

精析高校全域流量·智能AI助力安全运营

—— 高校网络安全沙龙活动

南京中新赛克科技有限责任公司

政策驱动：安全成为教育数字化的“压舱石”



《中华人民共和国网络安全法》（2026修订）

- 新增人工智能安全治理条款，强化算法安全监管。
- 明确数据全生命周期管理要求，强化个人信息保护责任。
- 网安法：日志留存不少于6个月
- 数安法/个保法：明确数据处理的安全保障义务，合规审计是底线要求。

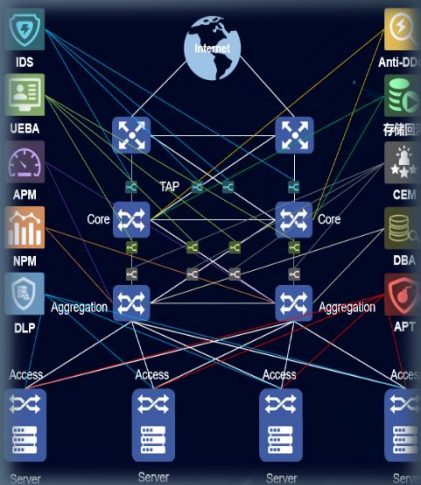
教育部等九部门《关于加快推进教育数字化的意见》

- 明确提出“筑牢教育数字化安全屏障”的核心目标。
- 重点强化核心业务数据与重要个人信息的防篡改、防泄露能力。
- 《推进教育新型基础设施建设指导意见》明确要求：需加强校园网络运行监测与态势感知能力，实现全网可视。

《教育强国建设规划纲要(2024-2035年)》

- 将网络安全能力建设纳入教育强国战略的重要组成部分。
- 要求提升关键信息基础设施保障水平，构建主动防御体系。
- 江苏省《“十四五”教育信息化专项规划》提出：2025年实现100%中小学建成网络监测平台，确保关键业务流量可视、可管、可控。

现状困境：高校网络安全运营的共性痛点



海量用户下的 “复杂网络流量”

端口资源枯竭

传统镜像端口有限，难以实现全网流量的全面覆盖与采集。

交换机性能过载

SPAN流量占用CPU，高峰期丢包严重，导致数据严重失真。

复杂流量适配不足

面对高校多样化业务的复杂流量模型，传统方案无法针对性适配，加密流量威胁难以有效识别。

数据孤岛严重

各安全设备独立运行，日志无法关联，难以进行全局溯源分析。



告警风暴下的 “失焦”与“疲劳”

告警数量爆炸

日均告警量高达数万条，安全团队陷入海量信息处理的疲态。

告警质量低下

误报率超过90%，大量无效信息淹没了真正的安全威胁信号。

安全运维过程慢

安全设备孤立，需要人工手动对单台安全设备进行运维，跨设备协同分析处置困难。

人工处置被动

平均响应时间超12小时，完全无法满足高强度攻防对抗的需求。

现状困境：高校网络安全运营的共性痛点



非法VPN滥用、加密协议隐蔽、黑灰产数据窃密等网络风险及异常上网行为

校园翻墙行为频频发生



违反法规

学生通过技术手段绕过校园网安全策略，私自访问境外非法网站。违反网安法及教育行业相关管理条例，属于明令禁止的违规行为。



信息泄露

境外非法站点多潜伏钓鱼链接与恶意程序，极易导致个人隐私或学校敏感数据被窃取。

校方法律风险的“压力”与“困境”



法律责任

学校作为网络运营主体，若因监管不力导致安全事件，需承担相应的行政与法律连带责任。



安全隐患

翻墙行为打破了校园网边界防护，可能成为黑客入侵的跳板，直接威胁内网服务器安全。

安全智慧校园建设的必然要求



教学场景多元化

在线授课、虚拟仿真实验等应用普及，对网络带宽、低时延和高稳定性提出了更高的承载要求。



AI攻击指数增长，传统模式失效

指数级AI攻击带来了“网络攻击”的指数级增长，传统人工研判的运营模式，在AI攻击面前捉襟见肘。迫切需要实现攻防对等



终端设备爆发式增长

PC、平板、IoT设备等大量接入校园网，网络终端数量倍增，导致整体流量呈指数级爆发式增长。



筑牢安全防线，消除监测盲区

建立全网可视化的威胁监测体系，消除安全死角，全方位守护师生敏感信息与校园数据资产安全。



数据资产安全防护

网络承载海量师生个人信息、科研数据等高价值资产，数据泄露风险加剧，安全防护刻不容缓。

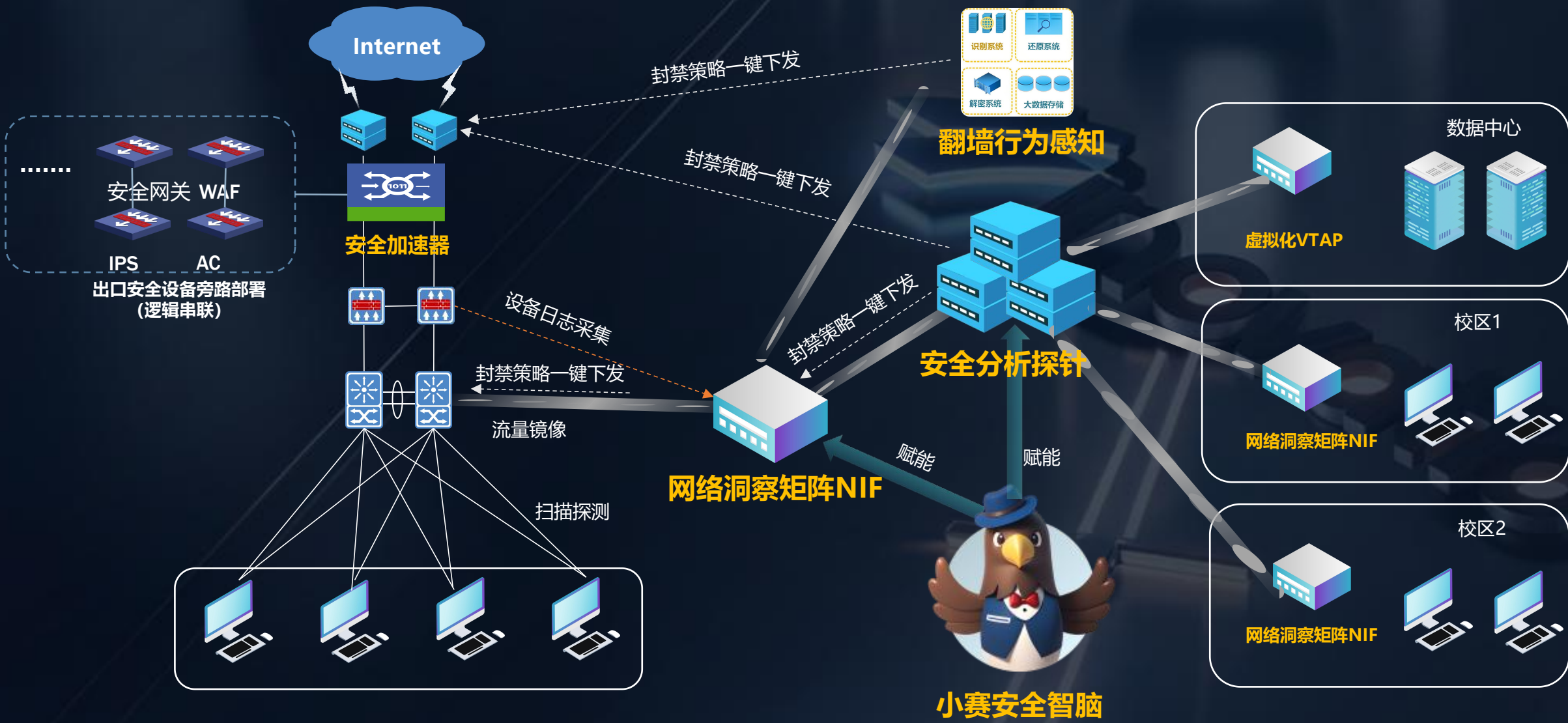


落实合规要求，规避法律风险

严格对标《网络安全法》、数据安全法等法律法规要求，补齐技术短板，确保完全符合监管合规标准。

结论：实现流量全面可视、精准管控与安全防护，是保障校园网络稳定运行的必然要求

网络可视化筑底，小赛安全智脑护航，共建高校数智安全新防线



场景分享一：校园多区域、网络流量统一采集



校园场景

校园出口面临宿舍网、校园网、数据中心等多区域巨大流量压力，师生终端多样导致网络行为复杂。HTTPS加密流量占比攀升，形成严重的安全监测盲区，并带来网络流量负担。

同时，高校需严格遵守网络安全法规，对全网行为进行合规审计，并有效识别隐藏在海量流量中的各类网络威胁。



解决方案

全流量镜像与智能分流

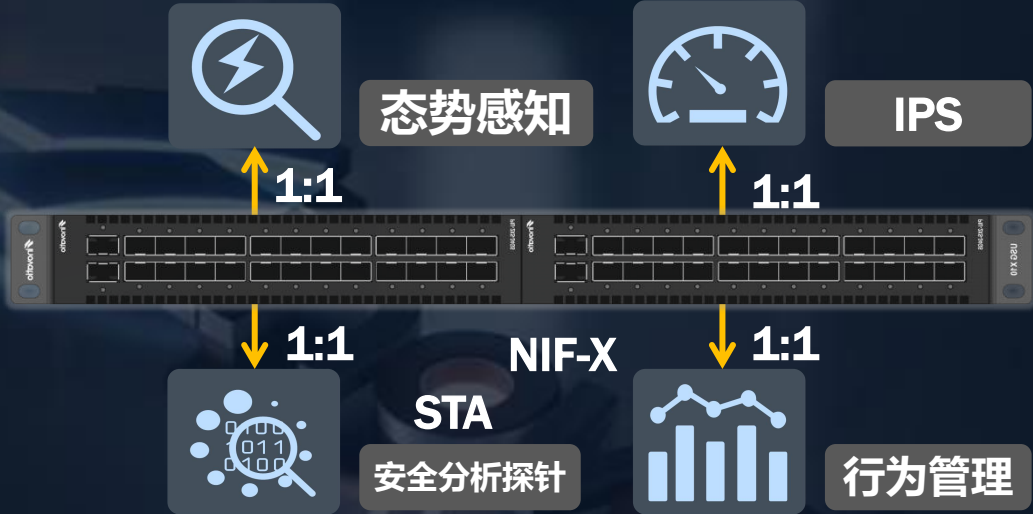
按需分发流量至IDS/IPS、态势感知等后端设备，提升利用率。

SSL/TLS 加密流量解密

提供高性能硬件解密能力，彻底消除加密流量带来的安全盲区。

深度协议解析与行为识别

精准识别HTTP/https、VPN、IoT等协议，快速发现网络异常行为。



消除安全盲区

确保全链路流量处于监控之下，无死角防范。

提升威胁检测

清洗提纯流量，大幅提升后端设备检测效率。

满足合规审计

提供完整访问记录，轻松满足等保合规要求。

精细化运维管理

洞察流量构成，支撑网络优化决策。

场景分享二：校园网络音视频流量监测剥离



场景挑战

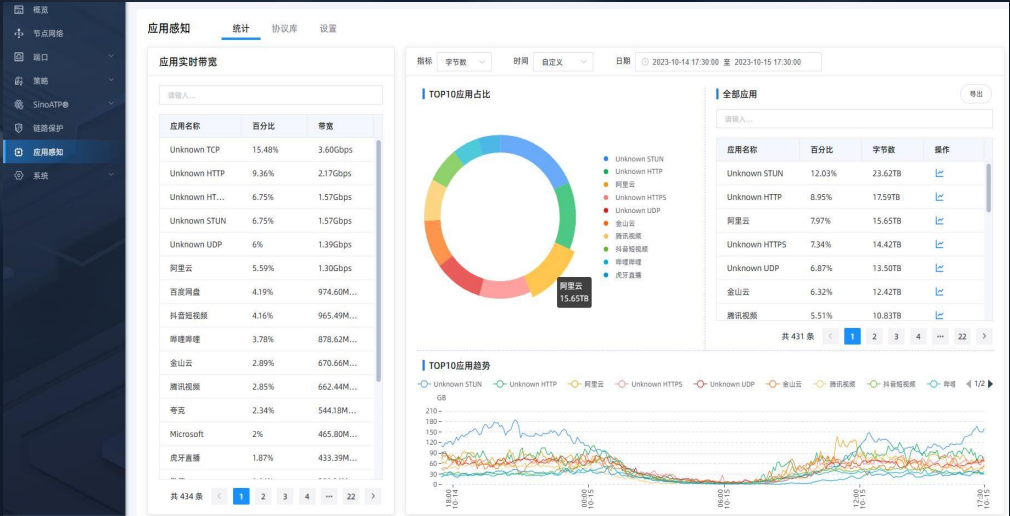
高校在线授课、虚拟仿真实验、视频会议等音视频业务流量占比极高，全量镜像转发给安全分析工具后，大量带宽与算力被低风险音视频数据占用，导致入侵检测、威胁分析等关键业务无法获得足够资源。无法按业务类型过滤流量，IDS/IPS、威胁分析平台被迫对海量音视频流量进行全量检测，误报率居高不下，安全团队陷入告警疲劳，无法聚焦真正的网络威胁。



解决方案

应用流量识别过滤

基于**应用层协议识别技术**，精准区分教学音视频（如在线授课、直播课堂、虚拟实验）与其他业务流量，支持按端口、协议、业务类型设置过滤规则，将低风险音视频流量直接分流或按需裁剪，避免其进入安全分析链路。对过滤后的流量进行定向分发，仅将安全分析工具需要的高价值流量（如未知协议流量、加密异常流量、跨区域访问流量）推送给 IDS/IPS、态势感知平台，实现“安全分析只处理有效流量”。



- ✓ **安全分析效率大幅提升**
安全工具的分析数据量可降低 40% 以上，运营效率显著提升。
- ✓ **节省成本**
无需为安全分析工具扩容处理音视频流量的算力与带宽，减少设备采购与扩容成本；
- ✓ **消除安全监测盲区**
通过精细化流量治理消除了安全监测盲区，实现教学业务体验与网络安全防护的双向兼顾。
- ✓ **适配高校复杂场景长期演进**
可扩展过滤与分发能力，能灵活适配业务变化，为后续安全分析平台的升级扩容预留充足空间。



场景挑战

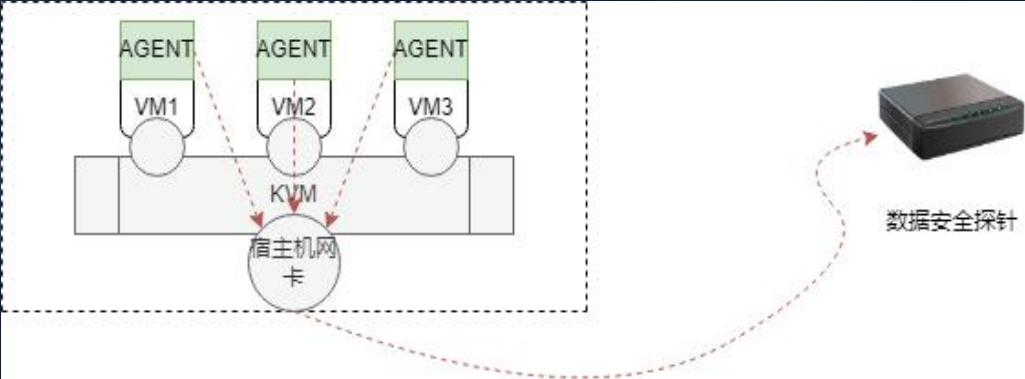
随着云计算的普及，高校虚拟化资源越来越多。部分云上业务数据报文无法获取，也无法进行监管和审计，这给师生隐私信息带来了安全隐患。



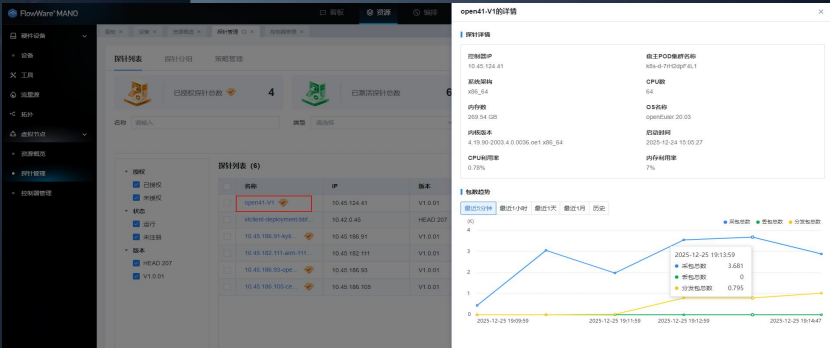
解决方案

虚拟探针技术

通过云主机/虚拟机上采集数据报文，将其进行封装后，发往我司的分流设备，由其将数据报文再按需发给网络安全设备，进行监管审计，解决这一安全隐患。



- ✓ **采集报文**：从虚机/容器中采集报文
- ✓ **预处理报文**：对报文进行截断/标识
- ✓ **筛选报文**：只采集需要的报文
- ✓ **转发报文**：将采集到的报文转发给USG设备
- ✓ **管理AGENT**：统一管理采集AGENT



场景分享四：校园网出口安全工具链弹性编排



场景挑战

传统“糖葫芦串”架构痛点

串联节点过多导致单点故障风险高；硬件堆叠扩容困难，运维管理复杂；加密流量层层解密造成严重的性能瓶颈。

亟需打破僵化的物理串联方式
部署安全设备



解决方案



逻辑化弹性编排

一次物理串联，流量按需调度，后端设备旁路接入。



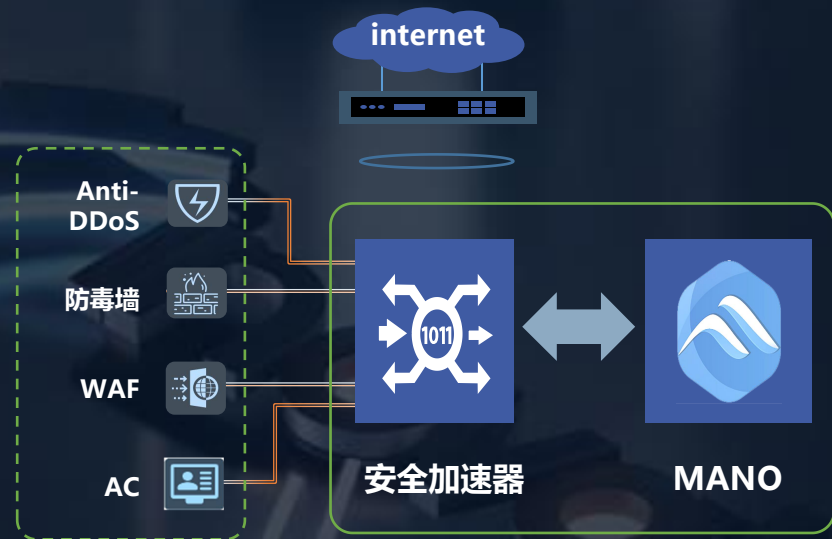
安全资源池化

异构设备统一纳管，实现“工具即插即用”的弹性扩展。



入站SSL集中卸载复用

一次解密多工具复用，消除重复解密带来的性能损耗。



- **提升出口网络可用性：**安全设备“由串改并”旁挂部署，形成安全资源池，流量转发路径与物理结构解耦，实现网络出口设备的逻辑串联，易于扩展；
- **提升出口网络可靠性：**支持安全工具健康检测，自动绕过故障工具，设备内置BYPASS确保网络永不中断；
- **流量优化筛选：**对互联网出口流量优化处理，过滤视频等无用流量，变相提升网络性能，音视频流量直通核心，入站流量解密，解决安全设备无法分析加密流量痛点。
- **优化资源利用率：**通过负载均衡与智能分流，延长老旧安全设备生命周期。

精析高校全域流量 · 智能AI助力安全运营

完整内容请咨询 400-100-8102,
或在官网填写咨询表单, 沟通获取完整方案。

南京中新赛克科技有限责任公司