



智维数据 NetsightAI

产品技术白皮书 • WHITE PAPER

NetsightAI 应用感知与 异常检测平台

应用全感知 • 异常早发现

出品方：智维数据 (Intelligent Analytics Platform)

文档类型：产品技术白皮书 | 版本：V1.0

部署形态：旁路镜像接入 · 私有化部署 · 数据不出域

文档属性	内容
产品名称	NetsightAI 应用感知与异常检测平台 (Intelligent Analytics Platform)
出品方	智维数据
适用读者	政企与能源行业信息化负责人、 CTO / 总架构师、网络与安全运维管理者
部署形态	旁路镜像接入 · 私有化部署 · 数据不出域

目录

- 1. [一、执行摘要](#)
- 2. [二、行业背景与挑战](#)
- 3. [三、产品定位与核心理念](#)
- 4. [四、产品总体架构](#)
- 5. [五、核心能力](#)
- 6. [六、典型异常场景](#)
- 7. [七、闭环处置：从看到异常到规则治理](#)
- 8. [八、应用台账与综合报告](#)
- 9. [九、产品功能矩阵](#)
- 10. [十、私有化部署与数据安全](#)
- 11. [十一、客户价值](#)
- 12. [十二、结语](#)

一、执行摘要

5 类	8 类	5 维	7 大
异常检测规则	应用分类体系	置信度评估	功能模块

Executive Summary

随着电力、政务、能源等关键行业数字化程度不断加深，数据中心与多级生产网络内部署了大量业务系统、数据库、视频物联终端与办公应用。网络规模与应用数量持续增长，通信关系日趋复杂，传统以“链路通断、设备存活”为核心的网管手段，已难以回答“网络里跑着哪些应用、谁在和谁通信、哪些行为偏离了正常基线”这一根本问题。

NetsightAI 应用感知与异常检测平台以**旁路镜像流量**为数据底座，在不改变现有网络拓扑、不影响业务运行的前提下，对全量网络流量进行被动采集、协议解析与应用自动识别，自动建立应用台账，并结合**业务预判**与**五维置信度**评估，对端口扫描、服务器外联、新增服务端口、流量基线偏离、新增客户端等五类典型异常行为进行实时检测与可核证告警，最终形成“看到异常—研判下钻—处置例外—规则治理”的完整业务闭环。

平台核心主张可概括为一句话：**应用全感知，异常早发现**——让网络中的应用与服务始终清晰可见，让潜在风险在造成实际影响之前被看见、被理解、被处置。

二、行业背景与挑战

要理解应用感知与异常检测的必要性，首先需要看清当前数据中心网络在规模、监测手段与风险潜伏方式上的三重变化。

（一）数据中心正在变得前所未有的复杂

现代企业级数据中心通常同时承载多类网络区域。以电力行业为例，一张网络内部往往并存以下区域：

- **生产控制区**：调度自动化、SCADA、变电站远动等关键生产系统，采用 IEC 104 等工控协议；
- **核心交换区**：承担区域间高速转发的核心交换机与汇聚节点；
- **办公业务区**：OA、ERP、Web 业务、数据库（MySQL 等）等管理信息类系统；
- **视频物联区**：视频监控平台、RTSP 视频流、海量摄像头与物联终端；
- **外联互联网区**：与外部网络、合作伙伴及互联网相连的边界区域。

这些区域之间存在大量星型接入、跨区互联与动态会话。应用以“IP:端口 + 协议 + 通信关系”的形式分散在网络各处，且随业务上线、扩容、下线不断变化。

（二）传统监测手段存在结构性盲区

面对上述复杂度，依赖人工台账、主动探测或单点日志的传统方式普遍面临以下问题：

1. **看不全**：资产台账依赖人工登记、更新滞后，新增服务、私开端口、影子 IT 长期游离在视图之外；
2. **看不懂**：即使采集到流量，也缺少面向“应用”的识别与归集能力，原始会话无法转化为业务语言；
3. **看不深**：传统告警多为设备级、阈值级的“黑盒报警”，缺少基线对比、证据明细与业务上下文，值班人员难以研判真伪；
4. **告警扰民**：静态阈值误报多、漏报也多，安全与运维团队疲于奔命，逐渐对告警失去信任；
5. **不敢部署**：生产网络对可用性极为敏感，串接式、侵入式的监测方案因担心引入单点故障而难以落地。

（三）异常往往潜伏在“正常流量”之中

大量安全事件与运行风险在爆发前并非毫无征兆：一台从不外联的 SCADA 服务器突然主动连接外部地址、一台数据库主机首次开放 3306 端口、某个 OA 系统的平均包长骤然下降、一个陌生 IP 第一次接入视频平台并建立大量会话……这些行为夹杂在海量正常通信中，单靠人工巡检几乎无法及时捕捉。行业真正需要的，是一个**以网络流量为客观事实依据、能够自动看清应用并主动识别行为偏离**的平台。

三、产品定位与核心理念

面对上述挑战，NetsightAI 在产品定位、设计理念与能力主线上形成了清晰而一致的思路。

（一）产品定位

NetsightAI 是一款面向政企与关键行业的**应用感知与异常检测平台**。它介于网络流量数据分析与安全监测之间，以流量数据为唯一事实来源，向上回答资产与应用问题（“网络里有什么”），向下回答行为与风险问题（“正在发生什么异常”），是连接网络可视化与安全运营的基础能力平台。

（二）核心理念

- **流量即事实**：一切判断以真实镜像流量为依据，不依赖代理、不依赖业务系统改造，结论客观、可回溯、可取证；
- **应用为中心**：不停留在 IP 与接口层面，而是把流量还原为“应用、服务、端口、业务归属与通信关系”；
- **可解释优先**：每条异常不仅给出结论，还附带基线对比、证据明细、影响范围与处置建议，拒绝“黑盒报警”；

- **越用越准**：通过例外规则、误判治理与阈值治理，让检测灵敏度持续贴合业务实际；
- **零侵入可落地**：旁路接入、私有化交付，充分尊重生产网络的可用性与数据安全要求。

（三）四步能力主线

平台将原始流量转化为可处置结论的过程，沿一条清晰主线展开：

步骤	能力	说明
01 数据底座	旁路全流量采集	镜像分光，会话、指标、协议、报文全程留证
02 应用感知	应用自动发现	识别应用、服务、端口与业务归属并自动分类归集
03 智能研判	业务预判 + 置信度	五维评估量化识别可靠程度，结论可解释、可核查
04 异常检测	五类异常规则	扫描、外联、端口、基线、新客户端实时比对触发

四、产品总体架构

NetsightAI 以一条分层数据处理链路为骨架，并在架构层面贯彻零接触、全留证与多站点汇聚等设计原则。

（一）一条链路：把原始流量变成可处置的结论

平台采用分层架构，数据自采集侧逐层加工，最终输出结构化告警与综合报告，全程被动旁路，不改变现有网络拓扑：

旁路采集 → 协议解析 → NetsightAI 分析中枢 → 异常检测 → 告警与报告

1. **旁路采集层**：通过核心交换机端口镜像（SPAN） / 分光获取全量流量，形成会话、指标、协议与报文级原始证据；
2. **协议解析层**：识别通信协议、端口与载荷指纹，覆盖 HTTP、MySQL、IEC 104、RTSP 等通用与工控、视频协议；
3. **NetsightAI 分析中枢**：完成应用归属判定、五维置信评分与历史基线比对，是平台的智能核心；
4. **异常检测层**：五类异常规则对实时流量与基线进行比对，命中即生成可核证告警；
5. **告警与报告层**：通过邮件、Webhook 按路由下发告警，并自动生成日报、周报、月报留档。

（二）架构设计原则

- **零接触业务**：采集设备不串接在业务链路中，无单点故障，镜像中断不影响生产；
- **全量留证**：不仅产生结论，还保留会话明细、包分布、扫描会话等原始证据，支撑下钻研判；
- **规则与基线内生**：业务预判、置信度、基线学习与异常规则全部在平台内闭环，无需外部依赖；
- **多站点汇聚**：以站点维度组织网络位置与资产，天然适配调度中心、变电站、营业厅等多级网络的集中监测。

五、核心能力

平台的核心能力沿数据链路依次展开：从全流量采集、协议解析与应用发现，到业务预判、置信度评估，再到五类异常行为检测。

（一）旁路全流量采集

平台通过核心交换机镜像口或分光方式接入流量，在交换机侧将指定端口流量复制一份引流至采集引擎，原始流量仍按原有路径正常转发，业务与网络均无感知。

- **无源旁路**：不串接、不改变拓扑、不引入单点故障，对生产业务零影响；
- **全要素留证**：完整记录会话五元组、流量指标、协议类型与关键报文，为后续研判提供证据；
- **多源汇聚**：可同时接入生产控制、办公、视频物联、外联等多路来源，统一汇聚分析；
- **弹性扩展**：采集与分析分层部署，可按链路带宽与站点规模横向扩容。

（二）协议解析与应用自动发现

采集到的流量经过深度协议解析，被还原为可理解的应用与服务。平台据此**自动发现网络中的应用**，识别其 IP:端口、协议、通信对端与流量特征，并将大量零散应用**自动分类、归集**到数据库、Web 业务、视频流、运维远程等业务类别中，形成结构化的应用视图，无需人工逐个录入。

应用发现完成“**发现** → **认领** → **台账**”闭环：新应用被自动标记为“新发现”，经运维确认后进入“已定义”台账，长期未认领的进入“待定义”，存在异常的单独标注，下线应用同步归档。应用台账完整记录名称、IP:端口、协议、分类、所属站点、客户端与流量信息，并支持通过 Excel / CSV 进行字段映射导入、冲突预检与一键回滚。

（三）新应用业务预判

对于新发现的应用，平台不止于简单标记“未知”，而是基于历史样本给出**可解释、可复现的业务归属预判**，列表与详情结果严格一致。判定遵循明确的优先级流程：

1. **同 IP 优先（优先级①）**：在同一主机上是否已存在已定义应用；命中则沿用该应用名称，直接输出预判；
2. **同端口加权（优先级②）**：结合同网段样本加权计数——/24 网段优先、/16 网段次之，输出权重最高的应用名；
3. **兜底策略**：同 IP、同端口均无样本时预判为“未知”，等待人工认领，不做臆测。

该机制把工程师“看这台主机上还跑过什么、同网段同端口一般是什么”的经验固化为规则，大幅降低新应用的人工判断成本。

（四）五维置信度评估

为量化应用识别结论的可靠程度，平台从五个维度动态计算置信度，并给出综合评分（如 **≥85 判定为高置信**）：

维度	评估含义
载荷特征	应用报文载荷内容与已知应用指纹的吻合程度
协议匹配	实际通信协议与该类应用标准协议的一致性
规律性	通信行为在时间、周期上的稳定与规律程度
多样性	通信对端、端口、行为模式的丰富与分散程度
连续性	会话与流量在时间维度上的持续稳定程度

综合置信度随识别证据动态更新，使“这个应用被识别成某业务”这一结论首次具备了可量化、可比较的可信度量，运维可据此优先认领高置信应用、复核低置信应用。

（五）五类异常行为检测

平台内置五类面向真实运维场景的异常检测规则，实时比对流量与历史基线，命中即生成结构化告警。每类规则均提供可配置的默认阈值：

编号	异常类型	检测逻辑	默认规则阈值
R-01	端口扫描探测	统计窗口内 TCP SYN / 命中端口数超阈值，伴随低建	60 秒内访问端口 > 20

		连、高 RST	个
R-02	新增服务端口	已认领主机出现基准期内未见端口，持续存在且可达	基准 30 天，持续 > 5 分钟
R-03	服务器外联	历史无外联的关键主机主动连接非已知服务器，可叠加扩散证据	30 天无外联，外联 ≥ 1 次
R-04	流量基线偏离	包结构偏移分或均包长变化超阈值，连续多个时间片持续	偏移 > 0.35 或均包长变化 > 60%
R-05	新增客户端	客户端 IP 首次出现且会话数超阈值，可叠加扩散范围判定	首次出现且会话数 > 5

五条规则覆盖了"被探测（扫描）、被暴露（新端口）、主动失陷（外联）、行为异常（基线偏离）、陌生接入（新客户端）"等典型风险面，既适用于安全监测，也能发现配置变更、业务异常等运行问题。

六、典型异常场景

平台对每类异常都能还原完整证据链。以下为五类典型场景的实际研判示例：

场景	严重度	关键对象	平台抓取到的证据
端口扫描探测	高危	源 10.10.8.200	60 秒内狂扫 312 个端口 ，含 24 条扫描会话，SYN 1,860+、RST 201，低建连高 RST 特征明显
新增服务端口	高危	10.10.5.15:3306	已认领主机首次出现 MySQL 3306 端口，持续存在且可达，基准 30 天内未见
服务器外联	高危	10.20.1.100 → 10.60.8.99	历史无外联的 SCADA 系统主动连接外部非已知地址，可叠加横向扩散证据
流量基线偏离	高危	10.10.3.20:443（OA）	OA 系统平均包长 骤降 68% ，包结构偏移分超 0.35，连续多个时间片持续
新增客户端	中危	172.16.100.50 → 10.30.1.10:554	陌生 IP 首次接入视频监控平台，已建立 8 个会话，超过阈值 5

与传统"黑盒报警"不同，每条异常都做到**可核查而非仅给结论**：

- **基线值 vs 当前值**对比并给出偏差百分比，异常程度一目了然；
- **扫描会话 / 包分布**明细可逐级下钻，精确定位到具体 IP、端口与会话；
- **站点 / IP 别名 / 业务预判**同步呈现，缩短从告警到业务的回查路径；
- 每条告警附带**影响范围与处置建议**，值班人员可直接据此研判、处置。

七、闭环处置：从看到异常到规则治理

异常行为检测页是平台的处置中枢。平台不止于“发现”，而是把发现转化为一条可持续优化的业务闭环：

1. **STEP 01 看到异常**：按严重程度、处理状态、异常类型多维筛选，异常卡片实时刷新、计数同步，高危事件以色条醒目标识；
2. **STEP 02 研判真伪**：打开详情查看基线对比、扫描会话、包分布等证据，结合业务上下文判断事件真伪；
3. **STEP 03 处置 / 例外**：确认异常可一键标记处理；确认为误报则按五类规则的差异化参数创建例外规则；
4. **STEP 04 规则治理**：在规则管理中心维护检测规则、误判记录与全局白名单，阈值可调、可溯、可审计。

平台提供三个治理视图：**检测规则**（启用/停用五类规则并调整阈值）、**误判记录**（沉淀历史误判）、**全局白名单**（维护可信对象）。例外规则支持按对象 / 网段 / 全局阈值分级生效，遵循“**精准豁免优先，而非整体关闭规则**”的原则——例如可将每周三 08:00–12:00 的授权安全扫描配置为例外，同类事件自动标记误判，同时不削弱其余时段的检测能力，从机制上避免“一误报就关停规则”导致的漏报风险。处理率自动统计，系统由此“越用越准”。

八、应用台账与综合报告

- **应用台账**：自动汇聚应用名称、IP:端口、协议、分类、站点、客户端与流量，状态涵盖已定义、新发现、待定义（超 7 天）、存在异常、已下线等，让应用资产始终在线、随时可查；
- **异常分布与处置建议**：按严重程度归类异常，自动统计处理率，支撑运维量化管理；
- **综合报告**：日报 / 周报 / 月报一键切换，汇总核心 KPI、异常分布与台账状态概览，支持按日历选择历史期，既满足例会汇报，也满足审计留档；

- **台账导入**：支持 Excel / CSV 字段映射、扩展字段、导入前冲突预检与一键回滚，兼容既有 CMDB 与资产数据。

九、产品功能矩阵

平台以一个统一工作台覆盖"监测·治理·运营"全流程，由七大功能模块构成：

模块	核心能力
全局概览	门户首页一屏掌握核心指标与实时态势，KPI 滚动、流量趋势 / 异常时间轴、应用分类 Treemap 与 Top10，作为下钻入口
异常行为检测	五类规则实时检测，详情 / 例外 / 规则三大弹窗，分级筛选与动态计数，批量处理与撤销
应用发现与管理	自动发现、业务预判、认领到台账，六状态台账、预判依据、排序 / 导出 / 通讯对分析
综合报告	日 / 周 / 月报一键切换，KPI 与异常分布、台账状态概览、历史期日历选择
账号与权限	账号、角色与状态管理，多类角色、启用 / 停用 / 锁定、数据范围分配，支撑鉴权与审计溯源
告警通知配置	邮件 / Webhook 通道，严重度 × 类型路由矩阵，告警升级、合并与静默抑制，让告警发给正确的人
数据导入与映射	台账、IP 别名、站点统一导入，五步向导、字段映射与扩展字段、冲突预检 / 一键回滚

此外，平台提供全平台统一的**全局时间选择器**，支持自定义起止时间、最近历史记录与多组预设范围，保证各模块在同一时间口径下分析。在能力规模上，平台内置 **5 类异常检测规则**、**8 类应用分类体系**、**5 维置信度评估**、**7 大产品功能模块**，构成完整的应用感知与异常检测工作台。

十、私有化部署与数据安全

面向能源、政企等关键行业，平台采用私有化交付，在企业自有机房或私有云内部署，分为三层：

层级	部署形态	关键特性
01 采集层	旁路镜像接入	核心交换机镜像 / 分光采集，不串接、不改变拓扑，对业务零影响；无源旁路、无单点故障，会话 / 指标 / 协议全留证，多站点统一汇聚
02 分析层	本地分析中枢	协议解析、应用识别、业务预判与五类异常规则全部在企业内网运行，五维置信度本地计算，规则可配、阈值可调、异常实时检测，数据不外传
03 运营层	告警与报告闭环	邮件 / Webhook 按严重程度 × 类型智能路由，日 / 周 / 月报自动汇总，账号角色与关键操作全程审计留痕，台账导入支持一键回滚

该交付方式带来三项关键价值：

- **数据主权可控**：旁路镜像加私有化部署，流量与台账数据始终不出企业边界，契合关键信息基础设施与政企数据安全、等级保护的合规要求；
- **多站点集中监管**：以站点维度组织网络位置与资产，适配调度中心、变电站、营业厅等多级网络的集中监测；
- **贴合业务可落地**：业务预判、IP 别名、站点归属、例外规则等设计均源自真实运维场景，检测结论可直接驱动处置。

十一、客户价值

- **资产清晰**：把“黑盒网络”变成动态更新的应用台账，新增服务、私开端口、影子 IT 无处遁形；
- **风险前置**：将端口扫描、违规外联、陌生接入等行为拦截在造成影响之前，缩短威胁潜伏时间；
- **告警可信**：基线对比 + 证据下钻 + 业务上下文，让每条告警可研判、可核证，显著降低误报疲劳；
- **处置高效**：告警、研判、处置、例外、规则治理在同一闭环内完成，处理率可视，能力持续进化；
- **落地稳妥**：旁路零侵入、私有化数据不出域，既不影响生产可用性，又满足行业合规要求。

十二、结语

网络流量是数字化系统运行状态最客观、最难以伪造的事实记录。NetsightAI 应用感知与异常检测平台以旁路镜像流量为底座，把复杂数据中心里原本分散、晦涩、易被忽略的通信行为，还原为清晰的应用资产与可解释的异常结论，帮助政企与能源客户真正做到“**看清资产、发现风险、闭环处置**”。

让网络里的每一个应用与每一次异常，都始终清晰可见——这正是 NetsightAI 的产品使命：**应用全感知，异常早发现**。

智维数据 NetsightAI · 应用感知与异常检测平台

本白皮书基于产品 V1.0 能力编写，具体功能与参数以实际交付版本为准。