筑牢数字金融基石

代码逻辑风险检测助力应用内生安全

方 芳 | 清科万道（北京）信息技术有限公司

业务安全事件案例-豆瓣“羊毛事件”

事件概述

事件时间

2026年3月2日凌晨

事件起因

运营失误将“满200减20”优惠券误设为“满200减200”，导致价格漏洞。

事件经过

漏洞迅速传播，大量用户涌入抢购，商品短时间内售罄。

事件结果

平台损失惨重，被迫自动退款并补偿，引发用户争议和品牌信任危机。

核心风控问题分析

发布缺少审核

未实现对活动配置的自动校验和审核流程业务逻辑的管控，导致异常配置直接上线。

优惠设置未设阈值

未实现对优惠力度的阈值校验业务逻辑，无法识别并拦截异常优惠配置。

使用无限制

未实现对优惠券使用场景、用户身份及次数的限制业务逻辑，导致漏洞被无差别利用。

批量下单无阻断

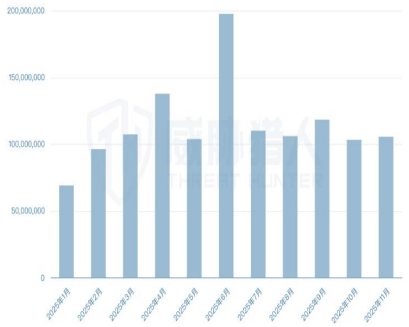
系统未在业务逻辑层面设计对异常批量下单行为的识别与拦截规则，导致恶意行为无法被有效识别和阻断。

风险趋势

- 2025年线上业务欺诈风险持续高企，相关攻击事件超**13亿条**。
- 2025年全年数据泄露事件共41644起，较2024年全年环比上升**10.83%**。
- 银行业数据泄露风险连续三年排行**第一**，消费金融行业则强势反超电商行业，跃升至**第二位**，软件应用行业首次登上**前10**。

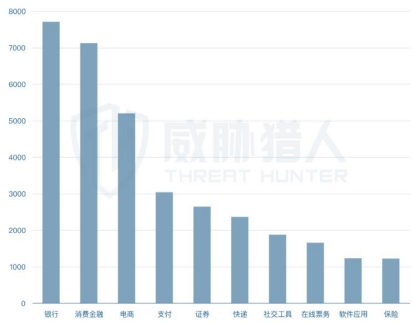
2025年业务欺诈攻击情报数

2025年1月至12月



数据泄露事件所属行业T0P10

2025年1月至12月



环境挑战

- !! 开放生态
- !! 业务多样性
- !! 应用攻击高发

能力挑战

- !! 专业人员配比不足
- !! 缺乏针对性检测工具
- !! 数据孤岛

数据来源：威胁猎人《2025年互联网黑灰产趋势年度总结报告》

监管趋势

2015年《国家安全法》

- 我国以法律的形式确定总体国家安全观的指导地位
- 国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，关键基础设施和重要领域信息系统及数据的安全可控

2017年《网络安全法》

- 第三十三条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

- 我国第一部系统性提出网络空间治理的法律法规
- 明确了个人信息保护方面的要求
- 规范了相关网络安全监管部门的责权范围
- 明确了个人信息保护相关主体的法律责任
- ……

2021年《数据安全法》

- 我国数据领域的基础性法律
- 建立国家级数据安全工作协调机制
- 建立数据分类分级保护制度
- 重要数据、重点保护、重点监管
- 明确数据安全评估、安全审查要求
- ……

2021年《个人信息保护法》

- 我国个人信息保护领域的基本法
- 明确个人信息处理的基本原则
- 明确了个人信息处理的合法性基础
- 明确了主体权利到处理者系列法律义务
- ……

中华人民共和国国家互联网信息办公室
Cyberspace Administration of China

《网络数据安全管理条例》

《网络安全审查办法》

《人脸识别技术应用安全管理办法》

《个人信息保护合规审计管理办法》

《数据安全管理办法》（征求意见稿）

……

中华人民共和国工业和信息化部
Ministry of Industry and Information Technology of the People's Republic of China

《网络产品安全漏洞管理规定》

《App违法违规收集使用个人信息行为认定方法》

《公共互联网网络安全威胁监测与处置办法》

……

中华人民共和国公安部
The Ministry of Public Security of the People's Republic of China

《网络安全审查办法》

关键信息基础设施安全保护条例（国务院令第745号）

关于印发《常见类型移动互联网应用程序必要个人信息范围规定》的通知

贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见

《GB / T22239-2019 信息安全技术 网络安全等级保护基本要求》

《GB / T28448-2019 信息安全技术 网络安全等级保护测评要求》

……

国家标准化管理委员会
standardization administration

《信息安全技术 个人信息去标识化指南》

《信息安全技术 个人信息安全规范》

《信息安全技术 个人信息安全影响评估指南》

《信息安全技术 数据安全能力成熟度模型》

《 数据管理能力成熟度评估模型》

《信息安全技术 数据库管理系统安全评估准则》

《信息安全技术 信息技术产品安全可控评价指标》

《信息安全技术 信息技术产品安全检测机构条件和行为准则》

……

技术趋势

安全漏洞趋势

传统安全运营模式中，安全介入相对滞后，多为事中、事后性处置，不论是风险影响和修复成本都较高

75 % 的安全漏洞已发生在应用程序层，而非我们以往认知的网络层

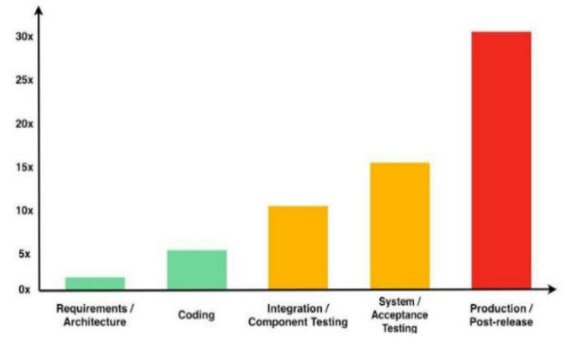
------Gartner Group

超过77% 的安全漏洞存在于代码应用上

------ NIST

安全左移的优势

搭建新型的研发安全体系，将“被动防御”转变为“主动防护”，将安全左移前置，从源头预防，势在必行



数据来源：美国国家标准与技术研究所（NIST）

图 2 研发运营各阶段代码漏洞修复成本

趋势

- 安全左移
- 化被动为主动
- 提高内生性安全

应用安全风险来源

应用安全缺陷的产生/引入主要源于AB两个层面

A

未能正确识别和实现所需的安全控制措施

被忽略（未实现）的安全控制

- **需求分析：**缺乏贴近业务场景的安全需求识别
- **设计：**缺少安全实现的设计考量
- **测试：**对安全控制的实现情况缺少有效验证

B

在编码实现系统功能的过程中，由于不良的编码习惯，引发了安全漏洞

不良的（错误的）编码习惯

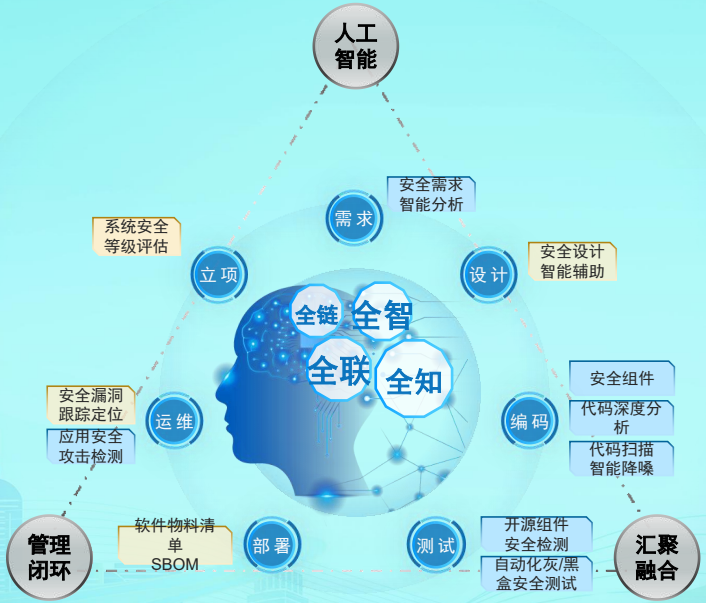
- 使用存在漏洞的开源组件
- 存在安全缺陷的外部组件
- 不安全的编码实现方式

针对第一类情况，应从需求分析入手，
实现安全需求的闭环管理，确保控制落实

针对第二种情况，则需从编码规范和
源代码管理入手，识别并修复漏洞

由于安全缺陷的产生原因不同，相应的，其管控机制也有所差异

构建应用安全智脑，为企业输送应用安全数字员工



一条链

集成多种安全开发工具，融入应用系统建设全生全周期，实现流程自动化管理

一套账

打破项目级管理，形成系统级台账，全覆盖，细粒度，全面掌握应用系统情况

一组图

安全能力建设全景图，知过去，懂现在，看未来

1个平台，2大特色引擎，多维数据融合

清科万道创新推出代码级业务逻辑漏洞检测、API资产检测两大特色引擎，具有非侵入，速度快，效率高，识别准的特点，在原有代码及开源代码检测的基础上，进一步实现了对业务逻辑漏洞的分析能力，更加全面地识别安全风险，补齐原有工具不足；还能快速识别应用API，为网络资产管理、受攻击面控制提供基础。同时，该平台还支持与原有代码扫描工具集成、与其它安全工具联动，打通多源数据，有效辅助提升应用系统内生安全保障能力。

检测漏洞类型

逻辑漏洞

◆ 由于程序逻辑不严谨，使得应有的控制缺失，或在特定情况下失效

- 交易欺诈
- 批量注册
- 控制绕过
- 暴力破解
- 短信轰炸
- 信息篡改
- 信息泄露
- 控制不足
- 文件上传
- 文件下载
- 并发重放

垂直越权

◆ 指低权限用户绕过系统的权限控制机制，行使高权限的功能或权限

- 提权
- 信息泄露

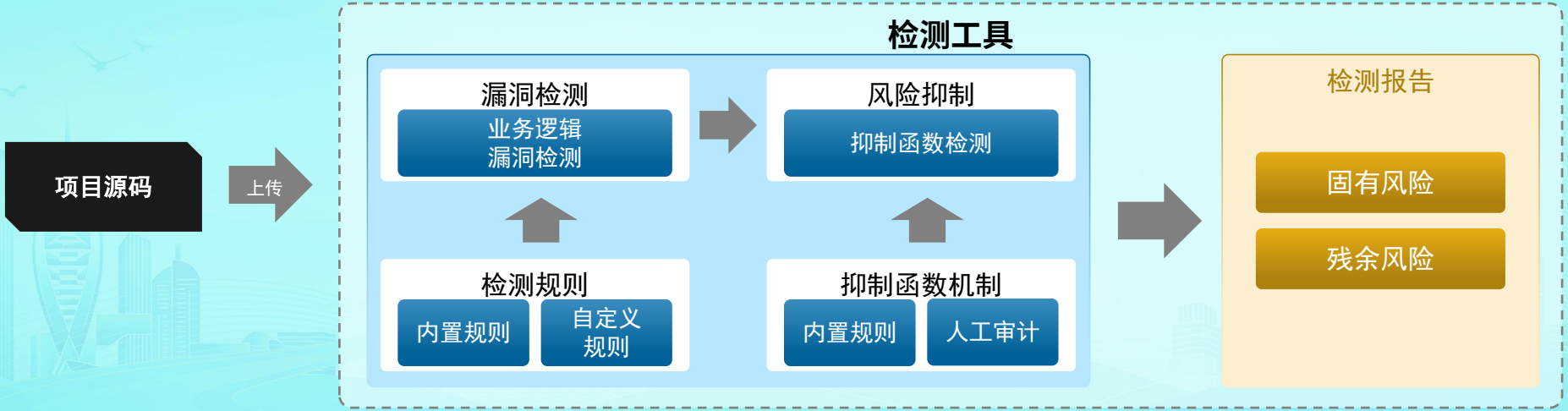
水平越权

◆ 指在同级别权限内，访问、操作或篡改其它用户的资源或数据

- 提权
- 越权操作
- 信息篡改
- 信息泄露

特色功能介绍-业务逻辑漏洞检测

- 有别于目前静态代码检测主要关注于常规的语法类代码缺陷，我们的工具提供更加贴合企业业务的检测引擎，针对常见的越权、资源消耗等业务逻辑漏洞进行识别。
- 配套提供现场服务，可针对企业业务场景进行分析，定制化针对企业业务特点的扫描规则，更加精准地识别个性化风险。
- 工具提供审计功能，能够通过审计反馈数据，优化扫描规则，持续提高检测的准确率。

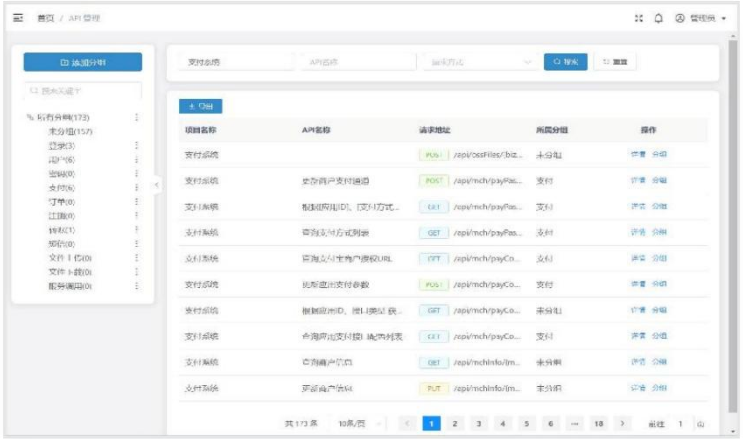


特色功能介绍- API资产识别及安全分析

- 通过对源代码的扫描实现对API资产的识别，无需插桩，无侵入性，不依赖流量，快速高效。
- 支持与开发环境集成，持续扫描版本迭代，跟踪API资产变更，动态跟踪掌握API资产情况。
- 支持与其它流量类工具对接，通过融合开发、测试与运维各阶段的多态数据，实现API安全管理左移，形成安全管理闭环，有效识别当前应用风险API，进一步提升对API资产的管理能力。

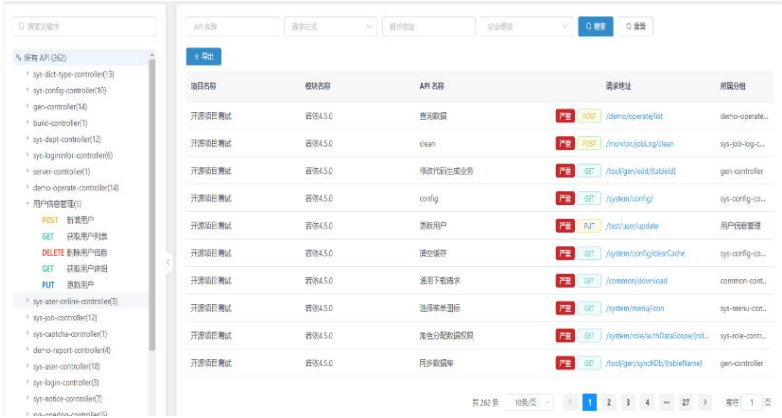
API资产识别与分类分级

- 有效识别应用系统中的API接口；
- 自动提取API详细信息，辅助API资产管理；



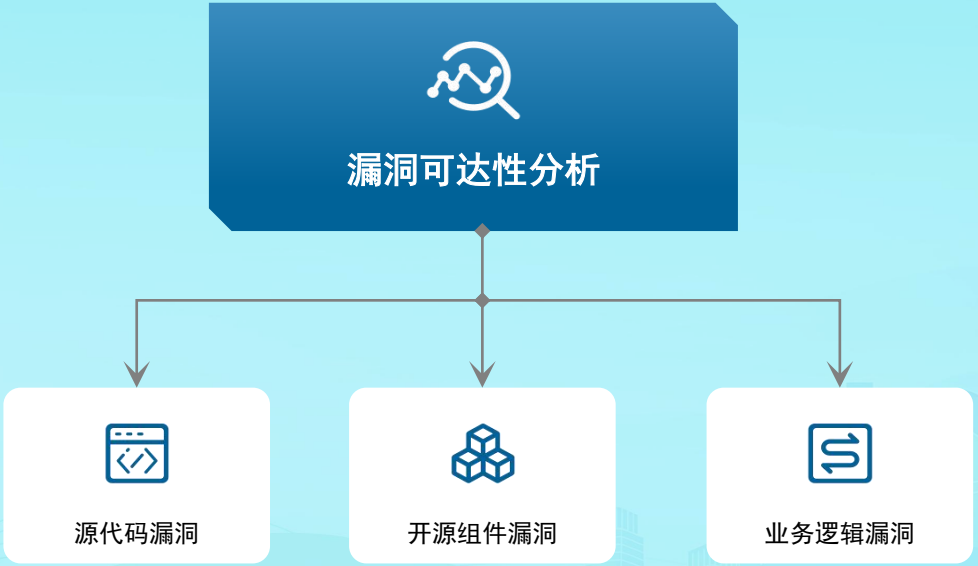
API风险标识

统一安全视图，综合安全编码、业务逻辑漏洞、开源组件等多引引擎检测结果，对API中存在的各类型风险进行标识和汇总分析



特色功能介绍-漏洞可触达性分析

通过对代码语法树的构建和分析，对于代码中的调用和依赖关系进行分析，进而识别所发现漏洞的可触达性（或可利用性），更有效地定位安全漏洞、指导有效控制。



工具应用

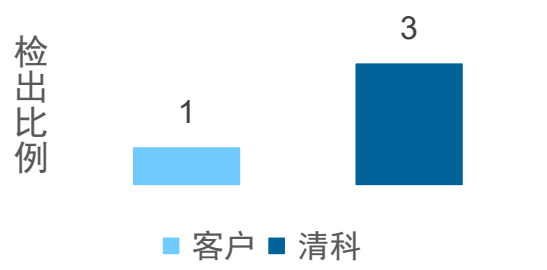
多引擎代码安全检测工具可跨岗位赋能，为安全工程师、开发人员、测试人员、运维人员等提供全方位的安全辅助。

职位	场景	功能价值
安全/渗透测试人员	安全性测试	➢ 全面识别风险API及风险触发条件，为渗透测试提供目标信息和攻击参数，极大提升测试效率及覆盖率 ➢ 针对发现的单一漏洞，可使用工具实现对全量应用的快速检测，避免同类漏洞反复发生
开发人员/开发安全员	编码漏洞发现与修复	➢ 借助API资产识别功能，快速全面盘点API资产情况，建立动态更新的API资产库 ➢ 提示API中存在的编码漏洞、业务逻辑风险、不安全的组件等，用于辅助网络受攻击面管理、威胁监测等
安全运营人员	护网/网络攻防	➢ 业务逻辑、白盒、开源组件三大扫描引擎与DevOps进行整合，在编码过程中持续扫描发现安全漏洞，并跟踪检测漏洞修复情况，避免带病上线

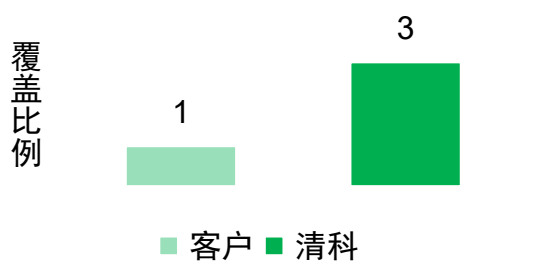
工具实际检测效果汇总对比分析

检测效果对比分析

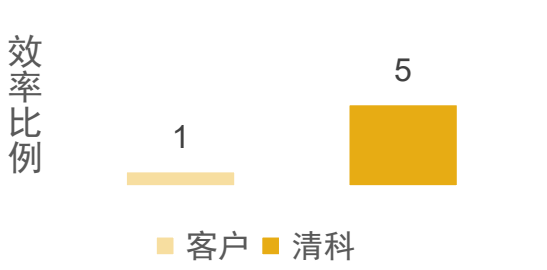
检出率



覆盖率



效率



*注：以上数据是由多家金融机构实际测试数据结果综合统计得出，检出率与覆盖率均提升200%，工作效率提升400%。

每比特都超值

视觉无损压缩，降体积不降画质

数字时代的信息困境

存储成本高企

高清音视频数据量指数级增长，导致存储硬件投入持续攀升，陷入“越存越贵”的恶性循环。

带宽资源紧张

海量视频传输占用大量网络带宽，造成实时监控卡顿、远程访问缓慢，严重影响业务协同效率。

传统压缩方案失效

传统技术难以平衡“高压缩比”与“高保真度”，且存在软硬件兼容问题，无法从根本上解决存储传输困境。

金融领域资料存储监管要求

银行业金融机构

银监办发〔2017〕110号

一般保存期限

至少保留至产品终止或合同解除后**6个月**

纠纷特殊规定

若发生纠纷，需延长**保存至纠纷最终解决后**

保险销售行为

保监发〔2017〕54号

分级保存要求

保险期**≤1年存5年**

保险期 **>1年存10年**

纠纷特殊规定

涉及纠纷时，**至少保存至纠纷结束后2年**

证券期货适当性

证监会令第130号 / 177号

核心保存范围

匹配方案、告知警示、录音录像、自查报告等

长期合规要求

保存期限不少于20年，需妥善保管接受检查

解决思路与原理：影像冗余与压缩方案

影像文件中的信息冗余

空间冗余 (Spatial Redundancy)
基于离散像素采样，未能充分利用相邻像素间的空间相关性。

时间冗余 (Temporal Redundancy)
相邻帧图像间的高度相似性，导致数据在时间轴上的重复存储。

视觉冗余 (Visual Redundancy)
人眼对色度、亮度的感知敏感度有限，大量信息无法被视觉感知。

信息熵冗余 (Entropy Redundancy)
用于表达某一信息所需的比特数总是大于理论最小值，存在编码浪费。

核心解决方案

视觉无损压缩 (Visual Lossless)

原理： 剔除人眼不可视范围内的信息，保留主观视觉效果。
特点： 不改变原始文件格式，保证无感知损失。

信息密度增强 (Density Enhancement)

原理： 提取时空冗余信息，采用更集约化的方式进行存储。
特点： 改变原始文件格式，显著减少存储空间占用。

一体化视频压缩解决方案

存量解决方案：历史数据优化

适用场景：

针对海量历史数据，解决存储空间不足问题

核心技术：

- 索引重构
- 智能选模
- 自适应压缩算法
- 智能质检（可选）

流量解决方案：实时数据传输

适用场景：

针对实时采集数据，解决带宽不足与传输延迟

核心技术：

- 智能选模
- 流式实时处理，数据不落地，毫秒级响应
- 异常监测，确保传输稳定性
- 播放端无感切换，保障用户体验

压缩比率范围：50% ~ 90%

注：压缩比率视原始文件格式、大小、清晰度，以及用户方对保真效果的要求而动态调整。

方案核心优势

画质高保真

特有底层编码技术，不改变帧数、不改变分辨率，确保影像质量无损。

保存原始信息

构建摄像头元数据，完整保留来源、时间戳等关键信息，便于溯源。

大幅节省资源

高比率压缩技术，最高可压缩至原文件的几分之一，极大降低带宽和存储成本。

保留原有格式

压缩后与原文件格式完全一致，可直接使用原软件任意调取、编辑处理。

广泛格式兼容

全面支持全球常见的音频、视频、图像格式，适应多样化数据源。

智能压缩策略

依据视频内容特征和信息价值衰减曲线，综合选择基础、静态或深度压缩。

其他核心功能

智能画质评估

基于拉普拉斯方差算法，自主评估媒体文件的清晰度，为压缩决策提供辅助依据

熵差分量化重组

构建视频全库，进行跨文件联合压缩，在原有基础上进一步提升整体压缩效率

环验证技术

对摄像头帧联合时间签名，精准取证时间信息，确保数据的真实性和可追溯性

区块链视频特征存证

利用区块链技术提升文件可信度，主要用于纠纷处理、取证等高要求场景

面向AI的视频压缩

以AI评价框架为导向构建压缩模型，显著提高AI对压缩后文件分析的准确率

支持水印

支持自定义水印内容和多种形态，用于标识文件信息、事件溯源，保护数据安全

降本增效，合规无忧

项目背景

某保险公司按监管要求需永久保存双录视频。存量数据约 2PB，年增量约 500TB，存储单价 120元/TB/月

首年成本节省

压缩前年均存储: 2298 TB
压缩后年均存储: 1581 TB

100万元/年

次年降本激增

压缩前年均存储: 2798 TB
压缩后:年均存储 1264 TB

220万元/年

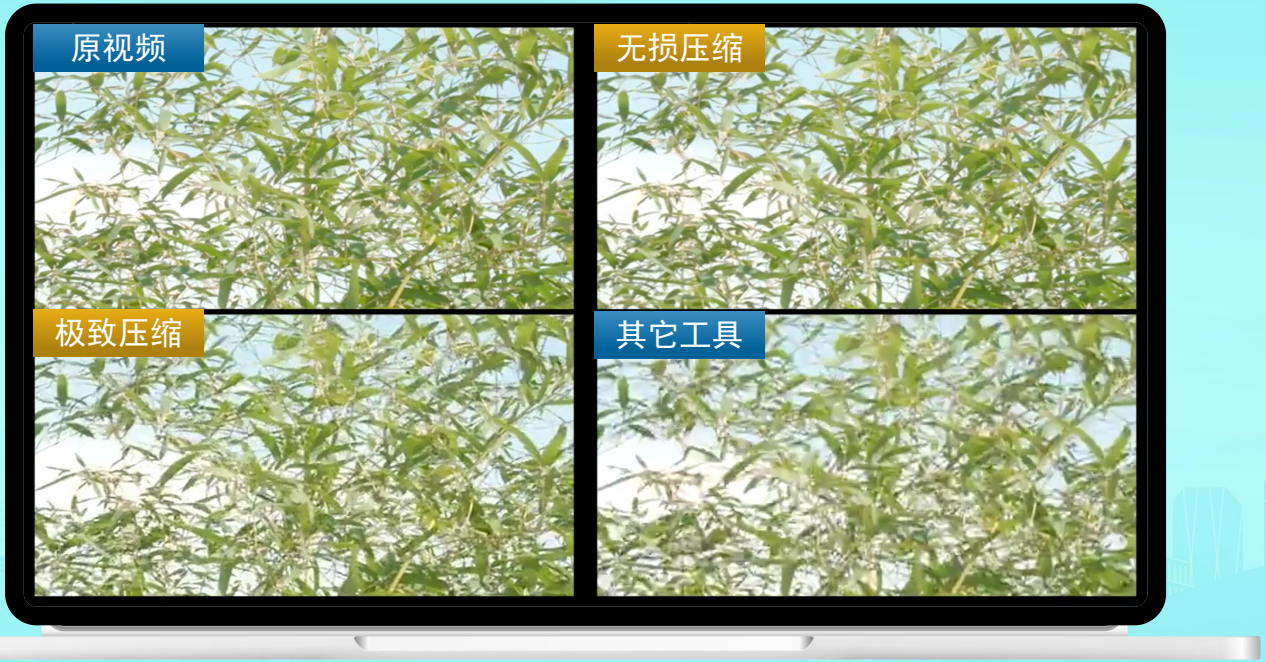
快速盈亏平衡

项目实施**第二年**起，节省成本完全覆盖设备投入，正式**实现收益**。

持续长期收益

收回成本后，预计**每年**稳定节省**超200万+开支**，实现显著的长期优化。

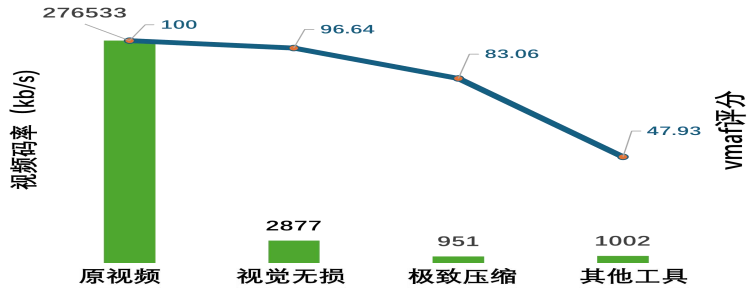
客户案例: 视频效果对比



客户案例: 同帧截取画质比对

压缩性能综合对比

码率优化与画质保真 (VMAF)

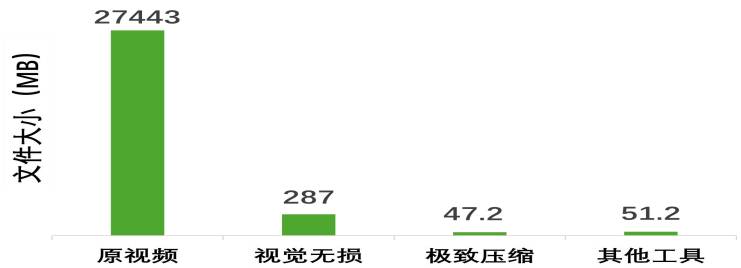


高保真与低码率的完美平衡

无损压缩码率可降至 2877kb/s，VMAF评分高达 **96分**；

极致压缩下，码率降低至 951kb/s，VMAF评分仍保持 **83分**，远超竞品的 47.9分，实现低码率下的高保真体验。

存储空间压缩效率对比



极致的成本节约与效率提升

无损压缩下，相比原视频节省 **99%** 空间（26.8GB→287MB）；

极致压缩下，相比原视频节省 **99.8%** 空间（26.8GB→47.2MB），相比其他工具再节省 7.8%，显著降低存储传输成本。

谢谢观看

智慧科技赋能数字金融