天御视频安全防护一体化平台

产品白皮书

北京天防安全科技有限公司

2025 年 10 月

目录

一、 应用背景

近年来，随着“平安中国”“智慧城市”“雪亮工程”等国家级战略的深入推进，视频 监控系统已从早期的治安辅助工具，演变为覆盖公共安全、城市管理、交通治理、应急指挥、生态环保等多领域的关键信息基础设施。然而，在视频网络高速扩张的同时，其安全防护体系却长期滞后。由于历史建设“重功能、轻安全”的惯性，大量视频设备在部署时未进行统一安全规划，普遍存在资产不清、弱口令泛滥、协议开放、边界模糊、终端不可控等系统性风险。视频专网中存储和传输的大量视频数据，不仅包含公共区域动态，更涉及个人隐私、重点单位布防、国家要害部位等高度敏感信息，一旦泄露或被恶意篡改，将直接威胁公民权益、社会稳定乃至国家安全。

国务院令第 799 号《公共安全视频图像信息系统管理条例》于 2025 年 4 月 1 日正式施行。条例对公共安全视频系统网络与信息安全提出了明确要求：1、产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施；2、完善防攻击、防入侵、防病毒、防篡改、防泄露等安全技术措施；3、使用视频图像信息，应当遵守法律法规，不得滥用、泄露。在这一政策背景下，公共安全视频系统管理单位在安全防护体系建设面临前所未有的合规压力与技术挑战。传统‘单点式’‘堆叠式’解决方案，针对公共安全视频系统的建设费用投入较高。亟需一套体系化、主动化、闭环化的综合防护方案，实现从“看得见”到“管得住”、从“防得住”到“溯得清”、从“数据不丢”到“数据不泄”的全面升级。

为此，北京天防安全科技有限公司基于多年深耕公安、交通、能源等行业视频安全的经验，融合资产准入、威胁监测、行为审计、数据防泄等核心技术能力，推出**天御视频安全防护一体化平台**。系统以“防入侵、防攻击、防病毒、防篡改、防泄漏” 为核心目标，覆盖视频网络全生命周期，构建纵深防御、智能联动、合规可信的新一代视频安全防护体系，为国家关键视频信息基础设施筑牢安全底座。

二、 系统设计目标

防入侵：**构建可信网络边界，杜绝非法设备接入**

前端摄像机分布广泛、部署环境开放，极易被替换、私接、仿冒；大量终端通过 USB 共享、双网卡、无线 AP 等方式违规接入，破坏专网封闭性。

通过**系统**实现对所有入网设备的自动发现、精准识别、动态画像与策略准入，确保“只有合法设备才能接入，只有授权行为才能通行”。

防攻击：**主动识别并阻断网络层与应用层威胁**

视频设备普遍存在弱口令、未修复漏洞（如海康身份绕过、永恒之蓝）、协议暴露等问题，成为 APT 攻击、Mirai 类僵尸网络的“跳板”。

通过**系统**建立覆盖资产脆弱性、边界完整性、攻击行为特征三位一体的主动监测体系，实现从“漏洞存在”到“攻击发生”再到“风险处置”的闭环治理。

防病毒：**阻断恶意代码在视频网络中的渗透与传播**

运维终端、管理服务器常因访问互联网或使用移动介质引入病毒，进而通过视频平台横向扩散，导致设备失陷、数据篡改或勒索加密。

通过**系统**在不依赖终端杀毒软件的前提下，通过网络流量层深度检测，实时识别并拦截含病毒的文件传输、恶意进程通信等行为，实现“病毒进不来、传不开、毁不掉”。

防篡改:**实现视频操作行为全链路可审计、可追溯**

视频平台普遍存在“操作无记录、行为不可查”问题，云台被恶意转动、历史录像被删除、敏感点位被频繁调阅等行为难以追责。

通过**系统**基于全协议信令还原技术，对 GB/T28181、GA/T1400 等标准协议下的 12 类操作（点播、回放、下载、控制、布控等）进行细粒度审计，确保每一条操作均有“五元组+账号+设备+时间+地理位置”完整证据链。

防泄漏:**实现视频数据从使用到外发的全生命周期受控**

视频数据在查看、下载、截屏、外发等环节极易泄露，传统手段无法防止“合法用户做非法事”。

通过**系统**通过终端播放控制、动态水印、外发包加密、服务器落地加密等组合策略，实现“数据不裸奔、使用有痕迹、外发可管控、泄露可溯源”。

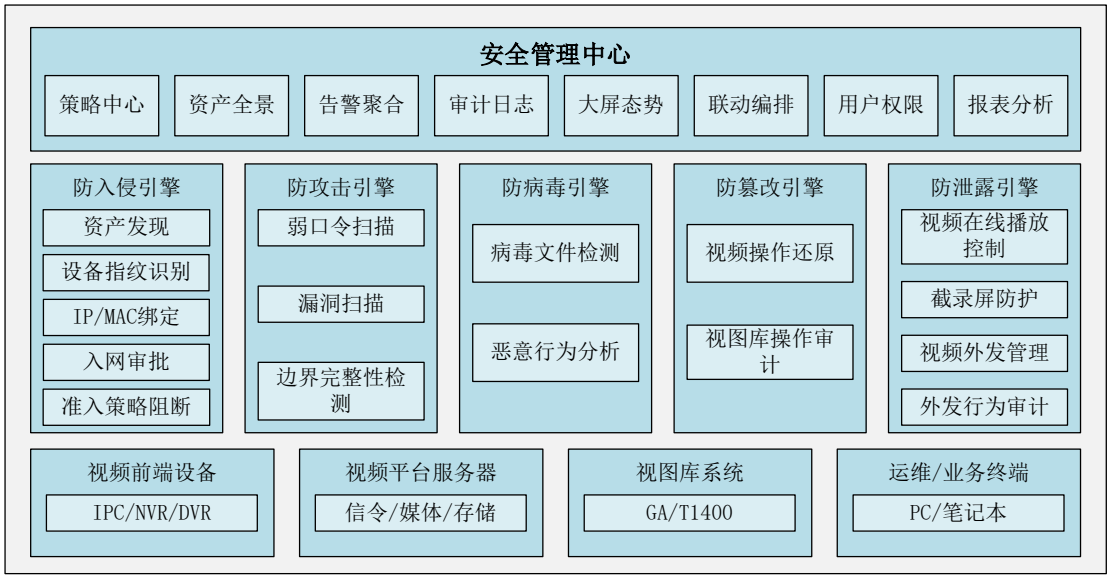
三、 天御视频安全防护一体化平台

3.1 产品概述

天御视频安全防护一体化平台是依据政策要求，面向公安、交通、金融、能源、文教卫等行业，围绕防入侵、防攻击、防病毒、防篡改、

防泄露五大核心需求，以 All In One 设计理念，深度融合资产管理、安全检测、网络准入、威胁监测、行为审计、数据防泄露等核心技术能力，全新打造的集成一体化主动监测与防御平台，为各行业公共安全视频系统管理单位，以较少的投入，便捷旁路部署，构建纵深防御、智能联动、合规可信的新一代视频安全防护体系，全面满足《网络安全法》《数据安全法》《GA/T 1788》及等保 2.0 等合规要求，为关键视频信息基础设施提供可信、可控、可审计、可追溯的安全底座。

3.2 产品架构



安全管理中心：提供策略管理、资产视图、风险告警、审计日志、大屏展示等核心功能。

五大防护引擎：

- 准入控制引擎：实现设备指纹识别与精准准入。
- 威胁监测引擎：执行漏洞扫描、弱口令检测、边界完整性检查。
- 恶意代码拦截引擎：基于流量深度检测病毒与恶意行为。

- 操作审计引擎：还原 GB/T28181、GA/T1400 等协议操作日志。
- 数据防泄漏引擎：管控视频使用与外发行为。

3.3 功能介绍

3.3.1 资产管理

通过主动扫描等技术手段，实现全网资产设备的自动化发现与动态识别，精准覆盖服务器、终端、网络设备、安全设备及物联网终端等各类资产形态；在此基础上，采集资产的硬件配置、软件版本、开放端口、运行服务等关键属性信息，确保资产画像的完整性与时效性。

通过资产发现、信息采集、智能分类的协同运作，系统能够持续构建并动态更新全网资产清单，有效消除资产盲区与管理死角，为安全风险评估、漏洞精准定位、威胁关联分析及合规审计等整体安全管理工作提供坚实、可靠、结构化的数据支撑，助力实现从"资产可视"到"风险可控"的闭环管理目标。

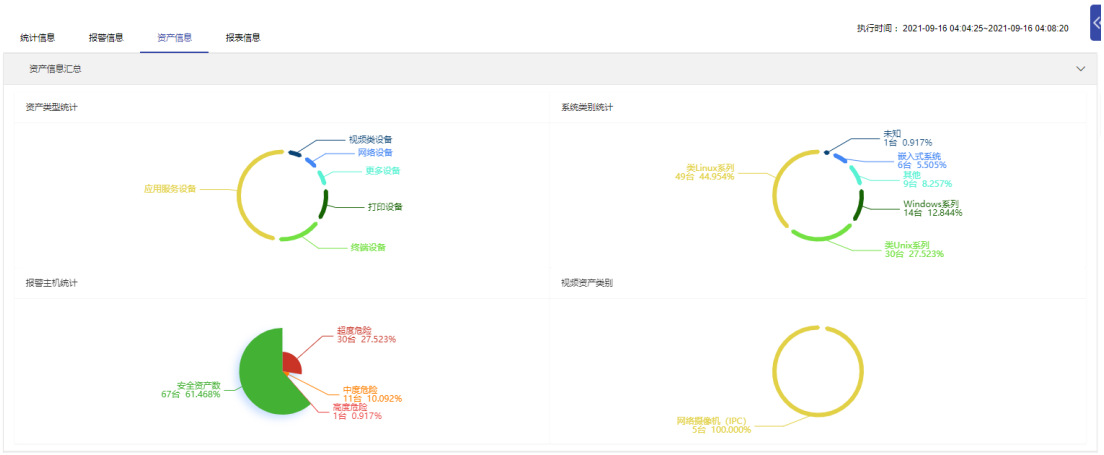


图 内部资产统计列表

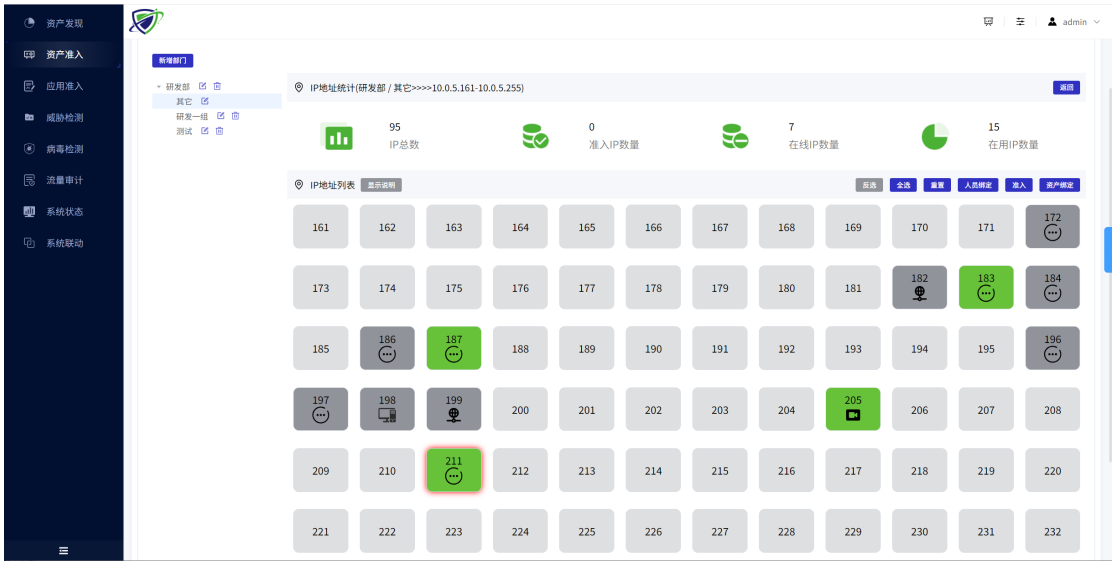
图 支持大屏数据展示（上述展示基于模拟数据）

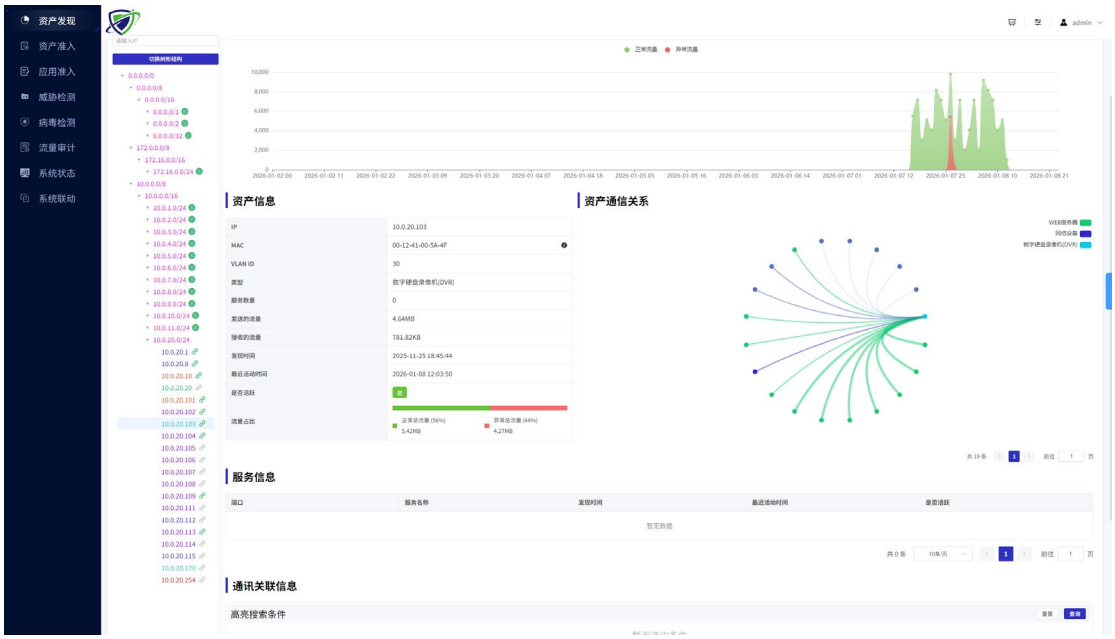
3.3.2 IP 地址资源管理

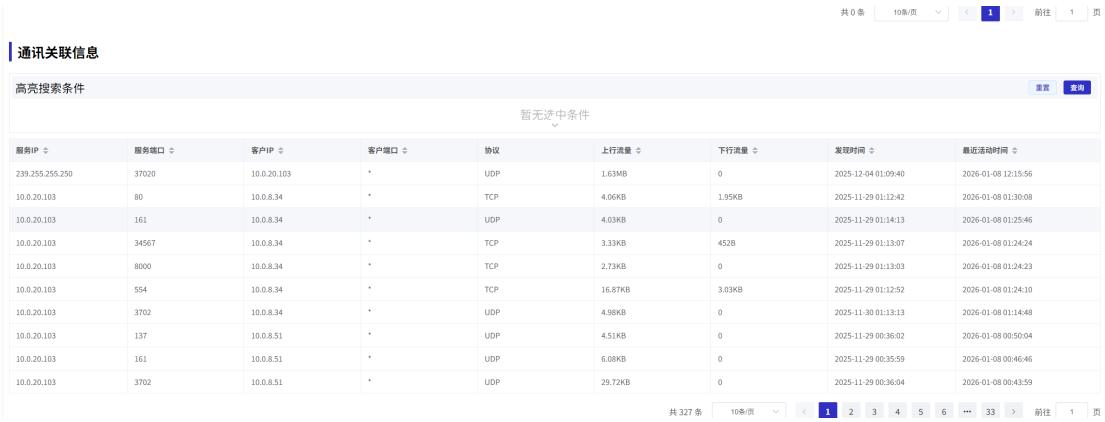
系统自动检测并精准识别网络中所有在线设备的 IP 地址信息，依托 IP/MAC 地址绑定、IP 分配授权审批等机制，实现 IP 地址资源的规范化分配、合规性校验与统一管控，有效防范地址冲突、非法占用及私接乱用等风险。

同时，系统围绕每一 IP 地址构建资产画像，整合关联设备的主机名、操作系统等属性信息，并结合 IP 访问行为日志进行全流程审计追踪，精准记录源目的地址、访问协议、通信时间及流量特征等关

键要素；辅以网络拓扑可视化引擎，动态呈现 IP 设备在网络架构中的逻辑位置与连接关系，为网络运维与安全分析提供清晰、实时、可交互的数据视图。







3.3.3 弱口令检测

1、视频监控设备弱口令专项检测

针对主流厂商的网络视频录像机（NVR）、数字视频录像机（DVR）、网络摄像机（IPC）等设备，内置覆盖海康威视、大华、宇视、华为、TP-Link 等数十家厂商的出厂默认口令知识库，并结合常见弱口令字典，对设备 Web 管理界面、ONVIF 接口、RTSP 服务等进行安全探测，可精准识别未修改默认凭据或使用弱口令的高风险设备。

2、视频监控相关数据库弱口令核查

针对支撑视频监控平台运行的后端数据库系统，检测其管理账户或业务专用账户是否存在空口令、默认口令或常见弱口令，防止因数据库凭证泄露导致视频数据被窃取、篡改或删除；

3、通用网络服务弱口令扫描

系统针对视频网络内部服务器开启的 FTP、SSH 及 RDP 等远程服务，自动开展简单口令专项检测，通过预设弱口令字典与策略规则，对常见默认密码、短位纯数字等低强度凭证进行匹配验证，及时识别并告警存在弱口令风险的资产，助力管理员快速加固认证配置，提升远程访问安全基线。

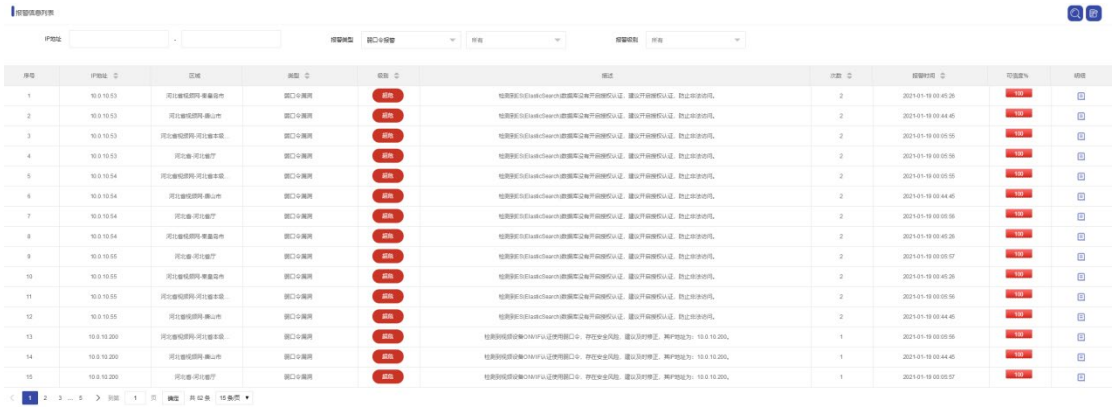


图 报警分类统计

3.3.4 漏洞检测

1、视频监控设备固件及服务层漏洞检测

针对 NVR、DVR、IPC 等视频监控终端设备，系统基于设备指纹识别自动匹配其品牌、型号及固件版本，并结合 CVE/NVD、CNVD、厂商公告及私有漏洞知识库，检测设备存在的高危安全漏洞。重点覆盖以下类型：

- 身份认证绕过漏洞；
- 敏感信息泄露漏洞；
- 命令注入/远程代码执行漏洞；
- 弱加密或协议缺陷；
- 固件更新机制缺陷。
- 检测过程采用非破坏性探测策略，避免对设备运行造成影响，

2、视频监控支撑应用中间件漏洞扫描

对视频监控平台所依赖的通用网络服务与中间件组件，系统进行深度漏洞识别，覆盖以下典型应用及其常见漏洞：

- OpenSSL：检测如 Heartbleed、CCS 注入等已知高危漏洞；
- OpenSSH：识别版本中存在的认证绕过、信息泄露或 DoS 漏洞；

- Apache Tomcat：检查默认示例页面未删除、管理接口弱口令、目录遍历等风险；
- Apache Struts2：重点识别远程代码执行类漏洞，此类漏洞常被用于攻陷视频管理平台后端。。

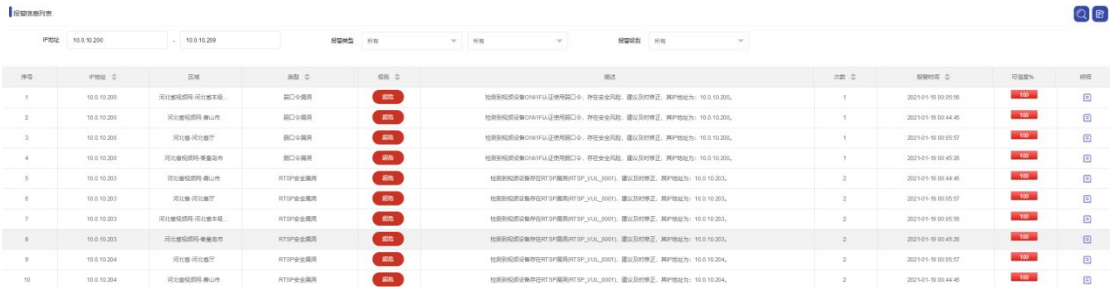
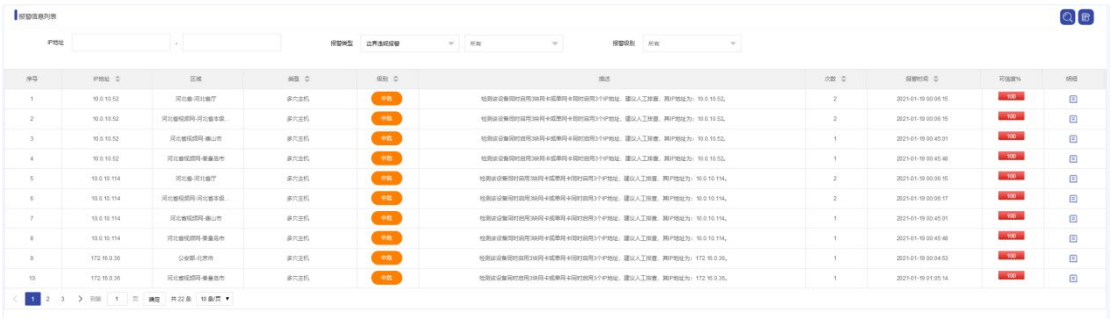


图 漏洞扫描结果

3.3.5 非法外联检测

为严守专网“物理隔离、逻辑封闭”的安全原则，系统对网络内部终端设备通过多种隐蔽通道违规访问外部网络的行为进行全方位监测、精准识别与实时告警，有效防范因非法外联导致的数据泄露、恶意软件传入或远程控制风险，切实提升网络边界完整性与安全防护能力。

- 双网卡/多网卡桥接：同一主机同时连接专网与办公网/互联网，并存在跨网数据转发；
- 智能手机共享网络：通过 USB、蓝牙共享或 Wi-Fi 热点将手机 4G/5G 网络引入专网终端；
- 个人无线热点直连：终端无线网卡主动连接非授权 SSID；
- 私接路由器/NAT 设备：在专网端口下级联家用路由器，形成 NAT 出口；



图边界违规行为查询

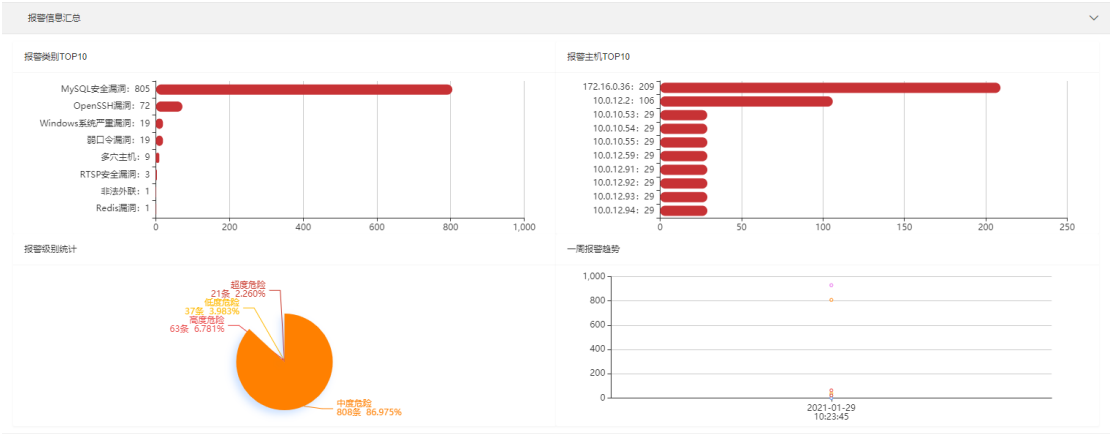
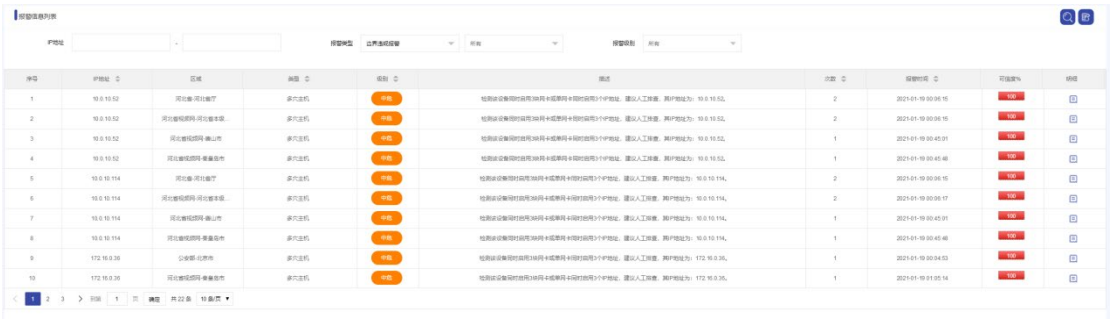


图 违规报警信息统计报表

3.3.6 违规内联检测

为严防外部设备绕过安全边界非法接入视频监控专网或关键业务网络，系统提供对违规内联行为的主动识别与实时告警能力。有效防止未经授权的外部终端、无线设备或远程控制工具从外部网络反向接入受保护的内部网络。

- 个人终端私接：如运维人员将个人笔记本、手机、平板等通过有线或无线方式接入视频专网交换机端口；
- 无线热点/路由器接入：在专网环境中私自部署 4G/5G CPE、家用无线路由器、手机热点等，形成隐蔽出口或入口；
- 远程控制工具反向连接：检测 TeamViewer、向日葵等工具，尤其关注非工作时间、非常规 IP 发起的连接；

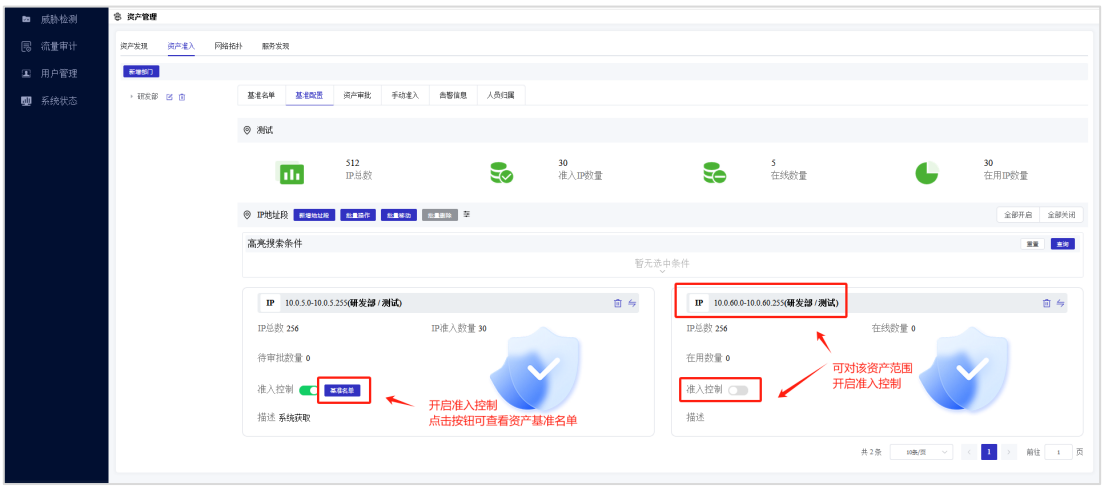


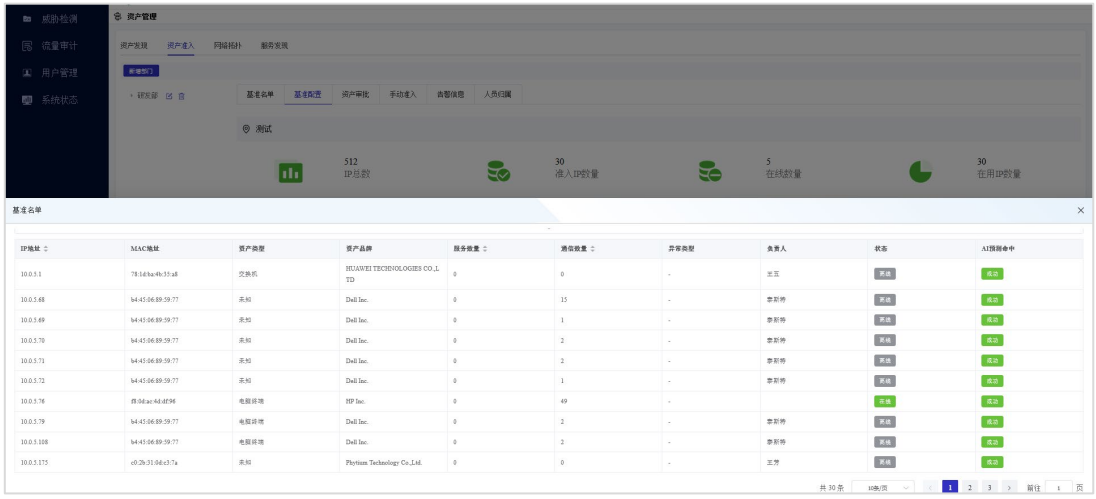
图边界违规行为查询

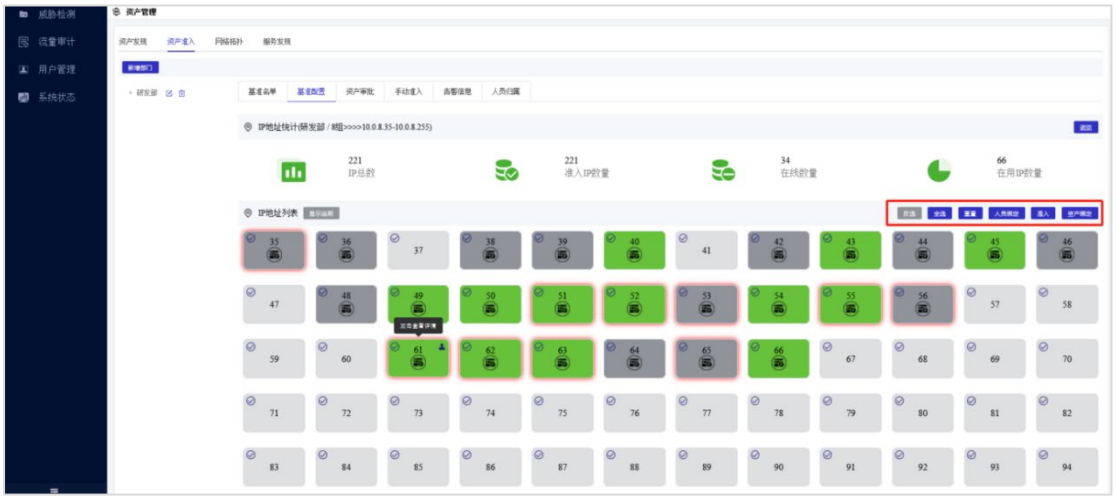
3.3.7 网络准入控制

系统采用 IP/MAC 地址绑定、设备指纹识别、应用协议分析及黑白名单匹配等多元化准入控制策略，对入网设备进行多维度身份鉴别与合规性校验，通过自动采集设备的硬件特征、网络属性及行为模式，构建精确的设备身份标识，并结合预设的准入规则进行实时比对与授权判定。

实现对所有入网设备的自动发现与动态识别，实时感知新设备接入行为并触发准入控制流程，对未授权设备自动阻断网络连接，对已授权设备实施精细化访问控制，确保只有经过身份认证与合规检查的合法设备才能接入网络，只有符合安全策略的授权行为才能正常通行，从源头构建网络接入安全防线。







3.3.8 视频应用协议管理

系统针对标准视频应用协议及各类私有视频协议实施准入控制管理，对视频设备的接入请求进行协议识别与合规性检查，确保只有符合规范的视频流协议才能建立连接；通过设备注册机制，对视频采

集设备、编码设备、存储设备及管理平台等进行统一登记与身份标识，建立完整的视频设备资产台账。

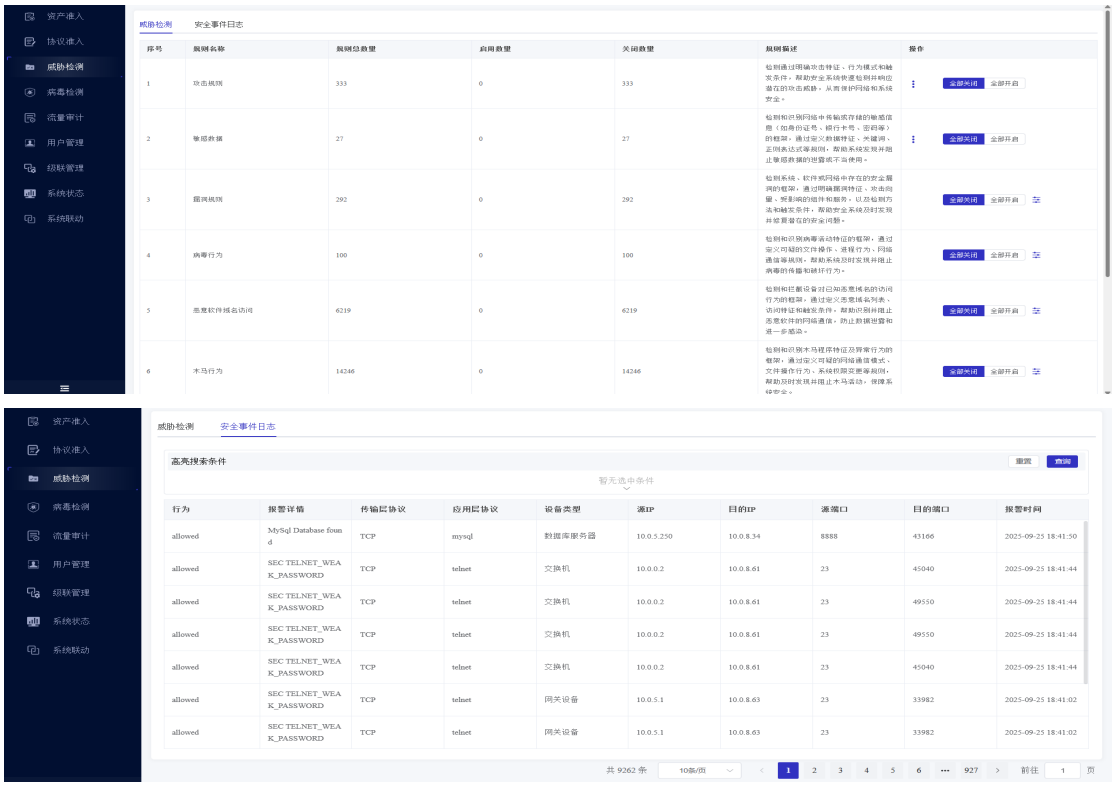
系统对已注册设备实施身份认证管理，验证设备凭证的合法性与有效性，防止未授权设备冒充接入；同时针对视频流的访问行为进行权限控制，确保只有经过认证的设备才能访问视频资源，只有获得授权的操作才能执行，实现视频设备从注册、认证到访问、控制的全流程有效管理。

3.3.9 网络攻击检测与防御

系统通过流量行为分析及特征匹配等技术手段，实时监测网络中的各类攻击行为，包括端口扫描、暴力破解、恶意代码传播、拒绝服务攻击、SQL 注入、跨站脚本等常见网络威胁，对异常流量模式、可

疑连接请求及违规访问行为进行持续识别与分析，确保第一时间发现潜在安全风险。

一旦检测到攻击行为，系统立即触发预警机制，通过告警日志、实时弹窗等方式通知管理人员，并提供攻击源 IP、目标地址、攻击类型、危害等级等详细信息；同时，依据预设的安全策略自动执行拦截防御措施，包括阻断恶意 IP 连接、丢弃攻击数据包、限制访问频率等处置动作，有效遏制攻击行为的扩散与危害，实现从威胁感知到主动防御的闭环响应。

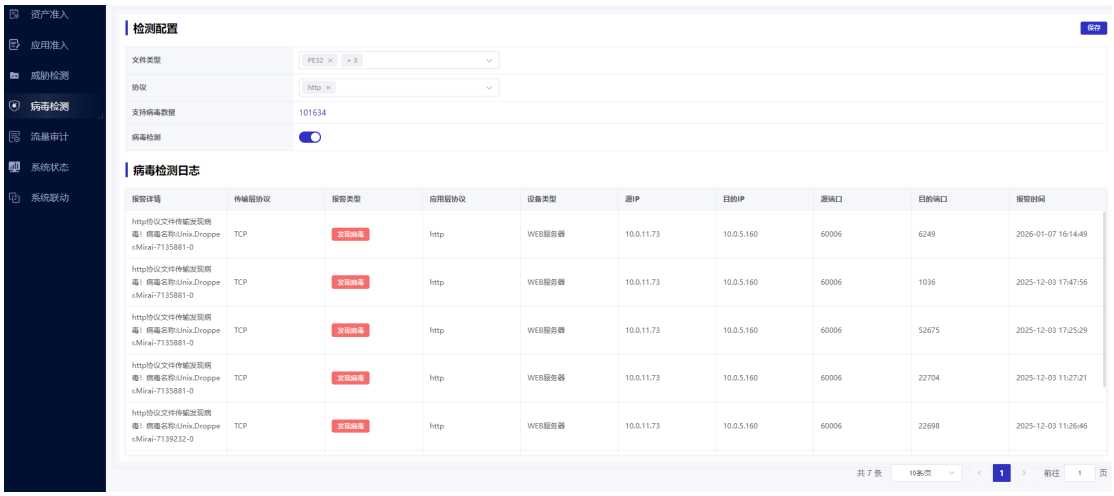


3.3.10 病毒检测与防御

系统通过特征码匹配等多维技术手段，实时监测网络流量与文件传输过程中的病毒攻击、恶意代码注入及感染文件传播等安全威胁，精准识别已知病毒变种、未知恶意程序及隐蔽载荷行为，对可疑文件

的下载、上传、共享等流转环节进行深度扫描与风险判定。

一旦检测到病毒或恶意代码相关行为，系统立即触发实时报警机制，通过告警日志、管理控制台及通知接口等方式推送风险详情，包含威胁类型、传输层协议、设备类型等关键信息；同时依据预设防护策略自动执行拦截处置，包括阻断恶意连接、隔离感染文件、终止可疑进程等操作，有效遏制病毒攻击的初始入侵与横向传播，保障网络环境与终端系统的安全稳定运行。

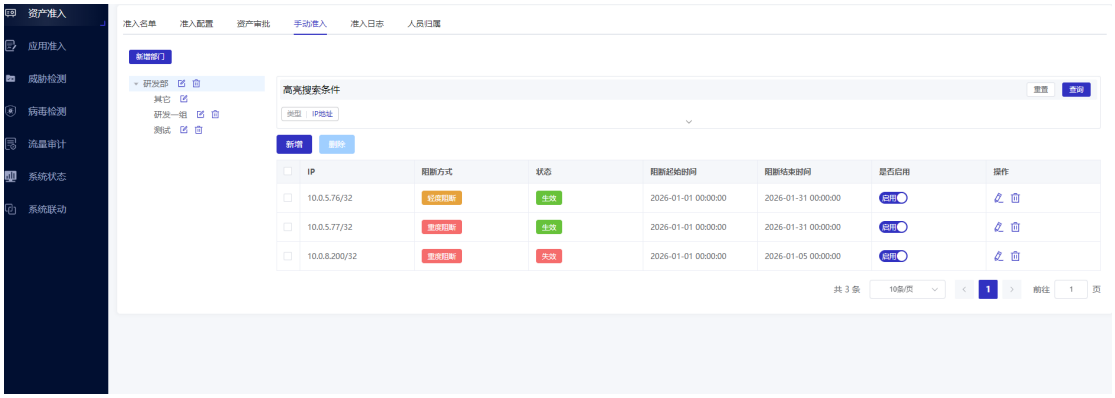


3.3.11 违规设备阻断控制

系统针对网络中发现的各类违规行为，包括未授权终端违规接入、设备身份冒用、终端非法外联、网络攻击行为及病毒传播活动等安全

威胁，通过预设的多维度管控策略进行精准识别与分类处置，依据违规类型、风险等级、影响范围等要素自动匹配相应的阻断控制措施，实现对违规行为的针对性响应与隔离。

在此基础上，系统支持灵活配置阻断策略，可对违规终端实施网络访问限制、会话连接中断等差异化管控动作，确保在最小化业务影响的前提下快速遏制安全风险扩散；同时记录违规行为的完整处置日志，为后续审计分析与策略优化提供数据支撑，有效保护网络整体安全性与业务连续性。

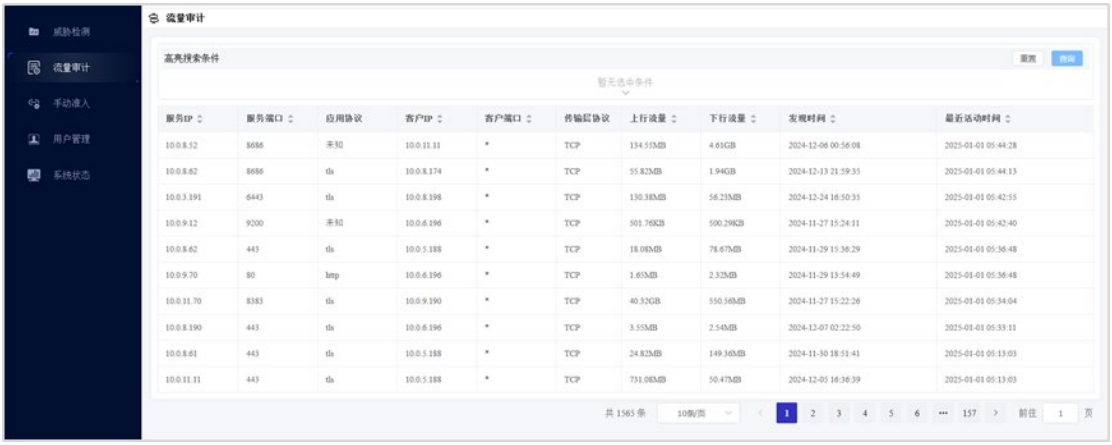


3.3.12 视频操作审计

系统针对标准视频应用协议的视频数据传输过程进行细粒度解析，对视频调阅、直播推送、录像回放等数据流转行为进行精准识别与关联记录；同时针对视频平台的访问与操作行为，对用户登录、设

备检索、云台控制、参数配置等关键动作进行指令级审计，确保每一步操作均可追溯。

在此基础上，系统对视图库的访问行为实施全流程监控，涵盖视频/图片资源的检索、预览、下载、共享、删除等操作，自动记录操作主体、目标资源、执行时间、客户端信息及操作结果等审计要素，形成完整、规范、不可篡改的审计日志体系，支持按时间、用户、设备、操作类型等多维度进行查询分析与合规审计，实现视频业务从数据传输到资源访问的全过程可管、可控、可溯源。



3.3.13 异常访问检测

系统针对各类视频操作及标准视频应用协议的配置参数进行深度检测与分析，自动识别视频编码过程中的编码格式错误、编码参数冲突、编码标准不兼容等异常问题，同时检测视频流中存在的编码重复配置、多路视频编码参数冗余等资源浪费现象，并对使用默认编码配置、编码强度配置不当、分辨率与码率匹配不合理等安全隐患进行精准发现与风险评估。

一旦检测到配置异常事件，系统立即生成告警信息，通过管理控制台、日志系统及通知接口等方式实时推送异常详情，包含异常类型、

涉及设备、配置参数、风险等级及优化建议等关键信息；同时对所有配置异常事件进行完整的审计记录，自动保存异常发生时间、持续时长、影响范围及处置状态等审计要素，形成可追溯的配置异常档案，为后续的配置优化、故障排查及合规审计提供数据支撑，确保视频系统的编码配置符合安全规范。

3.3.14 视频存储完整性检测

系统针对各路视频采集设备、存储设备及视频管理平台的视频数据保存情况进行持续监测，自动采集并分析视频录像的存储时长、归档周期，精准识别存储时间不足、超期未清理、策略未生效等合规性问题，确保视频数据的保存周期符合法规要求与业务规范。

同时，系统一旦发现保存时间不达标或完整性异常，立即生成告警记录并推送审计日志，包含涉及设备、异常类型、影响时段及修复建议等关键信息，助力管理人员及时开展存储优化与数据修复，有效保障视频存储的合规性、完整性与可用性。

3.3.15 视频访问控制

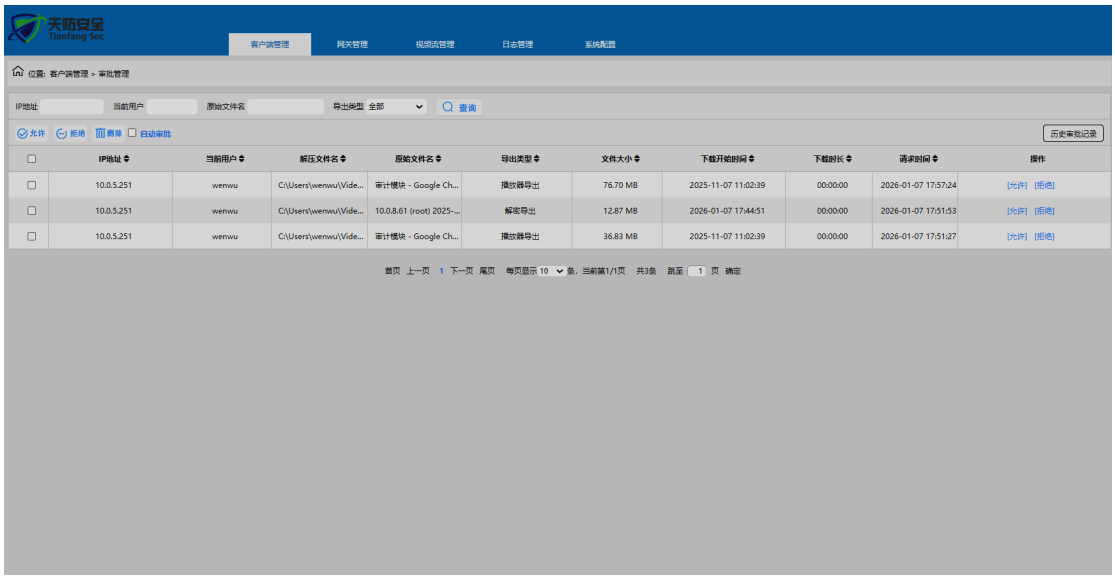
系统通过网络访问策略配置，构建可访问视频平台的授权终端白名单列表，对访问请求进行身份校验与权限匹配，自动拦截未授权终端的连接尝试，确保只有经过认证的合法终端才能建立与视频管理平台的网络会话。

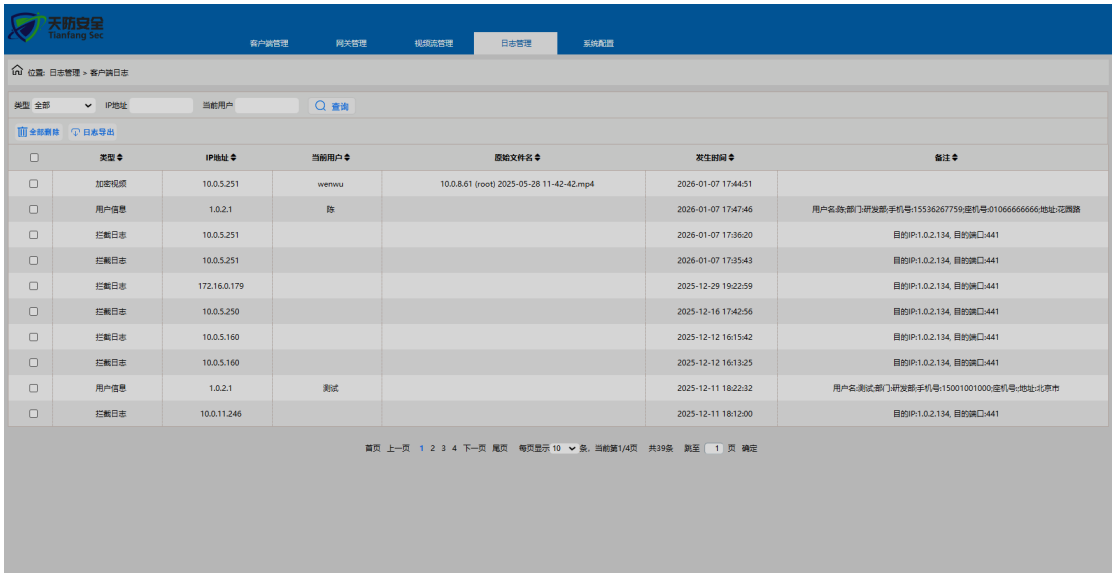
在此基础上，系统对授权终端的视频访问行为进行精细化管控，针对视频调阅、实时播放、录像回放等核心操作实施策略约束，结合访问时段、操作权限及流量阈值进行动态授权管理，确保终端仅能在许可范围内访问视频资源；同时记录所有访问请求的源终端信息、操作类型及执行结果，形成完整的访问审计日志，为视频平台的安全接入与合规使用提供可靠保障。

3.3.16 视频数据管理

系统对终端的视频下载行为实施严格的审批管控机制，终端用户发起视频下载请求时，系统自动拦截下载操作并触发审批流程，将下载申请提交至授权管理人员进行审核；审批内容包含下载申请人、目标视频资源、文件规格及操作时间等关键信息，管理人员根据安全策略与业务需求对下载请求进行合规性审查与授权判定。

只有在审批流程完成且获得明确同意后，系统才会解除下载限制，允许终端执行视频下载操作；对于未审批或审批拒绝的请求，系统持续阻断下载行为并记录违规尝试。同时，系统对所有视频下载审批流程进行完整审计记录，自动保存申请时间、审批人、审批结果、下载执行时间及文件信息等全流程日志，确保视频下载行为的事前审批、事中管控、事后可溯，实现视频数据外发的安全合规管理。



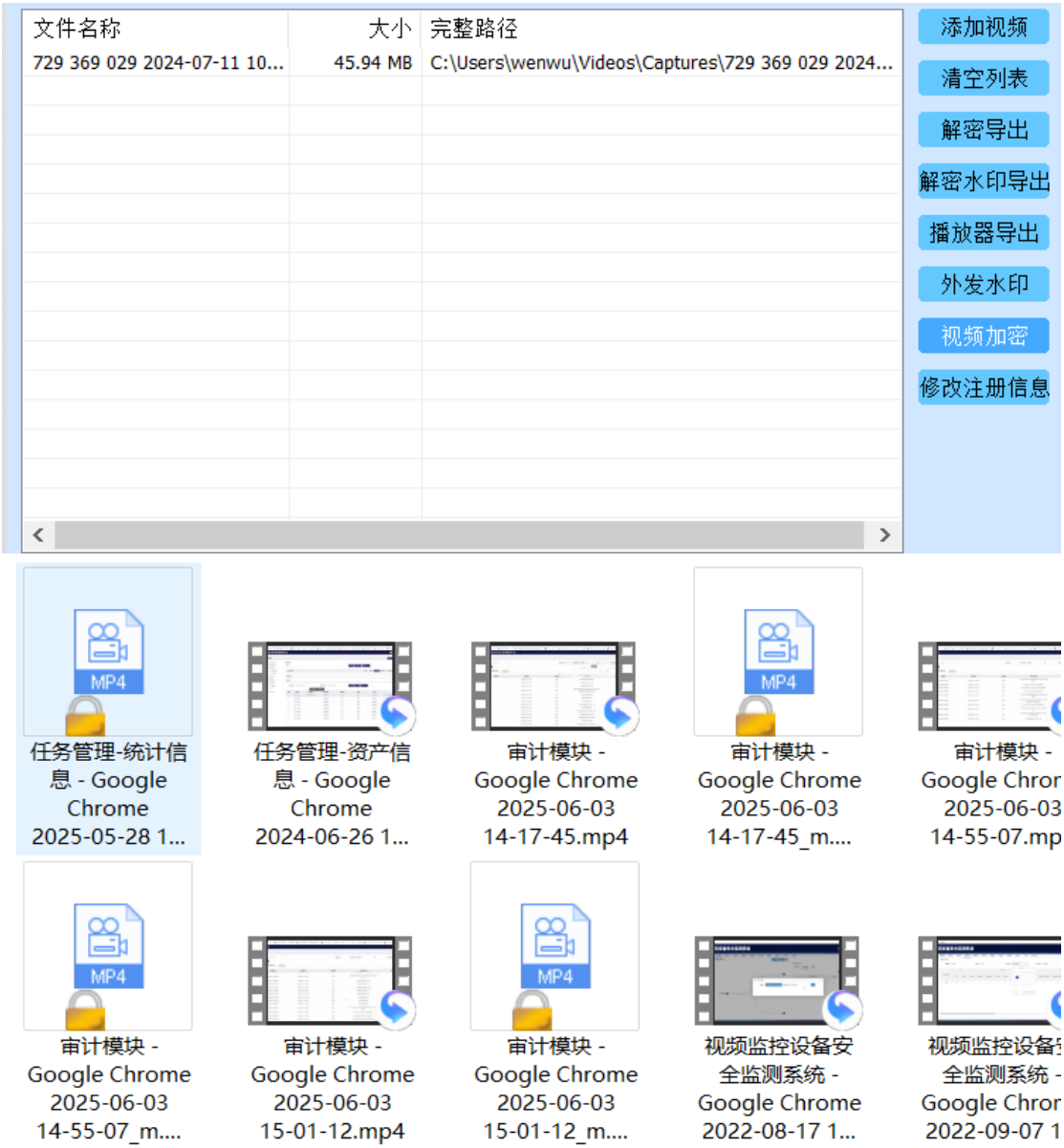


3.3.17 视频数据加密

系统对终端下载保存的视频数据及外发视频文件实施全流程加密处理，对视频文件的内容数据、元数据及索引信息进行加密封装，确保视频数据在终端本地存储、移动介质保存及网络传输过程中始终以密文形式存在，防止因设备丢失、非法拷贝或未授权访问导致的数据泄露风险。

在此基础上，系统对加密视频文件的访问实施密钥管理与身份认证机制，只有经过授权的用户或终端才能通过合法凭证解密并访问视

频内容，同时对加密策略、密钥使用及解密操作进行完整审计记录，确保视频数据在存储、传输、访问等各环节均处于加密保护状态，有效保障视频数据的机密性、完整性与可控访问，满足视频数据安全合规与隐私保护要求。

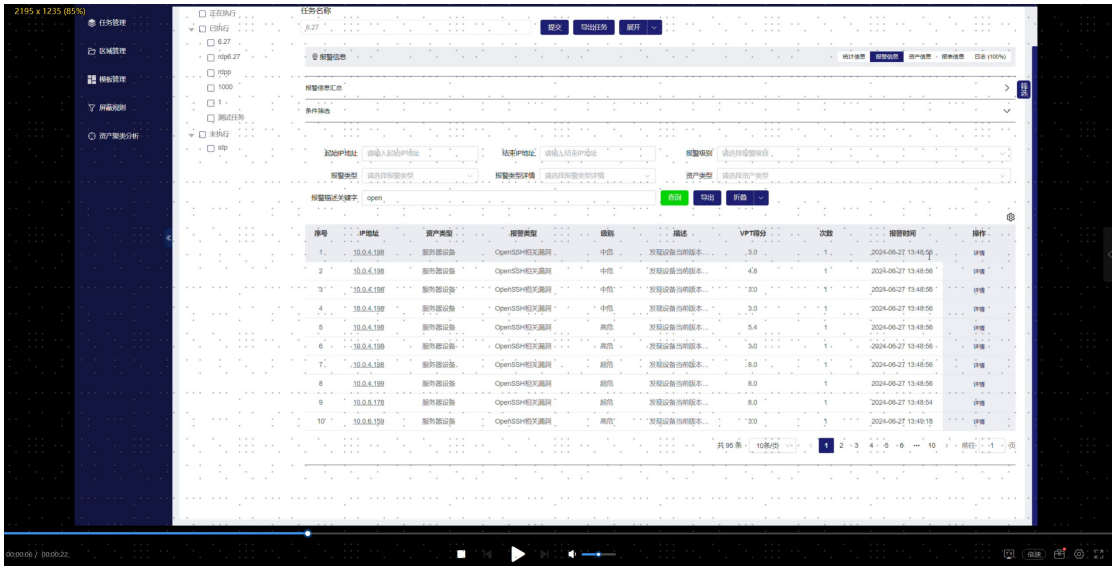


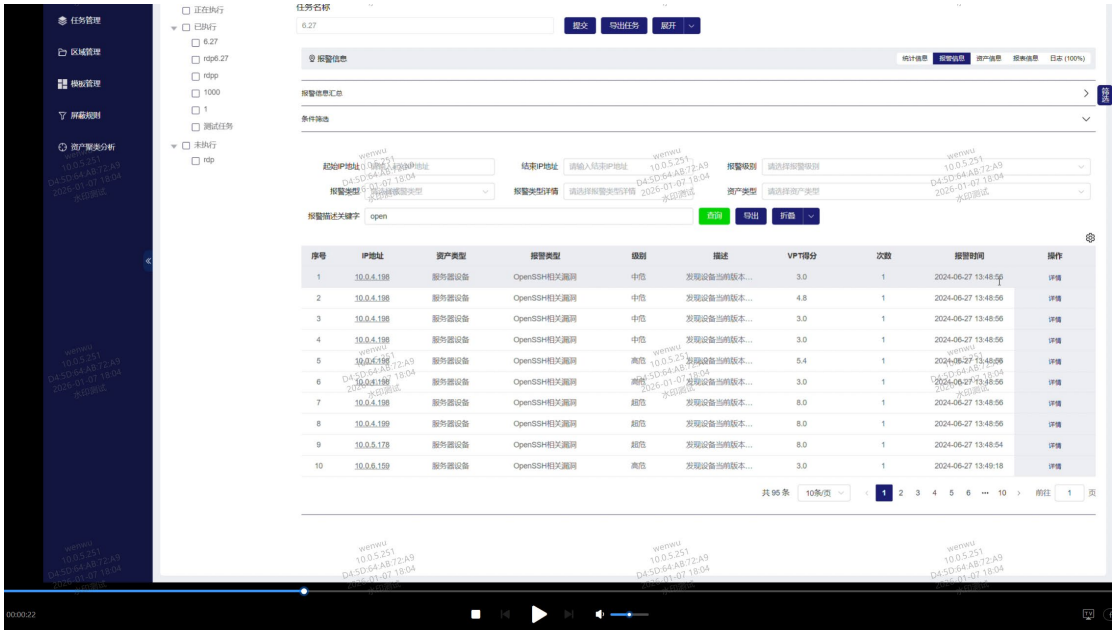
3.3.18 视频水印

系统在终端播放视频时，支持采用明文文本水印、点状暗纹水印、二维码水印等多种自定义水印形式，将用户身份信息、终端标识、播放时间、IP 地址等溯源要素以可见或不可见方式嵌入视频画面，其中

明文文本水印直接叠加显示于视频表面，点状暗纹水印以离散点阵形式隐蔽分布于视频帧中，二维码水印则编码关键溯源信息生成可识别图形，多种水印形式可单独或组合应用，满足不同场景下的安全管控需求。

当视频内容通过截屏、拍照、录屏等方式非法流出时，系统可通过水印提取与识别技术，从泄露的视频截图或录像中快速解析出水印信息，精准追溯泄露源头，定位到具体的播放用户、终端设备、播放时间及操作位置等关键要素，为视频泄密事件的责任认定与取证调查提供技术支撑；同时系统对所有水印添加操作、提取记录及溯源结果进行完整审计日志记录，形成视频内容流转的全链条可追溯体系，有效震慑和防范视频数据的违规传播与非法扩散。

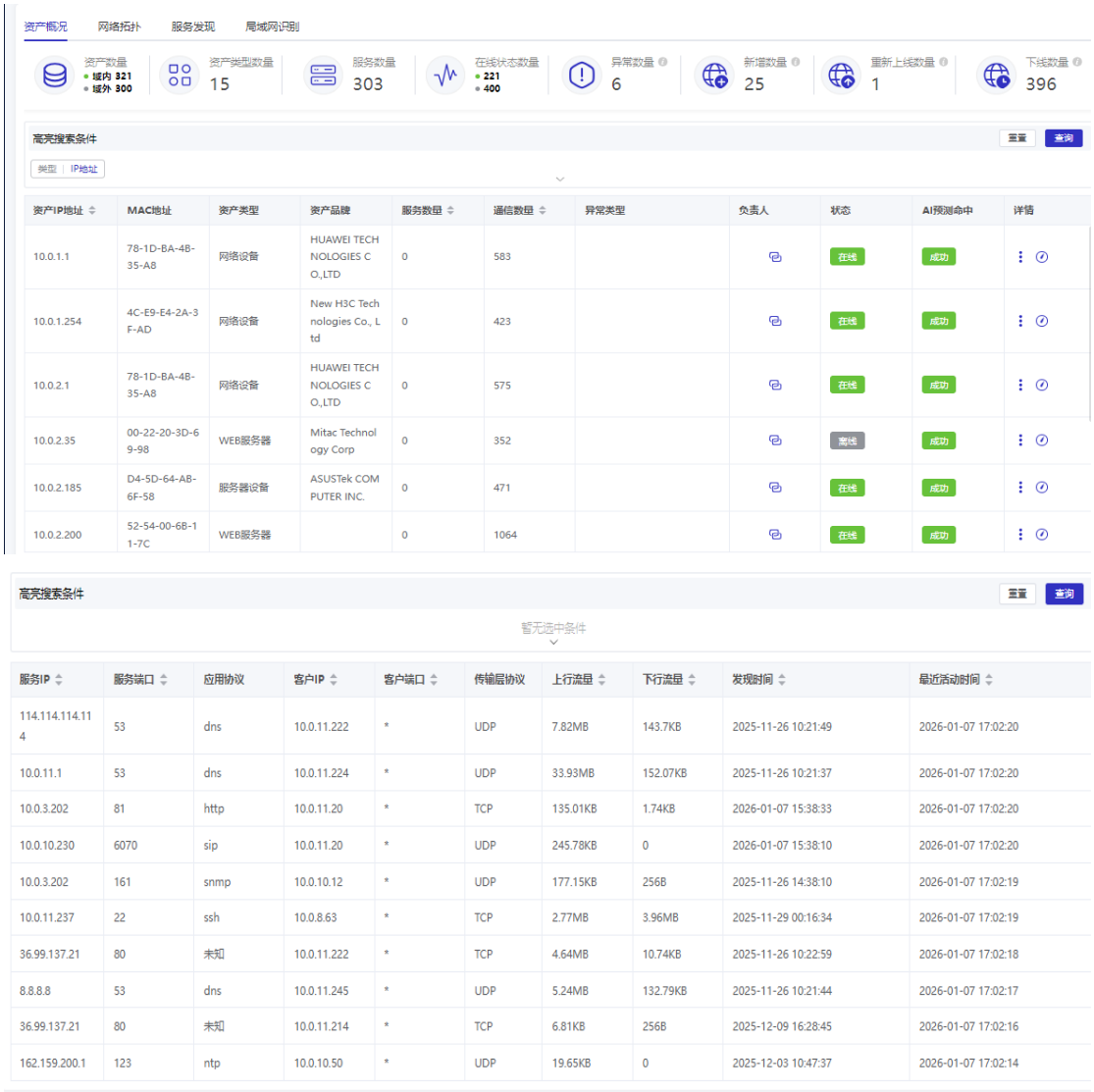




3.3.19 资产运维审计

系统提供对设备资产的全方位监测与审计管理能力，实时采集并展示设备的在线/离线状态信息，通过心跳检测、状态轮询及事件驱动等机制，精准感知设备的运行状况与可用性变化，自动记录设备上下线时间、持续时长等关键信息；同时对设备接入行为进行全过程监测，捕捉设备接入网络的认证过程、接入方式及接入时长等细节，确保设备接入行为的可管可控。

在此基础上，系统自动发现并绘制设备之间的通讯拓扑关系，通过流量分析、协议识别及连接追踪等技术手段，可视化呈现设备间的逻辑连接、数据流向、依赖关系及通讯频率；并结合网络流量审计功能，对设备间的通讯流量进行深度解析与统计分析，记录流量大小、协议分布、会话数量等审计要素，形成设备资产从状态监测、接入管理、拓扑展示到流量审计的多维度管理体系，为网络运维、安全分析及故障排查提供全面的数据支撑。

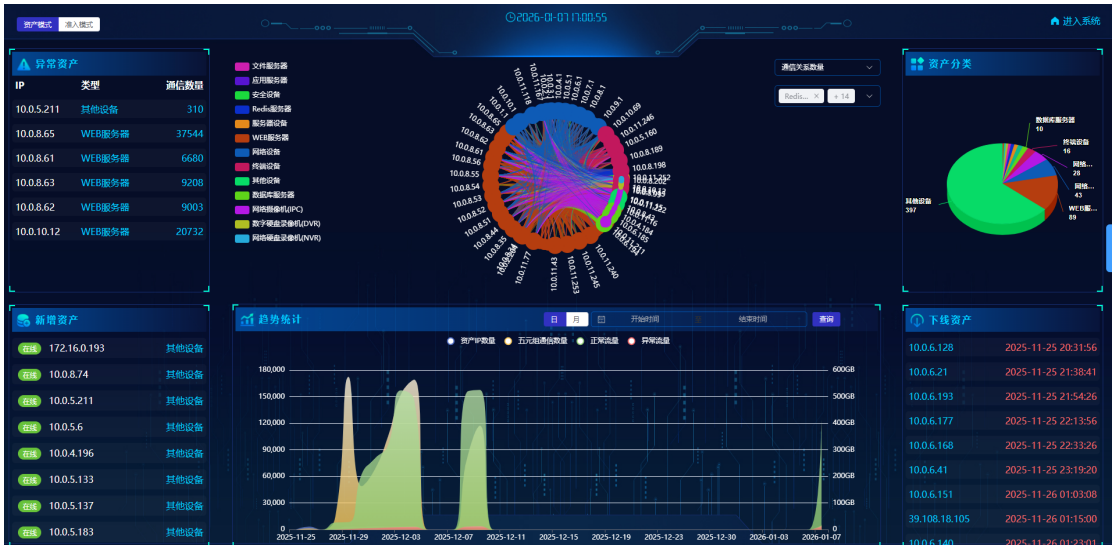


3.3.20 态势感知

系统提供全网资产态势、网络准入管理态势、安全状态态势等多维度的统计分析与可视化展示能力，针对全网资产态势，自动统计资产总量、在线/离线设备数量、资产类型分布等核心指标，支持按部门、区域、网段等维度进行资产分布与状态分析；针对网络准入管理态势，实时呈现准入设备总数、违规接入次数、准入策略执行效果等关键数据，动态展示准入控制的整体运行状况与合规水平。

在此基础上，系统对安全状态态势进行全方位统计，包括安全事件总量、威胁等级分布、攻击行为类型、病毒传播情况、违规行为统

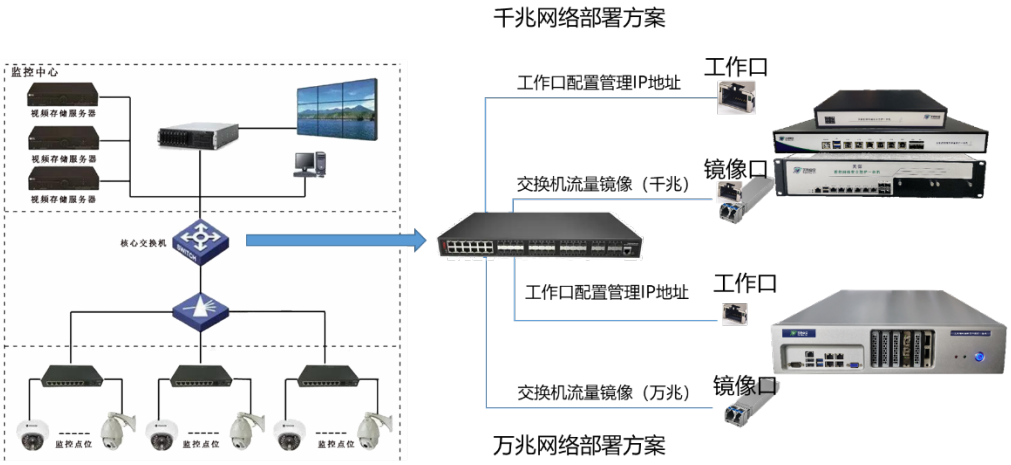
计、风险处置率等核心指标，并结合时间趋势、区域分布、设备类型等多维度进行交叉分析与关联展示；通过可视化大屏、图表、报表等多种形式，直观呈现各类态势数据的实时状态、历史趋势及对比分析结果，支持管理人员快速掌握全网资产状况、准入管理效果及整体安全态势，为安全决策、资源调配及风险管控提供数据支撑与可视化依据。



3.4 部署方案

系统采用旁路镜像监听 + 逻辑主动干预的工作模式。通过实时分析网络流量，识别病毒传播（横向移动）及异常扫描行为，并对攻击行为进行阻断。

系统的部署方式如下图所示：



系统基于流量检测实现对网络攻击、网络防病毒、准入控制等安全能力，因此本系统的部署取决于用户的网络架构和网络规模，原则上系统部署的点位位于用户的网络的三层交换（核心交换机）位置，并能够获取到网络中的大多数通讯数据的流量。为确保设备能有效“看见”危险行为并成功“阻断”，交换机侧必须满足以下限制条件：

- 部署位置限制（流量覆盖）

东西向流量获取： 病毒传播通常发生在同 VLAN 内部。镜像点必须选择在能够观察到终端互访的汇聚层或接入层交换机上。若仅镜像核心出口，将无法感知道内网横向攻击。

双向镜像要求： 交换机镜像源必须配置为 Both （同时镜像入站和出站流量），否则无法分析 TCP 握手状态，导致阻断失败。

- 镜像口 Trunk 模式限制

VLAN Tag 保留：交换机在镜像流量时，必须保留原始的 VLAN 标签（Dot1q）。技术原因： 设备需要根据镜像流量中的 VLAN ID，通过工作口在对应的广播域内发送阻断报文。若标签丢失，设备将无法定位目标路径。

四、 系统优势

- 合规化强：依据政策要求针对性设计，满足各行业公共安全视频系统的一站式“五防”建设需求。
- 性价比高：根据公共安全视频系统的规模，提供多款不同性能产品可供选择，在满足安全合规要求的同时，具备轻量化

部署特性与显著成本优势。

- 集成度高：All In One 设计理念，深度集成与融合多项安全能力于同一设备，实现统一策略管理与联动响应一体式解决方案。

五、 产品价值

- 合规价值：满足《条例》强制性要求，是实现合规的标准化“工具包”，避免因不符合《条例》安全规定而面临的法律责任与整改风险。
- 安全价值：构建主动防御体系，将零散的安全能力整合，有效应对网络攻击、病毒入侵、数据篡改和敏感信息泄露等综合安全风险，实现威胁检测、响应、取证的闭环管理，变被动防御为主动防御。
- 管理价值：实现集约化统一管理，通过一个平台统一管理安全策略、资产、日志和事件，大幅降低运维复杂度和管理成本，解决传统分散式建设导致的安全能力参差不齐、运维效率低下和应急响应慢的问题。