来实现对不同类型和条件的审计结果进行记录和报警。

本系统根据用户设置的规则进行网络信息的收集和分析，并及时做出反应。用户可以实时查看各种视频访问和摄像头操作行为，也可以通过历史记录查询，为审计事件的分析、取证提供有力依据。

本系统强大的功能、简单的操作、友好的界面、全面的技术支持为您的网络安全提供有力保障。

## 方案概述

天行应用系统安全审计系统是一款对视频应用访问行为进行完整记录、综合分析、集中审计、预警监测、处置管理、线索跟踪、取证核查等多功能于一体的安全审计产品。

系统采用旁路部署的方式，通过抓包还原技术，实时记录网络中的视频访问行为，可实时发现入网设备、发现非授权访问行为、发现授权用户异常访问行为。对敏感信息泄露、侵犯公民隐私的非法行为进行有效的取证、溯源。主要应用于公安、军队、政府、金融等单位。

## 产品功能

### 设备识别

- 前端摄像头识别
- 系统自动记录全网被访问过的所有摄像头信息并形成活跃资产库，摄像头可以根据唯一设备编号自动匹配所在地域，并可以发现新摄像头提示管理员确认。

## ➤ 终端设备识别

系统通过提取信令中的客户端信息，可获取登录客户端IP、MAC地址、设备编号、用户名等信息，并可以发现新客户端提示管理员确认。

## 行为日志审计

系统支持对重要视频监控业务系统进行视频业务安全审计，对用户访问视频监控资源、控制信令操作行为等进行日志记录。日志记录涵盖访问的时间、登陆用户、被操作摄像头、访问行为及其他与审计相关的信息。

## 策略管理及告警

系统支持根据设备类型、设备信息、源地址、目的地址、时间、操作类型、用户、协议内容、访问次数自定义报警策略；

系统支持全局黑白名单设置，支持规则例外名单设置；

系统报警级别可分为一般、重要、严重三级，事件类型可分为普通事件、操作事件、敏感事件、异常事件。

## 业务审核及统计

系统支持基于客户端、摄像头、地区的访问统计和排名；

支持“一机一档”国标率的统计；

系统支持各类播放、下载、控制、回看等操作动作占比的统计；

系统支持周报、月报功能，并支持将报表导出为 Excel、PDF、Word、HTML 格式。

## 审计数据挖掘

系统通过提取视频信令返回的错误代码，分析访问失败、访问异常的原因，按区县统计访问异常次数；

系统从视频信令层记录、定位运维事件，方便运维团队故障排查，有效提高了运维团队的工作效率。

# 产品优势

## 安全合规

满足《关于加强公安视频监控安全管理工作的通知》公科信[2017] 222号文件关于“严防边界、纵深防御、主动监测、全面审计”以及“雪亮2.0”《公共安全视频监控建设联网应用共享交换技术体系建设指南》的相关要求。

## 部署便利

采用交换机旁路镜像部署，不依托业务系统，可还原基于GB/T28181、GB35114、标准SIP协议格式的视频操作行为，支持海康、大华、华为等视频协议。

## 审计全面

可对视频监控资源的调阅查看、服务接口响应、服务性能监测、服务流量大小等多维度进行审计还原。



## 行为可视

能够形成全网综合审计态势，通过摄像头、终端、用户、服务器多维度画像关联分析，具备发现终端、用户的异常视频操作行为能力。

## 应用场景

天行应用系统安全审计系统通常采用旁路镜像部署方式，在视频数据汇聚节点交换机配制镜像，通过对应用层视频信令协议进行解析，按各视频厂商信令格式还原成视频操作信令语言，全程记录网内视频资源访问行为，形成一条完整的溯源证据链。真正做到可控、可管、可溯源。

### 【服务声明】

本档意在向您介绍拓尔思天行网安部分产品、服务的当时相关概况，部分产品、服务的内容可能不时会有所调整。您所购买的拓尔思天行网安产品、服务的种类、服务标准等应由您与拓尔思天行网安之间的商业合同约定，除非双方另有约定，否则，拓尔思天行网安对本文档内容不做任何明示或默示的承诺或保证。

### 【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 400-609-2500 。