附件 2

职业与成人教育数字化创新实践
典型案例申报表

案 例 名 称：基于态势感知与超融合架构的数据安全保障实践

案 例 负 责 人：杨振宇

所在单位及盖章：安徽交通职业技术学院

推 荐 时 间：2025 年 11 月 28 日

安徽省职业与成人教育协会 制

2025 年 10 月

申报人承诺书

在申报创新实践典型案例过程中，本人自愿做出如下承诺：

对填写的各项内容负责，案例申报材料真实、可靠，不存在知识产权争议，未弄虚作假、未剽窃他人成果。

案例负责人签字：_____

所在单位（盖章）：_____

2025 年 11 月 28 日

职业与成人教育数字化创新实践典型案例申报表

<table>
<tr><td>申报单位</td><td colspan="3">安徽交通职业技术学院</td></tr>
<tr><td>联系人</td><td>杨振宇</td><td>职 务</td><td>信息化建设与管理中心主任</td></tr>
<tr><td>手 机</td><td></td><td>邮 箱</td><td></td></tr>
<tr><td>部门领导</td><td>孙晓雷</td><td>职 务</td><td>校长</td></tr>
<tr><td>手 机</td><td></td><td>邮 箱</td><td></td></tr>
<tr><td>通讯地址</td><td colspan="3">安徽省新桥国际产业园寿州大道 16 号</td></tr>
<tr><td>案例名称</td><td colspan="3">基于态势感知与超融合架构的数据安全保障实践</td></tr>
<tr><td colspan="4">安徽交通职业技术学院，是全省唯一一所具有鲜明交通行业特色的高职院校。学校秉承“经世致用、实学报国”的办学理念，坚持“立足交通、服务行业、面向社会”的办学定位，校企合作，产学互动，孕育了“勤奋、通达、敬业、乐群”的优良校风，为安徽经济发展和交通运输行业培养、培训了 11 万余名高素质技术技能人才。学校现为教育部汽车类技能型紧缺人才培养培训基地、省级专业技术人员培训基地。</td></tr>
<tr><td rowspan="2">案例
背景</td><td colspan="3">随着智能化的普及,信息安全风险也逐渐增大,威胁类型复杂、安全管理运维人力不足的问题凸显。且传统规则防护无法应对 APT 攻击、内鬼行为等隐蔽威胁，勒索病毒横向扩散导致数据丢失、被窃取等风险。信息系统多，物理/逻辑故障恢复效率低，单点故障易引发业务中断和数据丢失。</td></tr>
<tr><td>佐证材料页码</td><td colspan="2">第 1 页-第 7 页</td></tr>
</table>

实施 目标	案例通过 AI 驱动的 UEBA 模型、自动化运维工具，实现异常行为自动识别、告警自动分类，通过超融合架构将安全能力嵌入计算、存储、网络环节，实现 “业务与安全同步规划”，彻底解决传统规则防护无法应对隐蔽威胁的问题，提升防护全面性，降低硬件成本与运维难度。使学校数据安全保障形成闭环，业务连续性提升，实现 “安全与业务深度协同”。不仅确保本校方案顺利落地，还应具备推广性，适配不同规模院校，可供同类院校借鉴后实现低成本快速落地。	
	佐证材料页码	第 8 页-第 10 页

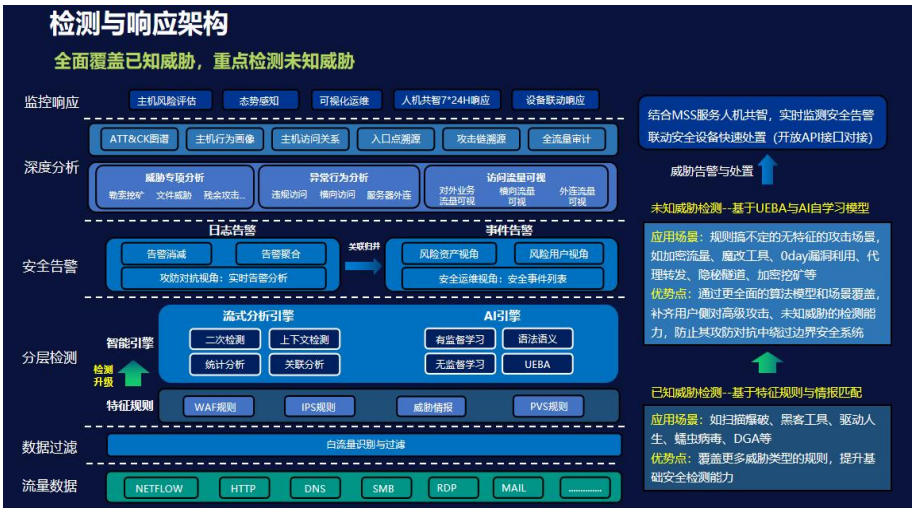
主要 举措	1. 以“全域流量采集+内生安全”双轮驱动，破解传统防护短板 学校摒弃传统 “外部设备叠加” 模式，将安全能力融入业务架构:网络安全层面通过全流量采集构建安全感知体系,结合 UEBA 模型构建动态行为基线，持续学习内部用户与资产行为特征，精准识别偏离基线的异常行为，有效发现内鬼行为与潜伏威胁，避免数据泄露风险;数据安全架构上,依托超融合技术实现安全能力内生，计算虚拟化支持虚拟机快照应对逻辑故障,存储虚拟化开启多副本同步确保数据高可用,网络虚拟化集成分布式防火墙阻断勒索病毒横向传播。 2.构建“分层协同”技术体系，实现“监测-防护-恢复”闭环 为避免技术碎片化，学校按分层逻辑设计架构: 监测层采用 “采集 - 检测 - 评估” 三级架构，采集层收集全流量、系统日志等多源数据，检测层通过特征规则与 AI 引擎识别恶意攻击，评估层实现多设备联动与威胁溯源; 防护层实施 “边界 + 核心” 双重防护，边界依托态势感知识别并联动安全组件拦截外网恶意流量,内网基础设施核心通过超融合的内生分布式防火墙实现虚拟机 L3-L4 层微隔离; 恢复层建立 “快照 + 备份 + 多副本” 三重保障，确保故障快速恢复。

	3. 聚焦“业务适配”场景学校避免“通用化安全”误区，针对校园核心场景构建“多手段协同”防护方案，打破防护技术单场景局限，按业务需求灵活组合技术，实现“场景精准匹配、技术互补支撑”。在教学管理场景，采用“全流量监测 + 分布式防火墙”防护：前者监控安全异常，防范师生隐私泄露；后者划分教学安全域，隔离非必要业务虚拟机，限制无关东西向流量，避免教学数据被非法访问。 4. 建立“标准化 + 低成本”实施路径，保障方案可落地可推广 学校从部署、运维、优化环节建立标准化流程：部署阶段明确探针覆盖范围、超融合架构搭建要求，分阶段推进确保稳定；成本控制上，通过超融合架构整合资源，大幅度提升资源利用率，降低硬件采购与人力成本。	
	佐证材料页码	第 11 页-第 13 页

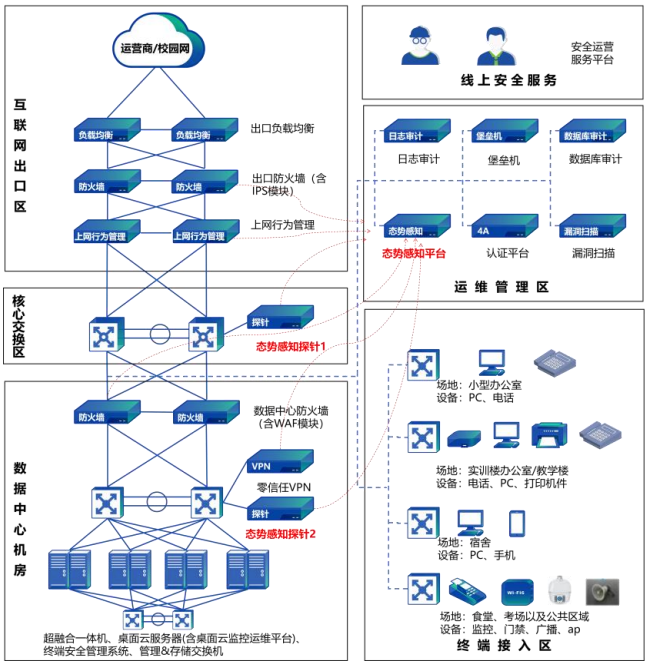
<table>
<tr><td rowspan="2">特色
应用</td><td colspan="2">1. 动态基线建模: 实现异常行为精准量化
突破传统固定规则局限，基于机器学习构建 UEBA 模型，通过持续学习用户与资产行为形成动态基线，以偏离度量化评估异常行为，解决 “未知威胁难检测” 问题，内鬼行为检测误报率≤2%，较传统模式大幅提升精准度。
2. 虚拟机级防护: 阻断云内横向攻击路径
创新应用超融合内生的分布式防火墙，实现虚拟机间 L3-L4 层微隔离，将防护粒度从边界缩小至 “虚拟机级”，即使攻击者突破边界，也能阻断勒索病毒在云机房内部横向渗透，2024 年运行期间未发生云内跨虚拟机攻击事件。
3. 漏斗式检测架构: 提升告警处置效率
设计 “采集 - 检测 - 评估” 三级分层告警提纯机制，采集层全量收集数据，检测层筛选有效告警，评估层实现多源关联分析，大幅减少无效告警，使运维精力聚焦核心威胁，处置效率提高 60%，重大安全事件响应时间≤30 分钟。
4. 智能化规则生成与预发布验证: 降低分布式防火墙配置风险
基于流可视历史访问数据智能生成分布式防火墙（Distributed Firewall，DFW）规则，且支持规则预览与修改；同时创新推出 DFW 规则预发布验证功能，避免误配置影响业务，同时通过日志上报持续优化规则，大幅度提升了规则配置效率。</td></tr>
<tr><td>佐证材料页码</td><td>第 14 页-第 16 页</td></tr>
</table>

成果展示

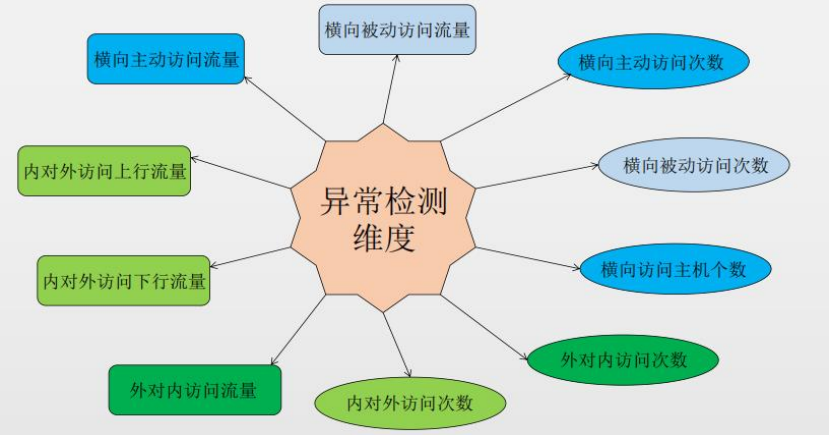
1. 校级网络安全态势感知平台



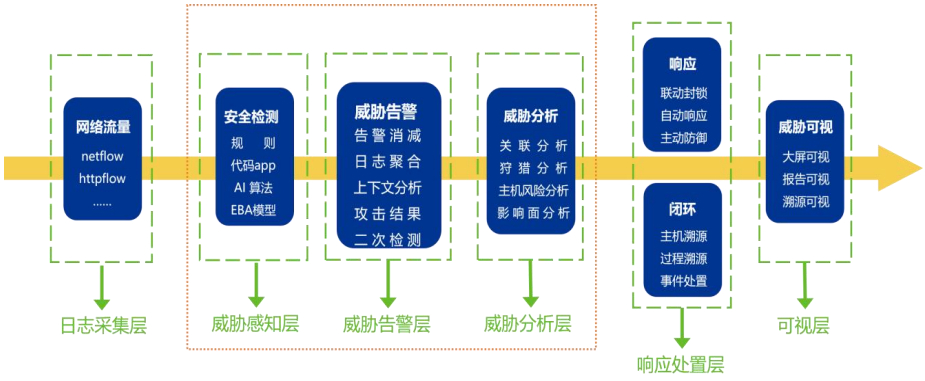
全域流量采集：在网络核心交换区、数据中心边界等关键节点部署潜伏威胁探针，实现对东西向和南北向全流量的实时采集。



智能行为分析：基于机器学习构建用户与实体行为分析（UEBA）模型，形成动态安全基线，对偏离基线的异常登录、数据异常访问等行为进行量化评估与预警，精准发现内鬼行为与已入侵的潜伏威胁。

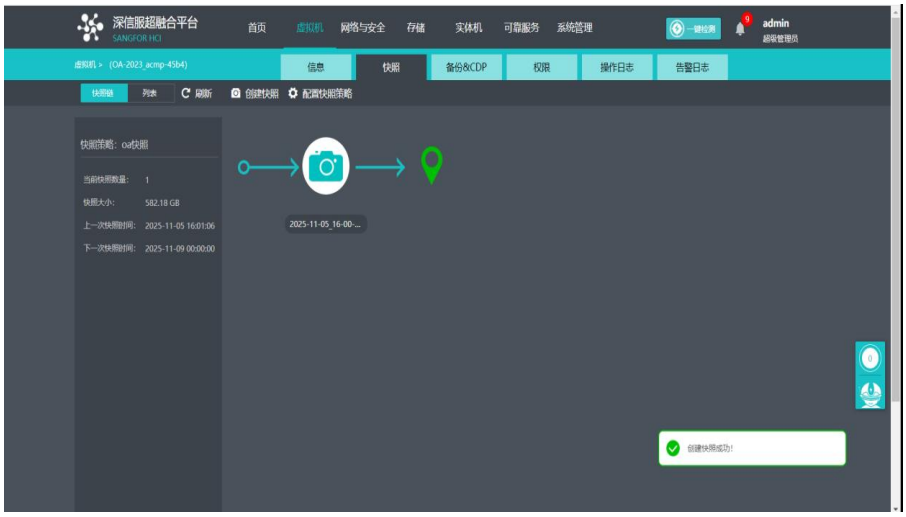


漏斗式告警提纯：采用三级分层处理架构（采集层→威胁检测层→风险评估与联动层），通过规则引擎与 AI 模型关联分析，层层过滤，输出高置信度的安全事件，极大提升告警准确率。

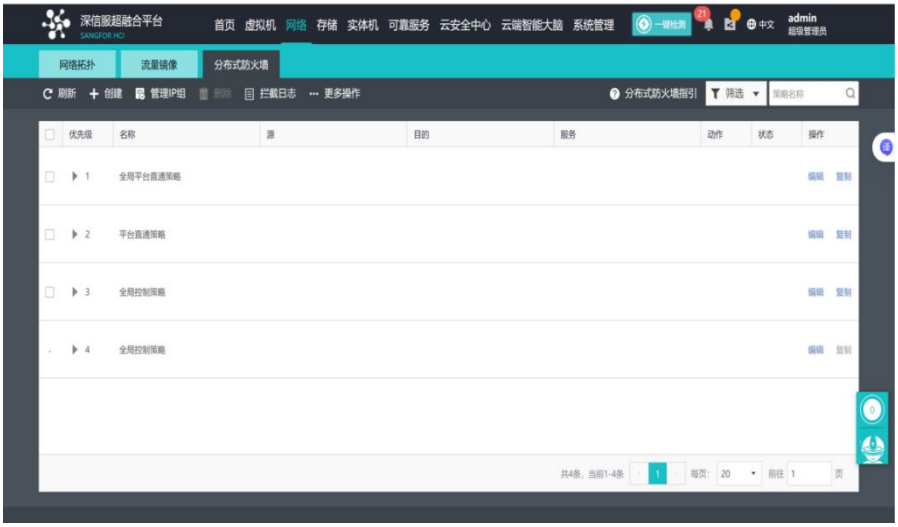


2. 超融合内生安全中心

数据高可用与快速恢复：利用超融合架构的计算与存储虚拟化能力，实现虚拟机快照、定期备份以及多副本数据同步机制。确保单点数据损坏或物理故障时，业务能无感知切换或在分钟级内快速恢复。



云内生勒索病毒预防：创新性启用超融合平台原生的分布式防火墙，在虚拟化层面为每台虚拟机实施 L3-L4 层的微隔离策略。基于历史访问关系智能生成规则，并支持预发布验证，有效阻断虚拟机之间的异常端口扫描、暴力破解等横向渗透行为，将勒索病毒遏制在初始感染点。



佐证材料页码	第 17 页-第 26 页

<table>
<tr><td rowspan="2">经验
总结</td><td colspan="2">一．数据安全建设需从 “外部附加”转向“内生融入”
传统安全模式易存在防护断层与资源浪费，案例通过超融合架构将安全能力嵌入计算、存储、网络环节，实现 “业务与安全同步规划”，不仅提升了防护全面性，还降低了硬件成本与运维难度，这一实践佐证了“内生安全”是数字化转型的重要核心方向之一。
二．AI 技术是破解 “人力不足 + 威胁复杂” 的关键
高校普遍面临运维人力不足、威胁类型复杂的矛盾，案例通过 AI 驱动的 UEBA 模型、自动化运维工具，实现异常行为自动识别、告警自动分类，大部分运维工作可自动化完成，人力成本可大幅度降低。这一实践做佐证了 AI 技术是平衡防护强度与运维成本的有效手段之一，能为高校数据安全保障提供重要支撑。
三．建设模式需平衡“标准化”与“差异化”
案例将核心模块（态势感知平台、超融合灾备单元）进行标准化设计后，按业务需求灵活调整策略，不仅适用于安徽交通职业技术学院，更能适配不同院校的个性化需求，避免 “一刀切”问题，这种模式同样利于在本科、职业院校等不同场景中推广应用。</td></tr>
<tr><td>佐证材料页码</td><td>第 27 页-第 32 页</td></tr>
</table>

未来展望	AI 技术是破解 “人力不足 + 威胁复杂” 的关键。高校普遍面临运维人力不足、威胁类型复杂的矛盾，案例通过 AI 驱动的 UEBA 模型、自动化运维工具，实现异常行为自动识别、告警自动分类，大部分运维工作可自动化完成，人力成本可大幅度降低。这一实践做佐证了 AI 技术是平衡防护强度与运维成本的有效手段之一，能为高校数据安全保障提供重要支撑。 政策与校企合作助力生态完善。案例响应教育部《教育信息化 2.0 行动计划》要求，通过校企合作优化技术方案，形成 “需求 - 研发 - 应用” 的良性循环。这提示在教育行业数据安全生态建设中，可进一步强化政策引导作用，深化校企协同，为方案落地与技术迭代提供更有力的支撑。

本单位全面了解申报本次案例征集活动的有关要求，承诺所提供的材料真实、有效。如有不实内容，自愿承担相应责任。 本单位作为上述案例作品的著作权人，如被专家推介，同意安徽省职业与成人教育协会指定出版社在中国大陆地区、在著作权保护期内免费使用该作品，用于出版，并以申报单位加审稿人、编写人姓名的方式署名。 单位名称：（盖章） 2025 年 11 月 28 日
专家组意见 年　月　日
专委会意见 （公章） 年　月　日

备注：请将申报表电子版于 2025 年 11 月 30 日前上传至申报平台《数字化创新实践典型案例评审系统》，系统网址：http://szh.zhijiao361.com。