TP-LINK
私接摄像头识别解决方案

项目咨询

数字化浪潮下，网络摄像头统一接入组织网络的趋势愈发明显，
如何管理这些网络设备，确保网络资源的安全流通，杜绝泄密与被入侵风险，成为亟待解决的现实问题。
TP-LINK 基于最新网络安全技术，结合下一代防火墙，安审一体机等产品推出私接摄像头识别解决方案，
确保授信终端始终能够安全稳定地访问组织的网络资源，
并杜绝任何非授信终端设备连接，同时做到审计合规，过程可追溯。

问题分析

私接现象层出不穷

随着监控摄像技术的发展，非法私接现象层出不穷，对受害方造成隐私和经济上双重侵犯。例如酒店场景中，房客私接摄像头，勒索酒店，使酒店经济与名誉受损。

问题终端定位不明

在接入设备数量较多的情况下，排查非授信终端耗时长、难度大，容易使问题终端定位不准确，导致告警不及时、不明显。

网络攻击愈发普遍

网络攻击门槛降低，攻击行为愈发普遍，没有完备的防护体系，无处不在的网络入侵会导致内部终端失陷，致使信息资源损失。

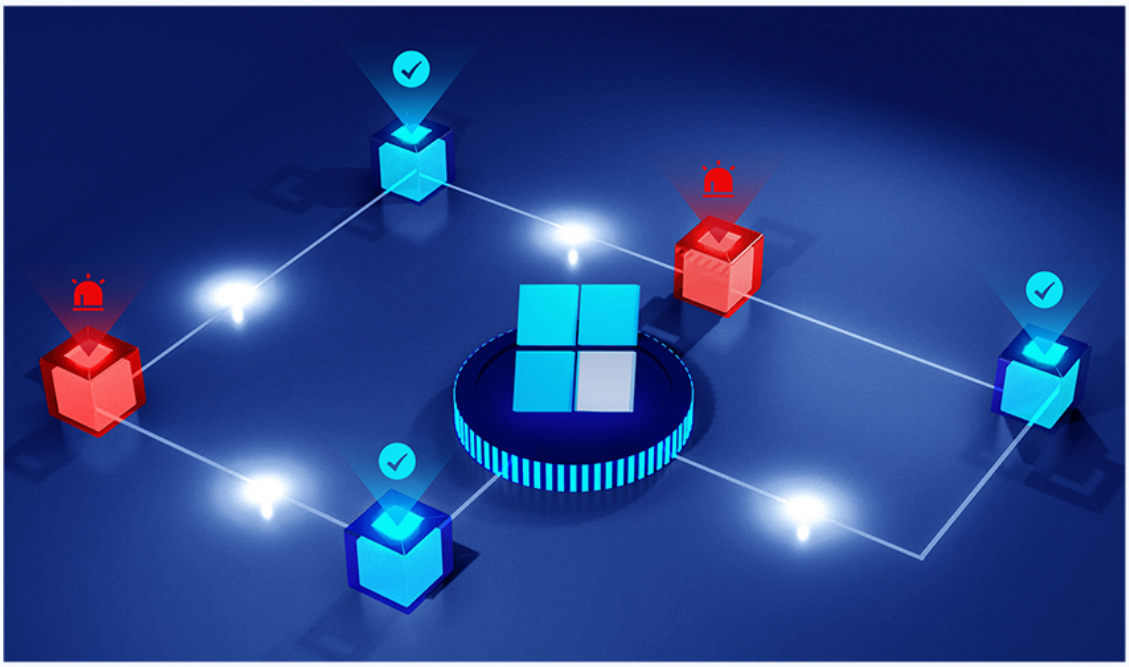
安全审计困难

私接摄像头偷拍产生的一系列隐私暴露、经济损失、安全侵犯问题难以回溯定责，令酒店、商场等陷入法律纠纷。

TP-LINK方案优势

精准防私接，阻断更灵活

准确识别并放行授信终端、临时接入的合法终端，比一般白名单更加灵活；
识别、阻断并告警私接设备*，避免损失。(*识别准确率随模型改善而不断提升)

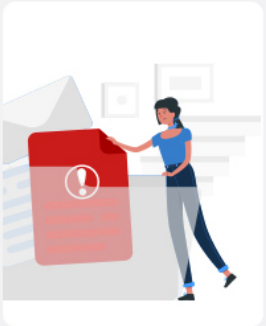


自动告警，明确通知，快速定位

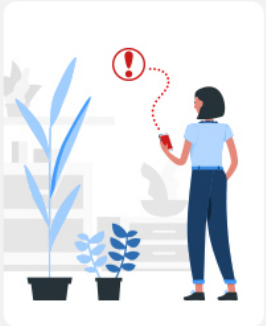
全面盘点网络资产，一旦检测到私接终端，提供多种告警方式，支持外接报警器；
能够准确定位私接终端位置*，帮助快速排查风险隐患。

*能够指示网络位置与物理位置，有关功能需要进行提前配置

外接告警器



邮件告警



短信告警*

*部分功能后续软件升级支持

下一代安全防护

方案兼具下一代防火墙防御能力，支持DPI深度探测流量报文，检测与抵御网络入侵，
并配备TP-LINK专属视频攻击特征库，全方位保护网络安全。

云边协防，功能扩展*

TP-LINK 云安全 边界防御服务

云安全——边界防御

封禁攻击源，隔离失陷终端，阻断恶意文件

查看 >

TP-LINK 云安全 健康上网服务

云安全——健康上网

不良网站一键封禁，AI 云库自适应扩充

查看 >

TP-LINK 云安全 批量配置下发

云安全——批量配置下发

云端运维，配置下发，省时省力

* 部分软件功能后续升级支持

安全审计，极速回溯*

长周期大容量存储

内置 512GB 大容量固态硬盘，支持外接硬盘扩容，轻松满足 6 个月以上的长周期日志存储。

高速的日志处理

每秒可处理超千条审计日志，满足大型场景对网络审计分析的需求。

日志筛选功能优化

常规查询近 7 天的日志数据，无数量限制，高级搜索最高支持 30 天日志检索。

* 须搭配 TP-LINK 安审一体机使用

客户价值

网络资产盘点，
实时掌握设备在线状况
与位置信息。

检测并告警、
指示私接设备位置，
避免敲诈损失。

正常上网
终端畅行无阻，
免去频繁配置白名单。

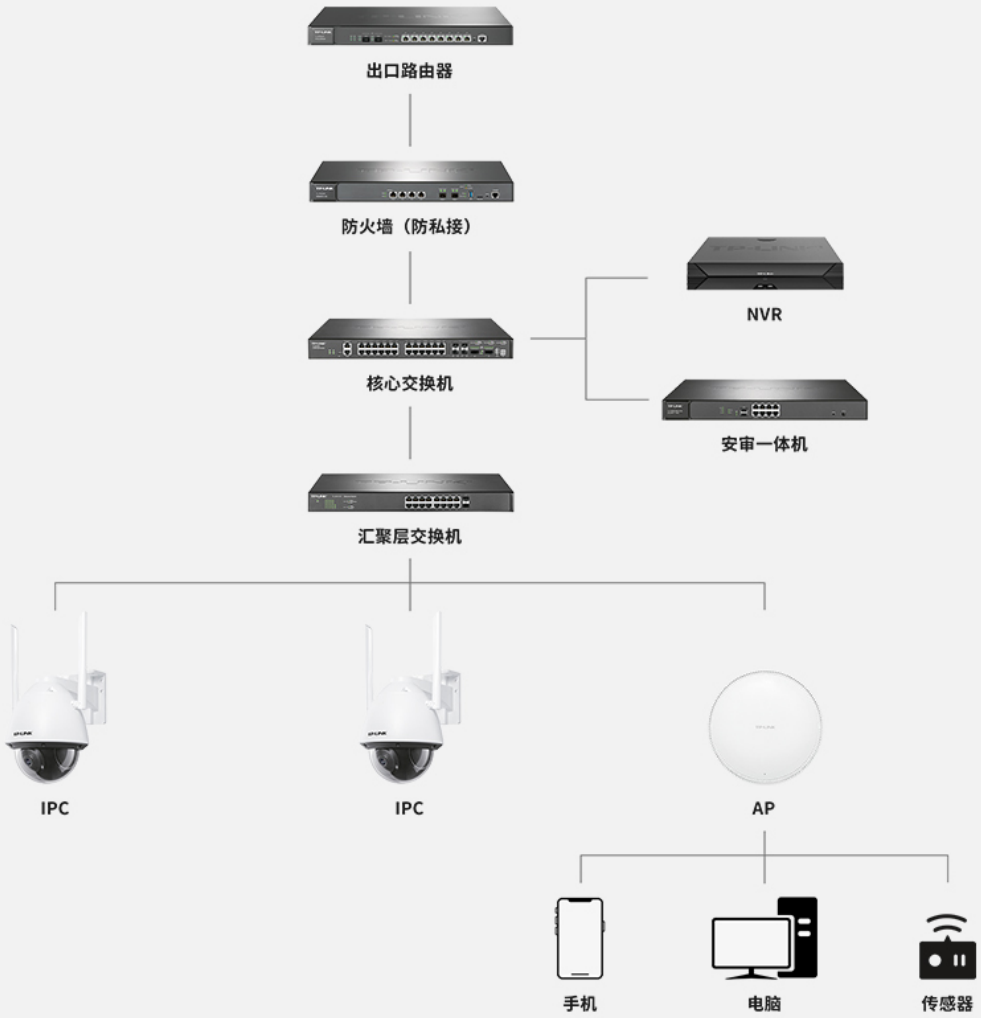
灵活部署，利旧无忧；
云端管理，运维便利。

下一代防护，
保障业务稳定运行

TP-LINK私接摄像头识别一体化方案

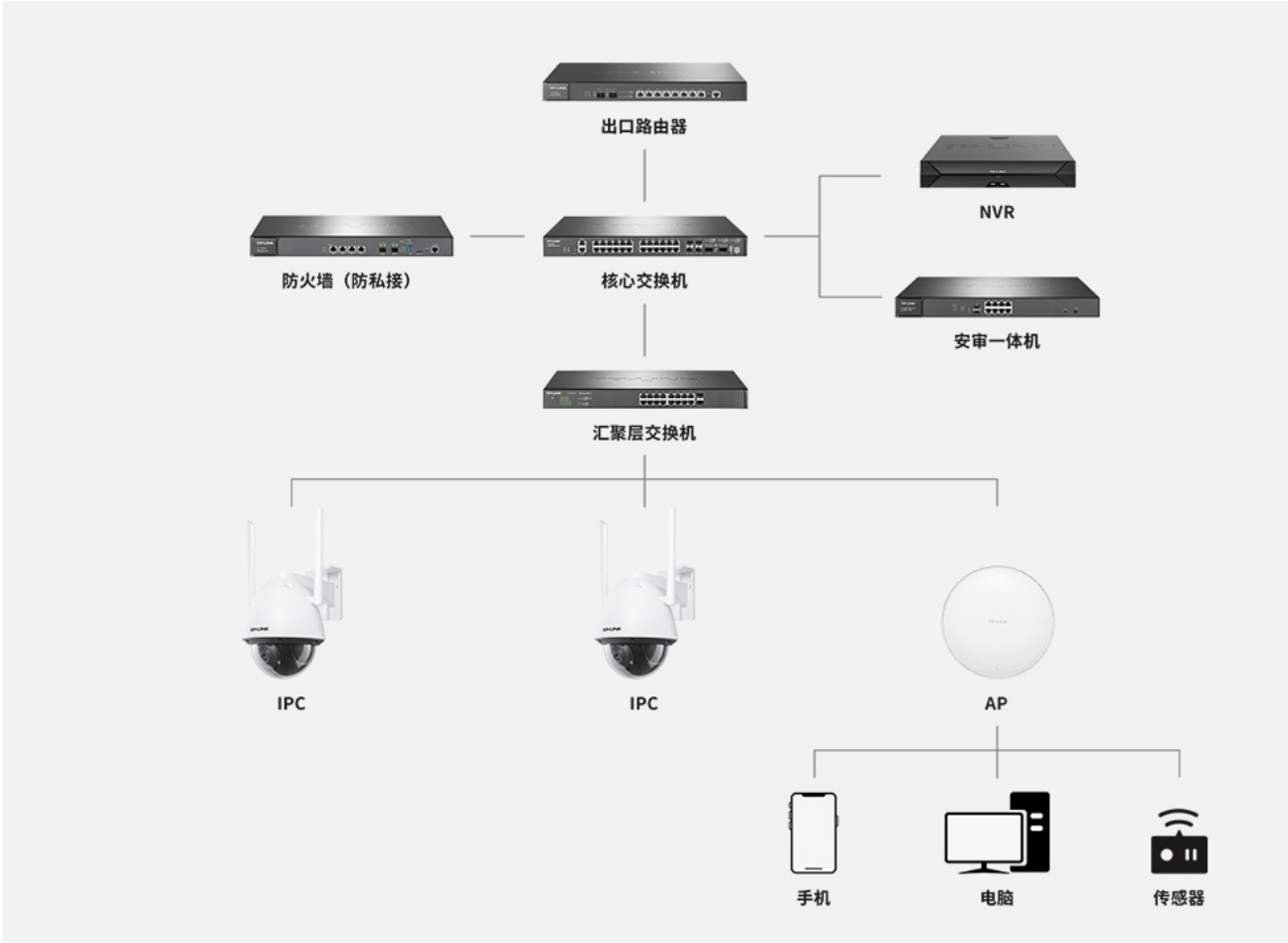
直连管控

管控网络出口，全面盘点网络资产，实时检测并阻断私接IPC，并能够抵御网络攻击。



旁挂监控

旁挂监控网络出口流量，不改变原有网络拓扑，利旧无忧，全面盘点网络资产，实时检测并告警私接IPC。



典型场景