**视频防泄密安全防护**

**解决方案**



 目 录

[1. 解决方案 4](#_Toc8536)

[1.1 前端接入层防护 4](#_Toc8868)

[1.1.1准入控制 4](#_Toc22490)

[1.1.2设备发现与识别 4](#_Toc9236)

[1.1.3网络拓扑图绘制 5](#_Toc30276)

[1.1.4 IP地址池管理 5](#_Toc11214)

[1.1.5设备管理 5](#_Toc21713)

[1.1.6 GIS地图物理定位 5](#_Toc21271)

[1.1.7报警管理 6](#_Toc10691)

[1.1.8图表管理 6](#_Toc14581)

[1.2 视频数据防护 7](#_Toc31407)

[1.2.1视频数据资源访问安全 7](#_Toc11456)

[1.2.2本地视频数据防拍照 8](#_Toc8505)

[1.2.3视频数据本地存储安全 8](#_Toc4731)

[1.2.4视频数据对外交互安全 9](#_Toc18082)

[1.2.5视频数据导出安全 10](#_Toc30364)

[1.2.6流程化审批管理 10](#_Toc5331)

[1.2.7数据图表分析 11](#_Toc13676)

[2. 方案优势 12](#_Toc4309)

[2.1 资产探测，精准管理 12](#_Toc31281)

[2.2 严格把控边界，杜绝滥用违规等行为 12](#_Toc29128)

[2.3 可视化运维管理，为处置提供决策 12](#_Toc15537)

[2.4 全方位、多视角的风险预警 12](#_Toc8411)

[2.5 监控数据全生命周期管控 13](#_Toc22489)

[3. 设备选型 14](#_Toc12766)

# 解决方案

提供综合化安全防护方案，前端防护层面，对网络内接入的各类设备进行识别、过滤、阻断，确保接入视频监控网络设备的合法性和安全性，对运行中的设备进行实时监控，利用独有的感知发现技术，及时发现网络中伪冒、入侵、异常的设备。数据防护层面是基于视频数据的整个生命周期，从对视频数据存储的访问安全控制、使用管控到事后的溯源追责，为用户提供整套的视频数据安全防护解决方案。

## 前端接入层防护

### 1.1.1准入控制

新一代准入控制技术以入网设备信息绑定、杜绝非法入侵和运行监测为主要设计理念，实现对设备的准入控制管理。秉承“不改变网络、不依赖网络设备、部署简单”的特性，兼容各种复杂的网络环境，支持分布式快速部署，为客户解决非法设备随意接入企业视频监控网的问题，达到“信任接入、接入可知、接入可管”的管理规范。

### 1.1.2设备发现与识别

通过SNMP协议、数据链路发现协议、设备特征识别技术，对视频监控网络内的所有前端设备进行主动探测+被动协议分析两种方式进行发现与识别。

系统通过协议分析后可获得网络内设备的信息，与系统数据库进行对比，鉴别设备的合法性，识别得到的设备属性主要包括设备类型、设备型号、设备IP/MAC信息及设备厂商等；同时采用网络感知发现模块，对网络内设备运行情况进行实时监控，检测是否存在设备异常，设备是否被伪冒替换、是否存在陌生入侵设备。系统将探测的前端设备信息与后台合法设备数据进行综合验证，对接入设备进行标定，对非法接入的设备系统自动报警、阻断。

### 1.1.3网络拓扑图绘制

系统可根据网内的设备连接真实情况，生成动态网络拓扑架构图，同时可显示相关设备的IP地址、设备厂商、设备型号等信息，并且可与入侵检测功能进行联动，实现报警图形化，方便管理人员快速进行故障定位。通过背板功能查看当前网络设备的端口情况，使端口信息及端口下联设备一目了然。同时提供端口开关功能，当网络发生异常时，快速定位并关闭端口，提高网络的安全性。

### 1.1.4 IP地址池管理

IP地址作为网内正常通信的关键件，其合法性与否决定了网络的正常使用，而在实际的运维过程中管理人员很多时候无法对某个IP地址的即时在线状态进行正确判断，从而导致IP地址重复分配，造成网络风暴的发生。

系统针对此类问题，提供可视化IP地址使用信息，根据网内IP地址情况，将信息分为“在线”、“离线”、“长期离线”和“未使用”四种模式，管理人员可快速辨别当前地址的状态。

### 1.1.5设备管理

系统采用可视化设备管理，可以清晰的了解组织结构下设备的分类、数量、在线状态，可对设备类型进行分类查询，设备列表中显示设备的类型、IP、MAC、厂商、物理位置（摄像头经纬度）、入网状态（信任/隔离）、事件信息（新增、网络入侵、MAC变化、类型失联、类型变化、离线、时间异常）等信息，并对设备指纹以二维码形式展示，扫描后显示设备详细信息。可实时查看视频图像查看，精准确认图像质量。可一键对设备进行信任入网、隔离通讯，可对列表中的设备进行物理定位操作。

### 1.1.6 GIS地图物理定位

系统融入了地图离线包，预留了警用地理信息系统（PGIS）接口，可以与PGIS系统完美对接，抽取摄像头地理位置信息，并将摄像头分布情况自动关联至矢量地图。当探测到摄像头发生故障与异常时，与报警模块进行联动，平台弹出报警信息的同时，在地图上自动定位闪烁报警，并在地图上呈现红色，以便管理员快速地区分，提高维护的效率。

### 1.1.7报警管理

系统报警模块内置多种报警触发事件（网络入侵、MAC变化、类型失联、类型变化、离线、时间异常等）支持对发生事件类型自定义报警等级（警告、严重、致命）。报警模块实时与设备发现模块、识别感知模块、准入控制模块进行数据交互，接收到入侵、伪冒、离线、时间异常等事件时，触发报警机制，可发送报警邮件、报警短信、报警弹窗消息、并在GIS地图定位、网络拓扑图闪烁标定。在报警管理中可查看报警的详细内容，包含报警时间、报警设备类型、报警IPMAC、事件类型、报警内容、入网状态等，管理可对报警的设备进行手动定位，查看物理位置，修改入网状态。同时提供可视化的报警查看功能，针对同一设备出现的历史报警信息以时间轴的形式进行统计展现。

### 1.1.8图表管理

图表管理是对视频网中的网络、设备等运行情况进行汇总展现，系统提供IP管理报表、资产报表、可用性报表、报警报表，管理人员可根据图表分析结果对存在的安全薄弱点进行安全加固，提高网络防护。

IP管理报表，清晰的展现出当前网络中IP资源的使用情况，分别统计在线、离线、长期离线和未使用的IP数量，方便对IP资源的统一管理，提高工作效率。

资产报表对网络中的所有设备进行统计分析，统计出各类资产的数量和占比以及摄像头品牌的分布情况，可根据组织结构进行实时查看，对全网资产全面掌控。

可用性报表包含了摄像头在线率、图像获取率和图像获取状态的统计，对网络健壮性和摄像头设备的可用性进行整体分析，提高摄像头的高可用性。

报警报表对网络中所有异常事件进行统计，展示出不同类型报警数量和占比，方便管理人员针对性进行网络维护。同时对网络内摄像头设备的初始口令进行探测，降低摄像头设备被攻击的风险。

## 视频数据防护

### 1.2.1视频数据资源访问安全

系统集成金盾软件自主研发的“下一代准入控制”系统，对视频资源存储网络系统进行网络层级的安全防护。管理员可指定仅安装有客户端系统的合法终端设备访问企业视频网络资源系统，阻断其他非法设备对资源的访问，有效的阻断黑客对企业视频网络内数据资源的入侵及非法用户接入，从网络数据流层面保障视频资源的访问安全。

系统中的准入控制功能，只对终端设备访问视频平台资源进行准入控制。终端访问其他系统资源平台时，不做任何准入控制，在保障视频平台资源访问安全的同时不会对员工的其他办公操作有任何影响。视频准入系统的IP地址需由管理员提前在控制台设置。

以旁路方式将服务器放置于网络核心交换机处，同时，在交换机（一般是核心交换机处，具体位置根据网络拓扑灵活确定）处进行端口镜像的设置，将终端电脑访问服务器的请求数据镜像至服务器，服务器对镜像数据进行处理，判断终端合法性，合法则放行不予处理，不合法则使用内网安全技术对终端按照相应规则进行引导处理。

* 非法终端（未安装专用客户端的电脑）禁止访问视频平台系统。非法终端企图访问视频系统时，准入控制功能自动将其访问界面做重定向跳转至“被准入”提示页面。
* 非法终端电脑可自由访问服务器A、网站B、系统C…等网络资源，不受准入功能模块控制。
* 管理员可在控制台增加终端电脑白名单IP地址，白名单地址内的电脑设备可不受准入功能控制。在未安装客户端的前提下自由访问视频系统资源。
* 安装有客户端的电脑可自由访问视频系统资源，不受准入控制。

该安全阻断技术不依赖于网络设备，对网络设备无要求，同时具备部署快速、不会对网络延时造成影响及设备逃生等优势。

### 1.2.2本地视频数据防拍照

终端设备完成用户合法性校验后，便可正常访问视频管理系统的数据资源，包括视频数据的查看、播放、下载等操作。为避免终端用户通过手机拍照录屏的方式将视频数据非法外流造成泄密事件的发生，系统为用户提供屏幕水印解决方案。终端用户通过拍照、录屏等方式将视频数据非法外发后，单位信息安全人员可依据水印内容对外泄数据及当事人进行快速的溯源、定位及追责处理。同时屏幕水印可对潜在的企图将视频数据外泄的人员起到很好的威慑作用。

终端用户打开客户端登录系统后，会自动在系统桌面内展示水印内容，关闭客户端后屏幕水印自动消失。

水印展示内容包括：当前登录用户所属部门名称、当前登录用户真实性、当前登录设备计算机名称、当前时间、管理员自定义水印内容、当前登录设备ip地址和MAC地址等。

系统支持显式水印及隐式水印两种屏幕水印展示方式。

**显式水印**：在本地电脑屏幕上显示传统数字水印，用户可肉眼识别水印中包含的内容信息。

 **隐式水印**：在整个电脑屏幕覆盖一层包含计算机信息的5\*5点阵列图案。非法人员通过对视频屏幕拍照或录像时，所得信息会包含点阵水印图案，系统可依据点阵图案信息在数据库中进行相应的查询，获得该视频流转的详细信息，包括用户所属部门名称、用户真实姓名、本地计算机名称、终端时间、管理员自定义水印内容、本地计算机ip地址和MAC地址等。

和显式水印相比，隐式水印可最大程度降低屏幕水印对视频查看者的视觉刺激，同时又兼具显式水印的视频追溯、定位及事件追责的作用。点阵水印颜色可依据单位视频一般内容场景进行灵活调整，确保隐式水印的水印效果。对于隐式水印的解码系统提供了手动识别和自动识别两种方式，手动识别比较繁琐，自动识别方便快捷，但是对隐式水印的清晰度要求比较严格。

### 1.2.3视频数据本地存储安全

提供虚拟安全磁盘存储空间，保障终端用户下载至本地视频数据的安全。通过文件重定向技术，把视频管理平台下载的数据强制重定向到虚拟安全磁盘中，保证涉密数据无法通过任何非法方式导出至虚拟安全磁盘外。能够将虚拟安全磁盘内的视频数据与终端电脑上的其他数据完全隔离，从数据根源出发保证了数据安全性。在实际使用过程中，严格控制数据出口，进而实现对视频数据的全方位安全防护。视频数据的生成、存储、访问、销毁完成整个生命流程均在虚拟安全磁盘中，从数据的根源对数据进行安全防护。

使用强加密技术对虚拟安全磁盘存储空间进行加密处理，确保保存有视频数据的磁盘在非法终端无法读取，保障视频数据的安全。虚拟安全磁盘技术在保障下载至本地视频数据安全的同时，不对视频数据文件本身做任何加密处理，不会对视频文件造成任何损坏，且对视频数据的打开播放速度几乎无任何影响。

对于需要对外交互的视频数据，可为用户提供灵活可控的文件外发及导出审批流程，保障对外交互数据的合法性及安全性。

### 1.2.4视频数据对外交互安全

在视频数据使用过程中，用户需要将部分视频数据外发至本单位以外的人员，为防止视频数据在对外交互过程中二次泄密事件的发生，系统为用户提供基于视频数据使用权限控制的视频数据外发解决方案。

* 外发视频使用权限控制

管理员可在控制台为每位终端用户设置视频数据外发权限控制的基线，终端用户可在该基线基础上对外发的数据设置一定的使用权限控制。例如，管理员设置的视频数据外发打开的次数是3次，此时终端用户在设置外发视频数据的最大打开次数时，该次数值只能够小于或等于3。

外发视频数据可设置的使用权限控制包括：是否允许截屏、使用次数、有效使用时间、使用外发视频数据时进行密码认证等。同时可针对企业实际需求，设置文件外发的审批流程。通过设置单级审批、多级审批及会签审批等灵活多种的审批流程，保证重要文件外发的正确性及合法性。视频数据外发使用权限控制可在保障视频数据对外办公交互的基础上，杜绝二次泄密事件的发生。

* 外发视频屏幕水印展示

视频数据外发操作权限控制的基础上，系统同时提供外发视频屏幕水印展示，可对屏幕拍摄及录像行为进行溯源、定位和追责处理。水印内容包括：视频数据外发人员所属部门名称、视频数据外发人员真实性、外发视频数据设备的计算机名称、文件外发时间、管理员自定义水印内容、外发视频数据设备ip地址和MAC地址等。同样外发视频屏幕水印支持显式水印及隐式水印两种水印展示方式。

### 1.2.5视频数据导出安全

视频数据外发功能可有效的杜绝对外交互视频数据二次泄密事件的发生，但是在很多的对外交互使用场景中并不适合使用视频数据外发功能对外发的视频数据进行使用权限的安全管控，而是需要将视频数据直接导出进行对外交互。直接将视频导出进行对外交互的方式使得视频导出单位人员无法对视频进行有效的使用权限控制，极易造成二次泄密事件的发生。

系统可对导出的视频数据进行视频水印处理，即直接将水印内容写进视频数据本身。一旦对外交互视频发生二次泄密事件，管理员可依据视频水印对该视频及当事人进行快速的溯源、定位及追责处理。同时可针对单位的实际需求，设置视频数据导出的审批流程，通过设置单级审批、多级审批及会签审批等灵活多种的审批流程，保证重要视频数据外发的正确性及合法性。

和视频外发中的屏幕水印一样，导出的视频数据水印同样支持显式水印显示和隐式水印显示，视频所包含内容信息字段均保持一致。导出视频水印和外发屏幕水印的区别在于，导出视频水印直接写在了被导出的视频数据里面和视频数据融为一体，外发屏幕水印则只是在屏幕上显示，水印并未写入视频数据本身。

### 1.2.6流程化审批管理

系统对导出及外发视频数据操作均可设置灵活的审批流程，经相关领导或系统管理员审批通过后方可把视频数据顺利移出至虚拟化安全磁盘外进行对外交互。审批流程可支持单级审批、多级审批及会签审批。

单级审批：仅有一个审批员，该审批员同意后方可外发或导出视频数据。

多级审批：拥有多个审批员执行多个审批级别。如申请提交后，先由负责科长审批、科长审批通过后，系统自动将审批流程发送至处长进行审批，依次类推。其中任何一个审批环节未完成或被拒绝，均不进行下一级别审批。

会签审批：申请提交后，申请单会同时发送至所有的审批人处进行审批操作。当多数人或所有人审批通过后方可将视频数据进行外发或导出。

灵活的审批流程设置，可满足多种复杂的用户使用场景。

为最大程度节约服务器系统存储空间及网络资源，同时如实向审批人传输被审批视频数据的内容，系统会对被外发或导出的视频数据进行“帧截取”处理，即有规律的截取视频数据图片传输至审批人处，不再传输整个视频文件。

### 1.2.7数据图表分析

完备的日志审计记录是每一个数据安全类软件必备的功能模块，系统为视频数据导出及外发操作提供详尽的日志记录及报表分析功能。所有视频数据在外发或导出时，系统会自动将相应的操作时间、操作人、操作人所属部门、审批人、视频数据信息、执行操作的计算机ip和MAC信息等保做详尽的记录，便于事后可能的追责处理。

为最大程度节约服务器系统存储空间及网络资源，同时如实记录被导出或外发视频数据的内容，系统会对被外发或导出的视频数据进行“帧截取”处理，即有规律的截取视频数据图片上传至服务器系统作为视频数据审计信息。

系统为管理员提供强大的视频数据外发及导出统计报表功能，如一定时间内导出或外发数据人员排行榜，一定时间内导出或外发数据量趋势，多种报表形式可有效的协助管理员快速对可能的安全风险进行预知、发现，保障视频数据安全。

# 方案优势

## 资产探测，精准管理

主动网络协议探测+被动协议分析式两种探测方式，对网络内的设备进行设备信息收集，具有品牌适应性好，准确率高的特点。采用SNMP协议及ICMP、ARP等协议，对网络中的IP设备进行主动式探测，对网内设备IP、MAC、在线情况进行收集，并通过SPAN技术对通过汇聚设备的网络数据进行协议分析，从中收集活动设备的实时信息。通过主被动相结合的探测技术，对网内设备的变化及违规情况进行实时监测，从而达到实时管控的目的。

## 严格把控边界，杜绝滥用违规等行为

对终端的入网管理，阻止非法移动终端任意接入网络。准入控制技术不依赖任何交换机等网络设备，不会改变用户网络拓扑架构，可满足各种复杂网络、混合型部署网络和纵级大型网络的准入管理要求。准入服务实时同步网络探测、设备识别模块中的数据对入侵、伪冒终端进行阻断，提升网络准入工作效率，保障接入网络安全性。

## 可视化运维管理，为处置提供决策

系统提供了网络拓扑图自动绘制功能，能够对全网拓扑进行展示。在拓扑图上可以全面展示网络中的网络设备、安全设备、服务器系统、网络连接等信息，整体上让用户实时了解网络的运行情况。TSA系统实时监测接入设备的运行状况，包括设备类型、IP地址、MAC地址、更新时间、地理位置、厂家等信息，并可分析在线率、全网安全指数、报警信息、弱口令占比、IP地址使用率等，让用户从全局的角度去掌控网络状况。

## 全方位、多视角的风险预警

系统从多个视角深刻反映网络的整体安全状况，提供“历史数据搜索”与任意扫描任务之间的“汇总查看”和“对比分析”功能。不仅对单个扫描任务的漏洞分布、危害等进行了统计分析，还对多个扫描过程进行综合的风险变化和安全对比评定，为您网络安全状况的评定和未来网络建设提供了强有力的决策支持。

## 监控数据全生命周期管控

监控数据自产出到删除都由系统进行隔离防护，提供环境生态的全周期控制以及对文件使用、导出、外发等行为的全实时审计，严格控制数据使用的恶意行为，针对数据导出的场景，提供对外数据使用的权限设定，有效的杜绝对外交互视频数据二次泄密事件的发生。

系统专注于视频数据自存储访问到使用的整个生命周期的安全性，具备极简的操作界面且对视频数据安全防护更具针对性。

* 产品设计具备极强的兼容性，可兼容几乎所有的的视频管理平台，对于个别不兼容系统可进行快速的适配处理。
* 基于虚拟磁盘安全防护技术理念，在保障本地视频数据安全的同时，对下载至本地的视频数据使用几乎没有任何影响，包括视频的播放质量及速度等。
* 集成金盾软件自主研发的NACP准入控制系统，可在网络资源访问控制层面保障视频数据存储系统的访问安全。
* 显式水印和隐式水印设计方案，更能够满足用户复杂的视频数据溯源处理环境，同时隐式水印能够最大限度降低水印对使用者的视觉刺激。
* 大屏水印解决方案，在防护终端视频泄密风险的同时，满足客户大屏视频泄密防护的需求。
* 对直接导出的视频写入水印信息，可进行有效的溯源处理，同时对企图泄密视频数据的人员进行有效的威慑。
* 视频数据外发解决方案，通过设置对外交互视频的使用权限控制，杜绝二次泄密事件的发生。
* 在客户端在设计上充分考虑到了终端用户的使用习惯，力图使用最简的界面设计向用户展现足够的操作信息，降低用户的学习成本。
* 水印策略的灵活控制。对实时的视频添加水印，水印支持位置、颜色和透明度等等参数，视频浏览下载端无感知，不影响视频质量和访问速度。

# 设备选型

|  |  |  |  |
| --- | --- | --- | --- |
| **产品型号** | **主要硬件参数描述** | **数量（台）** | **价格（元）** |
| GD-DBHY50 | 5台电脑终端视频数据防泄密硬件平台，1U专业服务器，硬件服务器采用专用嵌入式安全操作系统；最大吞吐量：≥6Gbps，最大并发连接数：120万（条）；标配6个千兆电口，具有1个扩展槽位，支持4个端口千兆光纤扩展卡或4个万兆光口扩展卡。 | 1 | x |