



智维数据

Intelligent Analytics Platform

灵眸智能监控系统

产品白皮书

NSMART · PRODUCT WHITE PAPER

AIOps 智能网络运维平台

北京智维盈讯网络科技有限公司

版本 V1.0 | 2026 年 10 月

目录

- 一、执行摘要..... 4
- 二、行业背景与运维挑战..... 5
 - 2.1 数字化转型带来的运维新挑战..... 5
 - 2.2 传统流量监控产品的局限..... 5
 - 2.3 AIOps 智能化运维成为趋势 6
 - 2.4 来自一线的真实痛点..... 6
 - 2.5 智能监控与传统监控的本质区别..... 6
- 三、产品概述..... 7
 - 3.1 产品定位..... 7
 - 3.2 核心理念..... 7
 - 3.3 产品亮点..... 7
 - 3.4 量化价值与收益..... 8
 - 3.5 产品能力总览..... 8
- 四、核心功能体系..... 9
 - 4.1 全局搜索..... 9
 - 4.2 告警中心..... 9
 - 4.3 智能分析..... 11
 - 4.4 智能巡检..... 12
 - 4.5 数据分析..... 13
 - 4.6 业务梳理..... 14
 - 4.7 系统与用户中心..... 16
- 五、AI 大模型智能能力 17
 - 5.1 AI 能力总览 17
 - 5.2 智能告警根因分析..... 17
 - 5.3 业务拓扑 AI 分析助手..... 18
 - 5.4 网络综合智能诊断（内置智能体） 18

5.5 AI 数据包分析	20
5.6 分析脚本智能生成.....	20
5.7 智能训练.....	20
5.8 智能体、技能与工具体系.....	21
5.9 竞争优势.....	22
六、产品架构.....	22
6.1 总体架构.....	22
6.2 智能中枢：贯通数据与应用的核心.....	23
6.3 数据流转：从数据接入到智能决策.....	24
6.4 安全保障体系.....	24
七、部署方案与资源准备.....	25
7.1 部署形态.....	25
7.2 软件环境要求.....	25
7.3 硬件资源参考.....	25
7.4 上线前资源准备清单.....	26
7.5 实施与初始化流程.....	27
7.6 运维与升级.....	28
八、典型应用场景与行业实践.....	28
8.1 七大典型智能场景.....	28
8.2 场景详解.....	29
8.3 行业实践方向.....	29
九、产品参数规格附录.....	30
9.1 数据模型规格.....	30
9.2 告警事件类型.....	30
9.3 建连失败 7 类根因	31
9.4 时延 5 维拆解.....	31
9.5 拨测任务类型（8 类）	31

9.6 通知渠道.....	31
9.7 认证方式.....	31
9.8 智能能力特性.....	32

版权声明

本文档版权归北京智维盈讯网络科技有限公司所有。未经书面许可，任何单位或个人不得以任何形式复制、传播、摘录本文档的全部或部分内容。

本文档所述产品功能基于灵眸智能监控系统 V2.5 版本实际实现编写，产品持续迭代，文档内容如有变更恕不另行通知。文中涉及的其他公司产品、商标及名称归各自所有者所有。

一、执行摘要

随着行业数字化转型进入深水区，核心业务系统大规模云化、微服务化，网络规模、应用类型与数据流向呈指数级增长。TCP 建链失败、业务时延异常、链路丢包、跨分区访问受阻等问题频发，传统以专家经验为核心、依赖人工下钻分析的故障处理模式，已难以满足业务连续性的严苛要求。

灵眸智能监控系统（英文名 NSMART，内部代号 ncompass smart engine）是北京智维盈讯网络科技有限公司面向数据中心、云原生及广域网场景打造的新一代 AIOps 智能网络运维平台。平台以“数据驱动的智能运维”为核心理念，将网络流量分析（NPM）、应用交付（ADC/灵珑）、主动拨测、云监控、CMDB 等多源数据统一汇聚，融合统计学算法、异常检测、机器学习与大语言模型（LLM），构建从告警感知 → 根因定位 → 处置建议 的端到端智能闭环。

灵眸的核心价值主张：

- **秒级故障感知、分钟级故障定位：**传统人工分析平均耗时 30 分钟至一周，智能分析平均仅需 1~5 分钟。
- **把图表翻译成人类语言：**系统直接告诉运维人员“发生了什么、原因是什么、如何解决”，极大降低使用门槛。
- **数据驱动而非记忆驱动：**大模型每次分析均实时注入拓扑、指标与告警上下文，结论具备时效性与数据支撑。
- **网络诊断深度行业领先：**支持 7 类建连失败根因分类、5 维时延深度拆解、拓扑路径还原 + 防火墙策略联动双维诊断。

- **智能能力可扩展、可管控：**提供智能体与领域分析技能的灵活扩展体系，支持以自然语言生成分析脚本，并对脚本进行规范约束与安全校验，保障分析过程可控、可审计。

本白皮书面向客户单位的技术负责人、网络与运维主管、架构师及评标专家，系统阐述灵眸的产品定位、功能体系、AI能力、产品架构、部署方案与资源准备，为产品选型、规划建设与项目落地提供参考。

二、行业背景与运维挑战

2.1 数字化转型带来的运维新挑战

行业数字化转型加速推进，越来越多关键业务和应用被部署到用户网络中，直接带来三方面变化：

1. **网络规模越来越大：**数据中心从传统三层架构向 Spine-Leaf、虚拟化、容器云演进，节点与链路数量激增；
2. **应用类型愈加复杂：**微服务拆分使一次业务交易涉及数十次服务调用，协议涵盖 TCP/IP、HTTP/HTTPS、DNS、Oracle 等；
3. **数据流向难以掌握：**业务在互联网接入区、DMZ 区、应用区、数据区之间纵向流转，并在多分区之间横向访问。

在业务流转发过程中，TCP 建链失败、业务流时延异常、链路丢包、访问被安全设备拦截等问题极易出现，给网络运维带来巨大挑战。如何**快速感知、准确定位、快速恢复**故障，有效提升运维效率，变得尤为重要。同时，为在复杂网络环境中实现业务精细化管理，**网络流量可视化**已成为明确趋势。

2.2 传统流量监控产品的局限

传统流量监控产品“难以用起来”，主要体现在：

- **监控逻辑复杂：**需要运维人员在大量曲线、表格之间自行判断关联关系；
- **对人员专业性要求极高：**只有极少数资深专家能够熟练使用；
- **部署与使用成本高：**耗费大量时间与精力，效果却难以保证；
- **告警噪音大：**固定阈值难以适应业务周期性波动，误报、漏报频发。

过去“以专家为核心”的故障处理模式，已难以应对种类繁多、瞬息万变的故障场景。

2.3 AIOps 智能化运维成为趋势

众多客户正在尝试以 **AI 算法 + 知识图谱 + 大模型** 的方式，开展智能化运维的探索与实践：

- 借助**基线学习**自动适应业务周期，减少误报告警；
- 借助**异常检测算法**快速发现指标突增突降；
- 借助**机器学习相关性分析**挖掘故障关联、自动生成标签；
- 借助**大语言模型**将复杂的监控数据转化为人类可读的结论与建议。

其目标是实现“机器的问题机器处理”，提升故障感知准确率与故障定位效率，把专家经验沉淀为平台可复用的智能能力。

2.4 来自一线的真实痛点

灵眸在产品的设计过程中，持续倾听客户不同角色的真实反馈：

角色	典型痛点
网络部门	"每天收到大量来自应用部门的故障分析需求——交易失败或响应慢，占用了大量时间与精力，如何提升效率？"
应用部门	"网络质量对我们是黑盒子。业务异常时，如何便捷地看到网络是否对业务交易产生了影响？"
数据中心领导	"如何提升 IT 支撑部门的检测与响应效率，主动发现故障、高效处理故障，实现秒级故障感知、分钟级故障定位？"

2.5 智能监控与传统监控的本质区别

对比维度	传统流量监控产品	灵眸智能监控产品
部署方式	复杂、耗时长	部署简单、逻辑清晰
人员要求	需极专业的专家	门槛低，普通运维即可使用
信息呈现	曲线、表格 Dashboard	转换为人类语言，直接告知现象与建议
告警机制	固定阈值，误报多	基线学习 + 异常检测，准确率高
分析耗时	30 分钟 ~ 一周	1 ~ 5 分钟
智能化	无	AI 算法 + 大模型，持续进化

三、产品概述

3.1 产品定位

灵眸智能监控系统是一款面向网络与云原生环境的 **AIOps 智能运维平台**。它并非简单的流量采集工具，而是在网络流量分析（NPM）等数据源之上构建的**智能分析与运维决策层**：

- **向下**：对接 NPM 网络流量分析、灵珑应用交付、NLC 数据接入、云监控、CMDB、主动拨测等多类数据源；
- **对内**：以统一对象模型和指标体系组织数据，运行告警引擎、异常检测与智能分析；
- **向上**：提供事件看板、智能分析、智能巡检、业务画像、AI 对话等应用，并支持大屏、自定义视图与开放接口。

3.2 核心理念

数据驱动的 AIOps——让每一次智能分析都建立在实时、可溯源的数据之上，而非依赖模型的静态记忆。

灵眸将大模型能力深度融入网络运维的**告警分析、拓扑诊断、自然语言交互、脚本自动化、智能巡检与模型训练**六大核心场景。

3.3 产品亮点

智能监控

基于**统计学算法、异常检测算法及机器学习算法**，结合人工标注能力，提升告警准确率、降低误报率。通过基线学习方式减少误报与错报，将重复劳动全部交给机器，大幅提升故障感知准确率与定位效率。

智能分析

通过对比历史数据模型，以异常检测算法为基础快速定位异常节点，对关键 KPI 进行深度分析，并结合**多维主因素（贡献度）算法**，输出机器分析的结论和建议。平台还提供易用的分析脚本编辑能力，让用户结合自身环境与使用场景，定制符合本部门需求的智能分析脚本，持续提升产品智能化能力。

智能分析"就医式"逻辑，形象清晰：

步骤	类比	说明
① 分诊台 — 挂	用户输入	分析谁？什么时间段？

号

- ② 血液科 — 验血

全指标检测

基于对象类型自动关联检测指标，全指标异常检测，生成"体检报告"
- ③ 会诊 — 分析

场景匹配

依据哪些指标同时突增突降，匹配系统预置场景库，得出诊断结果
- ④ 医嘱 — 结论

输出报告

提供现象、原因、后续建议及论证所需的相关数据

3.4 量化价值与收益

价值维度	传统方式	灵眸智能方式
单次故障分析耗时	30 分钟 ~ 一周	1 ~ 5 分钟
故障感知	人工巡检 / 用户报障	秒级自动感知
告警准确率	阈值告警，误报多	基线 + 异常检测 + 人工标注
使用门槛	依赖资深专家	普通运维自主分析
分析结论	图表，需自行解读	自然语言结论 + 处置建议
专家经验	存在个人脑中	沉淀为脚本 / 技能 / 智能体，团队共享

3.5 产品能力总览

灵眸平台由八大功能域与一套 AI 智能中枢构成：

灵眸智能监控系统 NSMART

└─ 全局搜索	统一入口，跨数据源检索 IP / 域名 / 应用 / 配置
└─ 告警中心	事件看板 · 对象管理 · 告警策略 · 告警统计 · 多渠道通知
└─ 智能分析	对象分析 · 即时拨测 · 场景分析 · 会话追踪
└─ 智能巡检	巡检报告 · 巡检任务 · 巡检策略
└─ 数据分析	流量 / 协议 / 云流量 / 拨测 / 灵珑 / 自定义视图 / 大屏
└─ 业务梳理	入向画像 · 出向画像 · 画像配置 · 应用定义
└─ AI 大模型	对话中心 · 智能体 · 技能 · 网络综合诊断 · 数据包分析
└─ 系统/用户中心	数据源 · 自动化 · 大模型管理 · 许可 · RBAC · 认证审计

四、核心功能体系

4.1 全局搜索

全局搜索是灵眸智能数据监控平台的集中、便捷数据查询与监控入口，帮助用户快速访问各类关键数据指标，及时掌握系统运行状态。

核心能力：

- **多数据视图切换：**支持"流量数据""业务日志""负载配置"三种视角。
 - 搜索"流量数据"需接入 NPM 数据源；
 - 搜索"业务日志""负载配置"需接入灵珑数据源。
- **多类型关键词检索：**支持 IP、端口、域名、应用名称、站点名称、视图、知识库脚本、告警策略、虚拟服务（VS）等。
- **数据概览卡片：**集中展示数据源、告警事件（当日 vs 昨日）、流量（流入/流出吞吐）、负载（设备数/VS 数/域名数）、日志（HTTP/DNS/Syslog 数量）、巡检事件、应用（响应时间/建连成功率）、拨测（告警数/任务数）等关键指标，支持一键下钻。
- **搜索历史：**自动保存本地检索历史，提升重复查询效率。

4.2 告警中心

灵眸对接 NPM 数据源，获取应用、站点、NFlow、VLAN、链路等多元对象，通过灵活配置告警策略实现数据实时监控与预警。

4.2.1 事件看板

将环形图、柱状图与数据表格结合，全面直观展示告警：

- **告警概览：**统计一段时间内对象告警、业务系统告警总数及监控对象总数；
- **告警分布 / 策略分布 TOP：**环形图展示告警最多的对象与策略 TOP，支持点击联动过滤；
- **告警趋势：**按小时/天/周分时段柱状图呈现告警数量变化与集中分布；
- **告警事件统计：**表格列出告警对象、策略名称、触发时间、持续时间、事件详情，支持筛选排序。

4.2.2 对象管理

NPM 数据源添加成功后，需在对象管理中添加监测对象，支持三级对象体系：

- **监控对象（单对象）：**网络（站点、VLAN、NFlow、链路管理）、应用、业务；支持**手动同步与自动同步**（按固定频率更新，需 NPM v2.5.204 及以上）；支持按名称、备注过滤勾选。
- **对象组：**应用组、站点组；手动添加需先添加监控对象（手动对象组不直接参与告警），自动方式可同步 NPM 的应用组与站点组。
- **业务系统：**支持手动配置（自定义名称、类型（互联网/分支机构）、数据中心、对象组层级）与自动获取（NPM 业务系统全套配置）。
- **智能分类（标签）：**根据监控对象历史数据相关性自动生成数据标签，方便后续使用与查看。

4.2.3 告警策略

对象添加完成后即可配置告警策略，系统内置常用策略模板，支持策略导入导出。

- **基础配置：**产品（NPM）、告警名称、模型、颗粒度、策略启停、告警压制、通知/回落通知服务器、消息模板、告警生效时间。
- **支持的数据模型：**TCP/IP、HTTP、HTTPS、DNS、ARP、TCP/IP 秒级、NFlow、链路管理、Oracle。其中 TCP/IP、ARP、NFlow、Oracle 默认为分钟级模型，其余默认为秒级模型。
- **颗粒度：**分钟级模型 60 秒；秒级模型 1/60 秒（1 秒颗粒度可能增加 NPM 负载，按需选择）。
- **告警规则：**支持**阈值、基线、异常度**三种监测方式，规则可多层嵌套；可按指标关联内置或自定义智能分析脚本。
- **对象配置与过滤维度：**按名称、备注、标签选择对象；可对对象进一步下钻（如"应用 = HTTP 应用 + 域名 = 错误!超链接引用无效。
- **AI 绑定：**每条策略可独立绑定 AI 智能体并启用/停用 AI 分析。

4.2.4 告警统计

按策略名称统计一段时间内告警触发总次数，用于策略优化。对触发偏高的告警可进行告警验证与策略优化，查看优化前后新增、减少、持续等类型数量，确认后可**一键更新告警策略**，形成"监控—评估—优化"闭环。

4.2.5 告警通知

支持接入多种通知服务器，并可自定义消息模板（支持告警名称、时间、详情、对象、指标、分析结论等参数）：

通知渠道

关键配置

邮件	服务器、端口（常为 465）、账号密码、TLS/SSL、多收件人
企业微信	企业 ID、自建应用密钥、应用 ID、部门/标签/接收用户（默认 @all）
钉钉	Webhook 机器人、手机号、是否通知所有人
飞书	Webhook、密钥、open_id、代理开关
Kafka	主题（Topic）、消息转发对接
Syslog（TCP/UDP）	主机、端口（默认 514）、UTF-8/GBK/GB2312 编码
HTTP / Restful API	请求地址、GET/POST 方法
短信	经由统一通知平台渠道扩展

通知发送类型：持续发送、触发发送（仅首条）、聚合发送（同策略多对象聚合为一条），并支持告警压制以降低噪音。

4.3 智能分析

智能分析包含对象分析、即时拨测、场景分析与会话追踪四大功能。

4.3.1 对象分析

基于 AI 算法与产品内置故障分析逻辑，实现告警事件自动化智能分析，用人类语言详尽表达分析结果，让所有人都能自主分析故障。

- 支持对**对象、业务系统、自定义对象**进行分析；
- 可选择分析的模型数据，配置时间范围（时间点/时间段），支持修改颗粒度，支持秒级模型；
- **知识库选择：**智能选择（系统按对象自动匹配脚本）与人工选择（多选脚本，多脚本结果汇总于同一报告）；
- 所有分析报告自动保存至**历史分析记录**，可追溯对象、时间与异常内容。

4.3.2 即时拨测

无需预先配置定时任务，可临时配置拨测源、拨测任务与拨测目标进行即时检测。任务结束后即释放，不占用拨测客户端资源，结果可进一步发起跟踪分析。

4.3.3 场景分析

针对**专线链路中断、路由器缺少路由、防火墙 Deny、交换机缺少路由**等典型场景匹配检测规则，输出分析报告，说明对象在何时发生何种异常，并给出建议与结论。

- **拓扑配置：**可视化绘制拓扑节点并命名场景；节点可配置名称、类型（客户端、防火墙、路由器、交换机、F5、分支机构、WAF、业务、SSL、其他）、监控节点方向、数据源、模型与维度过滤；支持业务流方向配置。
- **外联 NAT 关联：**防火墙/WAF 节点支持 NAT 关联，提供两种方式：
 - **流量方式：**在 NPM 端配置 NAT 前后关联，基于转换前后流量进行缝合分析；
 - **日志方式：**提供防火墙/WAF 的 NAT 日志，经 NLC 数据源解析后分析。
- **策略配置：**内置常规建连失败分析、设备自动诊断、丢包定位分析、时延定位分析等脚本，并支持自定义脚本策略。

4.3.4 会话追踪

面向网络故障排查与安全监测，按数据源时间范围、客户端 IP、服务端 IP 等条件筛选会话，通过总吞吐量、应用响应时间等判断传输是否正常，也可追踪特定 IP 发现短时间大量异常连接等安全威胁。点击单条会话可进一步"会话追踪"深度分析。

4.4 智能巡检

智能巡检可对互联网链路、广域网链路、外联链路等多类型链路，以及 TCP、HTTP、DNS、HTTPS 等协议应用进行定时检测，系统内置覆盖**用量、质量、异常、负载、性能**多维指标的巡检策略。

4.4.1 巡检报告

- 报告按天生成，日历颜色含义清晰：**黄色**（当日有异常）、**绿色**（正常）、**蓝色**（当前日期）；
- 卡片展示各任务巡检数据，黄色卡片代表发现隐患；隐患事件、巡检对象、检测规则均可点击跳转；
- 报告顶部呈现异常事件与异常对象 TOP 列表，下方表格默认仅显示异常数据，可切换"全部"查看完整指标。

4.4.2 巡检任务

巡检对象分两大类：

- **站点类：**互联网链路、广域网链路、外联链路、网络区域；
- **应用类：**TCP、HTTP、DNS、HTTPS 协议应用。

支持"每天"定时自动生成报告，以及"自定义时间"批量生成多份报告。

4.4.3 巡检策略

默认策略可修改、删除，也可自定义新增：

- **链路检测：**负载均衡状况、丢包率、传输时延、SYN 扫描、建连失败率、大小包占比等；
- **应用检测：**流量大小、新建连接数、访问量、建连时间、应用响应时长、服务端重置、源端口复用等；
- 各指标阈值均可灵活调整。

4.5 数据分析

数据分析提供全面深入的网络链路、应用性能、协议、云流量、拨测、灵珑负载数据分析能力，并支持自定义视图、表格与大屏。

4.5.1 流量分析

- **链路分析：**以站点、VLAN 为核心维度，分析吞吐量、时延、丢包率、建连成功率、新建会话数、应用响应时间与超时；
- **IP 分析：**以 IP 为维度的性能与质量评估，支持服务端/客户端双视角查看访问详情；
- **应用分析：**汇总新建会话、丢包、建连时间、响应时间，可视化呈现客户端访问到服务端返回各阶段指标及趋势。

4.5.2 协议分析

- **DNS：**层级表格、单值及趋势图呈现服务端 IP 与域名访问量、请求率、无响应次数、平均响应时间；
- **HTTP：**分别剖析请求与响应，涵盖访问量、请求率、成功率、响应时间、响应码分布（2xx/3xx/4xx/5xx）及慢响应。

4.5.3 云流量分析

云平台对接完成后，可查看资产分析（容器、云平台）、IP 分析、DNS、HTTP、NAT 会话、日志分析、事件分析，并可切换原始包、黄金指标、NPM-云模型查看更详细数据。

4.5.4 数据表格

内置应用、站点、通讯对、HTTP、DNS、会话数据表格，与全局搜索互联，精准过滤关注流量。

4.5.5 拨测分析

按 Ping、Telnet、HTTP、HTTPS、DNS、Traceroute、UDP、WebSocket 八种类型分类查看。卡片展示任务概览（绿色正常、红色异常），详情页以柱状图 + 表格展示成功/失败/告警，支持时间滑动联动、指标双击出曲线、多指标对比，并可查看含拨测拓扑的跟踪分析报告（异常节点红色标记，支持自定义拓扑）。

4.5.6 灵珑负载数据分析

接入灵珑数据源后，左侧列出负载应用，可查看应用的配置、流量、服务、日志等详情。

4.5.7 自定义视图与大屏

内置 NPM-流量分析视图与标准数据表格，支持自定义创建视图、表格、大屏：

- **图表类型：** 曲线图、条形图、柱状图、仪表盘、地图、饼图、环图、表格等；
- **多组件联动：** 一个视图可添加多个组件并相互关联，实现数据联动；
- **导入/导出：** 支持视图 JSON 在线导入导出与数据源映射。

4.6 业务梳理

生产环境网络分区通常采用"纵向分层、横向分区"模式，业务访问流程经过多个分区的多台应用交付设备。灵眸提供清晰、可自助查询的**应用访问路径与业务访问关系画像**，帮助运维人员理解业务访问关系、评估故障影响范围。

4.6.1 两类业务画像

- **互联网业务（入向画像）：** 输入业务域名，即可列出域名对应的业务地址，以及从互联网接入区到 DMZ 区访问关系的关键路径，实现以业务为单位的互联网路径梳理；相关配置详情可一键导出。
- **内网业务（出向画像）：** 通过采集高速日志并结合 CMDB 信息，描绘内网业务模块之间的访问关系，帮助理解调用关系与某服务故障的影响范围。

4.6.2 数据依赖与初始化

业务梳理属消费数据模块，需对接以下数据源：

数据源	作用
灵珑数据源	拉取负载配置（DNS 配置、VS 数据）
画像配置（内置）	管理防火墙、WAF、Nginx 等设备配置，支持手工/自动/批量添加

云产品数据源	拉取云/容器环境配置（按需）
NPM 流量分析平台	获取应用/应用组流量分析指标（需提前部署）

4.6.3 画像配置内容

业务画像依赖核心网络与资产配置数据，关键配置表包括：

配置表	作用
DNS 域名	设备域名与 IP 映射，识别业务入口与服务依赖
NAT 映射	公网 IP/端口与内网转换规则，定位真实后端
负载 / 加解密设备	灵珑未覆盖的负载与加解密设备接入
应用网关	Nginx、Tomcat、中间件、数据库等，映射流量枢纽
LLDP	设备间物理连接拓扑，构建物理网络拓扑
接入交换机	梳理交换机与服务器连接关系
NPM 连接表	补充 Nginx 与下层 App 连接关系
路由表 / CMDDB	路由转发规则与设备资产属性

各类配置均支持**手动录入**、**批量导入/导出（标准 Excel/CSV 模板）**与**脚本自动化对接**（单次/每分钟/每小时/每天/每周定时更新）。目前自动化对接支持 F5、深信服、信安世纪、迪普、神州云科、山石、弘基、飞塔等主流厂商设备。

4.6.4 应用定义与画像视图

- **应用定义：**完成业务系统更新后，可将业务系统包含的 VS 一键定义并同步至 NPM 与灵眸，规则涵盖协议类型、应用名称、应用组名称；定义完成后即可在拓扑中查看流量数据。
- **画像视图：**每个域名可查看视图、立即更新、下拉查看业务详情；视图包含告警事件、应用检测表与应用拓扑。
 - **告警事件：**近一个半小时告警分布柱状图与详情表，支持在线智能分析；
 - **应用检测：**各层级应用指标表，异常数据自动标黄，支持上下层/路径分析与多层级对比；
 - **应用拓扑：**可视化展示 VS、Pool 等节点连接关系，支持按数据中心、IP 类型、云模型筛选，点击节点查看配置、资源、趋势、路径分析与数据表格。

4.6.5 工作原理

业务梳理模块首先从灵珑拉取负载配置，启动应用定义解析业务系统的层级关系与虚拟服务并标准化，推送至 NPM；同时将业务系统同步到灵眸对象管理，由灵眸主动拉取各对象流量指标并运行分析算法，最终以图形化方式呈现在画像拓扑中，形成**"配置拉取 → 应用定义 → 数据同步 → 智能分析 → 拓扑呈现"**的完整链路。

4.7 系统与用户中心

4.7.1 数据管理与数据接入

- **数据管理**：添加、编辑、删除数据源（NPM/灵珑），支持连通性测试；配置 URL、TOKEN、序号及云服务/拨测/大屏可用性开关。
- **数据接入（NLC）**：接入日志、配置、CMDB 等第三方数据；数据模型分指标模型与配置模型两大类。

4.7.2 系统管理

- **产品管理**：展示各模块路径、版本、简介，支持页面启停/重启服务、查看运行状态与日志；
- **产品升级**：页面上传安装/升级包，无需登录底层即可升级并输出安装日志、提供升级验证；
- **系统配置**：页面配置 NTP 时间同步与 DNS 解析，无需底层重启。

4.7.3 系统维护

提供系统日志、操作日志、性能监控（实时监控 CPU/内存/网卡/硬盘及各服务占用）、路由配置、参数配置（NCD 网关、灵珑地址、NPA 地址等）、事件中心（低/中/高三级，含影响与解决方式）、通知记录、基线排除（内置法定节假日/调休，可自定义工作日）、异常检测规则配置、LOGO 自定义更换等。

4.7.4 用户与权限

- **用户管理**：用户列表、新增/编辑/删除、启停、密码修改；
- **权限管理（RBAC）**：按产品模块与数据范围授权；
- **认证管理**：支持本地认证、企业微信、第三方协议（RADIUS、TACACS、LDAP）、单点登录 SSO；可配置验证码、密码强度、最大登录次数、IP 黑白名单；
- **登录日志与审计**：记录登录时间、IP、系统、方式，支持行为追溯。

4.7.5 许可授权与其他

- **许可授权：**依据设备机器码申领激活码，按功能需求与数据类型授权，可查看机器码、序列号、许可时长、有效期与许可详情；
- **云监控：**配置云平台账号等信息；
- **代理服务器：**支持配置代理，满足访问限制、安全与负载均衡需求。

五、AI 大模型智能能力

5.1 AI 能力总览

灵眸平台（NSMART）以"数据驱动的 AIOps"为核心理念，将大模型能力深度融入网络运维的**告警分析、拓扑诊断、自然语言交互、脚本自动化、智能巡检与模型训练**六大核心场景，实现从告警感知 → 根因定位 → 处置建议的端到端智能闭环。

能力模块	功能定位	触发方式
智能告警根因分析	告警事件关联大模型，自动输出根因与处置建议	告警看板一键触发
业务拓扑 AI 分析助手	结合业务拓扑与实时指标，进行链路根因定位	拓扑视图嵌入式启动
AI 大模型对话中心	自然语言交互、智能体管理、可扩展技能	独立功能页面
网络综合智能诊断	多场景自动路由，覆盖 IP/站点/应用/通讯对	内置预置智能体
AI 数据包分析	网络报文级自然语言问答	数据包分析助手
分析脚本智能生成	自然语言 → 可执行分析脚本	脚本生成助手
智能巡检	定时/手动巡检，自动生成含拓扑链路分析的报告	任务调度 / 手动
智能训练	时序相关性分析与自动标签，优化异常检测	后台轮询执行

5.2 智能告警根因分析

在告警策略中开启 AI 分析并选择适配的分析智能体；告警触发后，运维人员在告警看板点击事件，系统即自动汇集相关信息并给出分析结论，同时支持就该问题持续追问。

能力项	说明
信息自动汇集	自动提取告警对象、异常指标详情与关联下钻数据，无需人工整理

策略关联智能体	每条告警策略可独立选择适配的分析智能体，不同业务场景采用专属分析逻辑
汇集信息范围	告警对象（虚拟服务、云原生工作负载等）、异常指标变化描述、多维性能指标（吞吐/时延/建连成功率/应用响应时间等）及相关事件日志
告警事件识别	自动识别突增、突降、基线上偏离、基线下偏离、阈值上越限、阈值下越限等异常类型
多轮追问	支持围绕同一告警持续提问、逐层深入
启用控制	可按告警策略单独开启或关闭 AI 分析

分析过程：系统依据告警类型自动匹配适配的分析智能体 → 汇集相关指标与图表 → 整理为完整的分析背景 → 由智能体输出根因判断与处置建议，全程实时呈现。

5.3 业务拓扑 AI 分析助手

嵌入在业务系统拓扑视图右侧的 AI 对话助手，自动拉取当前业务拓扑画像作为背景上下文，引导大模型完成链路异常根因定位，并将根因结果以列表形式回写前端视图。

能力项	说明
画像信息自动汇集	自动汇集当前业务的拓扑链路、节点分组、应用检测数据及告警节点详情（指标、配置、日志、资源信息）
自动发起分析	打开助手即自动开始分析，无需人工输入
分析范围	可按指定时间范围分析对应时段的拓扑链路异常
多轮交互	初步分析后可持续追问、深入诊断
结果呈现	智能分析定位的异常节点直接在拓扑视图中高亮展示
时间变更提醒	调整时间范围后，系统自动提醒重新发起分析

5.4 网络综合智能诊断（内置智能体）

平台内置网络综合分析智能体，可根据用户的自然语言描述自动识别分析场景，并匹配相应的标准化诊断流程，输出结构清晰的分析报告。

5.4.1 场景自动识别

用户只需用日常语言描述问题，系统即可自动判断应采用的分析方式：

输入特征	自动进入的分析场景
包含两个 IP（可含端口）	通讯对网络排障

五元组（源 IP:端口 → 目的 IP:端口）	通讯对网络排障
"站点"关键词 / 站点名称	站点异常分析
"应用"关键词 / 应用名称	应用异常分析
单 IP + 端口号	IP:端口异常分析
单 IP 地址	IP 异常分析

当描述存在歧义时，智能体会自动检索并列出候选对象请用户确认，不凭猜测下结论。

5.4.2 诊断能力矩阵

诊断能力	说明
多维流量指标分析	总吞吐量、流入/流出吞吐量、丢包率（客户侧/服务端）、网络时延、新建会话数、建连失败率、应用响应时间，共 10 项核心指标
7 类建连失败根因	服务端无响应、服务端重置、源端口复用、客户端重试不足、异常 SYN、异常 SYNACK、服务端队列不足
5 维时延拆解	建连时间、应用响应时间、网络 RTT（客户侧/服务端）、重传时延、小窗口时延
渐进式时间缩放	大跨度查询自动多级缩放（全周期→天→小时→分钟），定位异常时段后下钻
应用层协议分析	TCP/IP 建连诊断、HTTP 异常请求、DNS 解析异常
拓扑路径追踪	还原完整路径（含无采集点中间设备），识别 NAT 转换节点
防火墙策略联动	自动查询沿途防火墙/应用防护策略，判断访问放行或阻断，给出策略名称与原因
多维下钻	按应用、通讯端口、客户端 Top-N 下钻，识别高异常贡献者
数据包下载建议	定位到异常通讯对但无法完全确定根因时，引导报文级分析

5.4.3 诊断报告规范

- **结构清晰：**依次呈现结论、指标概览、异常分析、拓扑路径分析及优化/进一步分析建议；
- **路径可视化：**报告以图形化方式直观展示流量路径、设备类型及监测点状态；
- **关联分析引导：**报告尾部自动推荐相关分析入口，可一键跳转继续深入。

5.5 AI 数据包分析

面向网络抓包数据分析场景，用户可用日常语言向 AI 助手提问，无需了解专业协议细节。

- **典型问题：**"是否存在网络攻击？""列出值得注意的异常事件""客户端访问中断，分析原因""应用响应缓慢，是网络还是应用原因？"
- **上下文自动感知：**自动获取当前分析对象的网络连接信息（IP、端口、协议）、数据包信息、抓包文件名以及统计数据（包数、字节数、时延、丢包）。

5.6 分析脚本智能生成

用户只需用自然语言描述分析需求，系统即可自动生成可在平台内运行的分析脚本，并在安全校验通过后执行、返回结论。

能力项	说明
输入方式	自然语言描述（如"分析过去一小时 HTTP 5xx 错误的来源分布"）
脚本规范	生成的脚本遵循平台统一规范，结构完整，必须包含结论输出
内置分析模板	提供丰富的分析模板，覆盖突增检测、基线对比、维度下钻、贡献度分析、TCP 建连失败、HTTP 5xx/4xx、流量突增等常见场景
安全校验	对生成脚本自动进行语法、结构与安全性检查，拦截危险操作
受控执行	所有脚本在平台受控环境内运行，不可访问无关文件或网络
多轮调整	支持在对话中持续提出修改意见，逐步完善脚本

5.7 智能训练

后台智能训练服务基于时序数据进行相关性分析，自动计算指标间相关性系数并生成标签，辅助异常检测模型优化。

参数项	规格
任务管理	创建/编辑/删除，支持立即执行与定时执行
时间范围	自定义，预设最近一周/两周/一月
相关性分析	自动计算指标间相关系数，可按高/中/低三级敏感度进行分析
自动标签	根据分析结果自动生成指标标签，可独立启停
状态管理	未执行→执行中→完成/失败；支持停止中/停止成功/停止失败
进度与结果	实时进度（0-100%），输出对象维度相关系数与标签

5.8 智能体、技能与工具体系

5.8.1 智能体

智能体是平台中承载特定分析职责的 AI 角色。用户可根据运维需要自定义智能体的分析视角、关注的指标范围与分析深度，并将其关联到相应的告警策略，实现"不同告警场景 → 专属分析策略"的精细化管理。平台提供智能体的创建、编辑、删除与卡片化管理，内置覆盖 DNS、TCP、HTTP 等常见场景的预设智能体；在配置智能体时，还可借助 AI 辅助优化其分析口径。

5.8.2 分析技能

分析技能是智能体可调用的专项分析能力，用于将某一类排障经验固化为标准流程。智能体在处理问题时按需调用相应技能，严格遵循既定分析步骤，避免凭记忆跳步。

全生命周期管理：支持通过对话快速创建技能、在线编辑、规范校验、能力评测、发布与版本回溯、导入导出，以及启用/停用，使用户可像管理业务资产一样管理分析技能。

技能评测：上线前可为技能配置测试用例，由系统在独立环境中真实执行并依据实际表现评分，支持量化通过率、历史轮次对比及"使用/不使用该技能"的效果对比，帮助用户在发布前验证质量、防止能力回退；评测意见可直接反馈给 AI 进行迭代优化。

内置分析技能：

技能	适用场景
告警分析	基于告警上下文执行根因分析，输出结构化报告
网络诊断	通讯对/五元组排障，拓扑路径与防火墙策略检查
IP 分析	单 IP/IP:端口流量分析、7 类建连失败诊断、5 维时延拆解、协议分析、路径追踪
应用分析	应用/域名性能分析、响应时间拆解、建连诊断、时延多维分析
站点分析	站点流量、丢包、时延分析及 Top 应用/客户端/服务端排查
VLAN 分析	出口链路异常、流量突变、疑似攻击检测、域名溯源
负载成员分析	负载均衡虚拟服务/成员两侧对比，定位异常成员

单个智能体可同时调用多个技能协同工作，例如网络综合分析智能体可协调 IP、应用、网络诊断、站点等多项技能，完成跨场景的复杂诊断。

5.8.3 工具与外部能力集成

平台为智能体提供数据查询、拓扑追踪、防火墙策略检查等一系列可调用的分析工具，同时支持通过标准化方式接入客户环境中的外部工具与服务，持续扩展 AI 的分析边界，且所有工具调用均在授权范围内进行。

5.9 竞争优势

5.9.1 与通用 AI 助手的差异

- **数据驱动而非记忆驱动：**每次分析实时注入平台拓扑、指标与告警上下文，结论具备时效性与数据支撑；
- **结构化上下文注入：**自动组装告警维度、历史指标、关联拓扑，无需手动粘贴数据；
- **业务感知场景路由：**依据 IP/站点/应用/通讯对/五元组自动路由专属流程。

5.9.2 网络诊断深度

- **7 类建连失败分类：**多数平台仅提供"建连失败率"单一指标，灵眸可精确定位故障层；
- **5 维时延拆解：**精准区分网络侧与应用侧故障，避免误判；
- **拓扑 + 防火墙联动：**形成"流量路径 + 策略"双维诊断。

5.9.3 可扩展与安全可控

- **经验轻松沉淀：**资深工程师的排障经验可便捷地固化为分析技能，无需开发介入；
 - **全生命周期管控：**提供技能的可视化创建、评测、发布、版本管理与团队共享；
 - **分析过程安全：**自定义脚本需通过平台规范约束与多重安全校验，并在受控环境内运行，确保安全合规；
 - **数据使用可控：**智能分析所使用的拓扑与指标由平台统一整理后提供，AI 不直接接触底层数据库。
-

六、产品架构

6.1 总体架构

灵眸采用**分层解耦、多源汇聚、智能中枢**的产品架构。系统自下而上完成多源数据的接入与智能分析，自上而下面向用户实现业务呈现与运维决策，整体可划分为五个逻辑层次，如下图所示。



层次	面向用户的能力
智能应用层	全局搜索、告警看板、智能分析、智能巡检、业务画像、可视化大屏、自定义视图/报表、AI 对话中心
智能中枢层	告警引擎、对象与标签统一管理、巡检调度、画像服务、主动拨测、分析上下文智能组装
AI 智能能力层	智能体与智能路由、领域分析技能、根因分析（建连失败 / 时延拆解）、分析脚本生成、数据包智能解读
大模型与算法层	主流大模型灵活接入、异常检测算法、智能基线学习、相关性分析训练、私有知识增强
数据接入层	NPM 网络流量分析、灵珑应用交付、云监控（云/容器）、主动拨测、CMDB 资产配置、第三方日志/配置

6.2 智能中枢：贯通数据与应用的核心

智能中枢层是灵眸产品架构的核心，承担"承上启下"的关键作用，对用户体现为以下能力：

- **统一告警引擎：**集中运行所有监控策略，支持阈值、基线、异常度多种检测方式，自动抑制告警噪音；
- **对象与标签统一管理：**以统一模型组织应用、站点、链路、业务系统等监控对象，并基于历史数据自动生成分类标签；
- **巡检调度：**按计划自动发起巡检任务并生成报告；
- **画像服务：**自动构建互联网与内网业务访问关系画像；
- **主动拨测：**调度分布式监测点，对目标进行多协议主动探测；
- **分析上下文智能组装：**在发起 AI 分析时，自动汇聚告警对象、异常指标、关联拓扑与下钻数据，无需人工整理。

6.3 数据流转：从数据接入到智能决策

以一次典型的告警智能分析为例，灵眸的产品数据流转路径如下：

1. **数据接入：**从网络流量分析、应用交付、云监控、主动拨测、CMDB 等来源汇聚数据；
2. **对象统一：**将监控对象与业务系统纳入统一管理；
3. **实时检测：**告警引擎按策略对指标进行实时监测，命中后生成告警事件；
4. **上下文汇聚：**系统自动汇聚与该事件相关的对象、指标与拓扑信息；
5. **智能分析：**大模型与分析技能基于实时上下文输出根因判断与处置建议；
6. **结果呈现：**分析结论实时呈现，根因节点在拓扑中高亮，并自动保存分析报告；
7. **告警触达：**按用户配置，通过邮件、企业微信、钉钉、飞书等多种渠道及时通知相关人员。

6.4 安全保障体系

灵眸从数据、权限、分析与认证四个方面，为用户构建完善的安全保障能力：

- **数据安全：**AI 分析所使用的拓扑与指标数据由平台统一整理后提供，AI 不直接接触底层数据库，敏感数据可控；
 - **权限管控：**支持按功能模块与数据范围进行精细化授权，不同角色看到不同内容；
 - **分析安全：**平台对自定义分析脚本进行规范约束与安全校验，所有分析在受控环境内运行，防止危险操作；
 - **认证安全：**支持本地认证、企业微信、第三方认证（RADIUS、TACACS、LDAP）及单点登录（SSO），并提供验证码、密码强度策略、登录次数限制与 IP 黑白名单；
 - **审计追溯：**操作日志、登录日志、通知记录与系统事件全程留痕，支持行为审计与责任追溯。
-

七、部署方案与资源准备

本章面向技术与运维负责人，说明灵眸系统的部署形态、环境要求与上线前需准备的资源，为项目规划与实施提供依据。以下资源规格为通用参考，实际配置应结合**监控对象规模、数据源数量、数据保留周期及是否本地化部署大模型**进行评估，建议在项目勘察阶段由双方共同确认。

7.1 部署形态

灵眸支持**一体化部署**与**分布式部署**两种形态，可根据网络规模和运维要求灵活选择：

部署形态	说明	适用场景
一体化部署（单机/单节点）	平台各功能组件集中部署于一台设备，开箱即用	小规模环境、POC 测试、分支机构
分布式部署	平台按功能分层部署、多节点协同，支持随规模扩展	中大型数据中心、高并发生产环境
大模型独立部署	大模型可独立部署于客户环境，也可使用外部模型服务	数据安全要求高、需离线运行

平台采用标准化交付，部署过程简便，支持主流及国产化硬件与操作系统平台。

7.2 软件环境要求

类别	要求 / 说明
客户端浏览器	推荐 Chrome 浏览器（访问地址 https://管理地址/nsm ）
操作系统	支持主流 Linux 发行版及国产化操作系统
时间同步	建议配置 NTP 时间同步（系统页面可直接配置）
名称解析	按需配置 DNS 解析（系统页面可配置）
运行环境	平台所需运行环境与数据存储均随产品内置，无需单独采购

7.3 硬件资源参考

下列为**平台软件自身**运行所需的参考规格，不含 NPM 探针、灵珑设备及独立大模型推理集群的资源。

7.3.1 一体化 / POC 环境

资源	参考规格
CPU	8 核及以上

内存	32 GB 及以上
系统盘	200 GB 及以上 SSD
网络	千兆及以上

7.3.2 生产环境（中等规模参考）

资源	参考规格
平台应用节点	8 核 CPU / 32 GB 内存 / 100 GB SSD，可按多节点扩展
智能分析节点	8 核 CPU / 32 GB 及以上内存 / 100 GB SSD
数据存储节点	8 核 CPU / 32 GB 内存 / 500 GB 及以上 SSD（依数据保留周期调整）
网络	千兆 / 万兆

7.3.3 本地大模型推理（如启用）

若出于数据安全性与合规考虑，选择**私有化本地部署大模型**，需额外准备 GPU 推理资源。灵眸不绑定特定模型，具体资源依据所选模型参数规模与量化方式评估：

项目	参考要求
GPU	建议采用具备充足显存的企业级 GPU；模型参数规模越大，所需显卡数量/显存越高
显存 / 内存	依所选模型参数规模与量化方式评估
存储	模型权重通常需数十 GB 至数百 GB，视具体模型而定
说明	也可采用外部大模型服务，无需本地 GPU

模型无关（Model-Agnostic）设计：灵眸采用业界主流的标准化大模型接口，可灵活接入公有云大模型服务、国产大模型或私有化部署模型，客户可依据数据安全策略、算力条件与成本自主选择。当模型迭代升级或需要更换时，无需改造平台即可平滑切换，从而保护既有投资、持续享受模型能力升级带来的收益。具体兼容模型清单以最新版兼容性说明为准。

7.4 上线前资源准备清单

项目启动前，建议客户方按以下清单提前准备，以保障实施进度：

7.4.1 基础设施

- 分配服务器/虚拟机资源（CPU、内存、磁盘、网络），或可用的容器平台；
- 规划管理 IP、访问端口与网络策略（开放客户端到平台的访问）；

- ☐ 提供 NTP 时间源、DNS 解析；
- ☐ 如需本地大模型，准备 GPU 资源或确定外部模型 API。

7.4.2 数据源与对接信息

数据源	需准备信息	是否必需
NPM 网络流量分析	管理地址（URL，默认 8088 端口）、TOKEN；建议版本 ≥ v2.5.204（支持自动同步）	流量监控必需
灵珑应用交付	管理地址、TOKEN；如与灵眸非同机部署需提供其 IP	负载/画像场景需要
NLC 数据接入	日志、配置、CMDB 等数据源及脚本	按需
云监控	云平台账号、访问密钥	云环境按需
CMDB	资产信息或对接接口	按需
拨测客户端	拨测程序安装位置（分布式监测点）、客户端网络策略	拨测场景需要

7.4.3 通知与认证

- ☐ 告警通知渠道信息：邮件服务器、企业微信（企业 ID/密钥/应用 ID）、钉钉/飞书 Webhook、Kafka、Syslog 接收端或 Restful API；
- ☐ 认证方式确认：本地认证，或企业微信 / RADIUS / TACACS / LDAP / SSO 对接参数；
- ☐ 用户角色与权限规划。

7.4.4 许可授权

- ☐ 设备首次安装后生成**机器码**；
- ☐ 根据功能需求与数据类型向厂家申领**激活码（序列号）**；
- ☐ 确认许可时长、有效期与授权模块。

7.5 实施与初始化流程

平台标准上线流程如下，初始化配置仅需在首次登录时完成：

- 设备安装 → 申请并导入激活码 → 登录系统（Chrome）
- 配置数据源（NPM/灵珑，连通性测试）
 - 同步监控对象 / 对象组 / 业务系统
 - 配置告警策略与通知服务器
 - （按需）拨测配置 / 云监控 / 画像配置 / 应用定义
 - （按需）接入大模型并导入知识库

- 配置智能巡检任务
- 系统正式运行

关键初始化步骤说明：

- 数据源配置：**在"系统设置 → 数据管理"添加数据，填写名称、产品、URL、TOKEN 及云服务/拨测/大屏可用性，完成连通性测试后保存；
- 对象导入：**在"告警中心 → 对象管理"选择手动或自动方式导入网络、应用、业务对象及对象组、业务系统；
- 策略与通知：**配置告警策略（模型、规则、对象）与通知服务器，完成后系统即开始实时监控。

7.6 运维与升级

- 页面化产品管理：**可在页面启停、重启服务模块，查看运行状态与日志；
- 一键升级：**上传安装/升级包即可完成升级，无需登录底层，输出安装日志并提供升级验证；
- 系统监控：**实时监控 CPU、内存、网卡、硬盘及各服务资源占用；
- 备份维护：**支持系统数据备份与维护操作。

八、典型应用场景与行业实践

8.1 七大典型智能场景

场景	输入	AI 处理流程	输出
告警根因快速定位	告警事件（ID）	获取告警上下文 → 创建分析会话 → 多轮追问	根因判断 + 处置建议
业务链路异常诊断	业务系统 + 时间范围	获取拓扑画像 → AI 分析链路异常节点 → 输出根因列表	异常节点高亮 + 根因报告
通讯对不通排障	源 IP + 目的 IP + 端口	查找监控点 → 路径还原 → 防火墙策略查询 → 建连失败分类	路径图 + 策略结论 + 根因
应用响应慢分析	应用名称	流量分析 → 趋势分析 → 5 维时延拆解 → 协议层分析	时延瓶颈层 + 原因 + 建议
自定义脚本生成	自然语言需求	模板生成脚本 → 安全校验 → 平台执行	分析脚本 + 执行结论

网络健康 巡检	巡检任务 + 策略	自动采集 → 风险评级 → 结构化报告	巡检报告（PDF 导出）
指标相关 性训练	模型 + 指标 + 时 间	时序采集 → 相关性计算 → 自动标签	相关系数 + 标签 数据

8.2 场景详解

8.2.1 通讯对网络排障

运维人员输入源 IP、目的 IP 与端口，系统自动：查找沿途流量监控点 → 还原完整拓扑路径（含无采集点设备与 NAT 节点）→ 查询路径上防火墙/WAF 策略是否拦截 → 对建连失败进行 7 类根因分类。最终输出完整路径图、策略检查结论与明确定位，将原本需多人协查数小时的问题压缩到数分钟。

8.2.2 应用响应慢分析

输入应用名称，系统先进行整体流量与趋势分析，再将总响应时间拆解为建连时间、应用响应时间、网络 RTT、重传时延、小窗口时延 5 个维度，精准区分"网络慢"还是"应用慢"，并下钻到 HTTP/DNS 协议层定位具体原因，给出优化建议，避免网络与应用团队之间责任不清。

8.2.3 业务健康度主动巡检

配置每日巡检任务后，系统自动对互联网/广域网/外联链路及关键应用进行用量、质量、异常、负载、性能多维检测，按天生成报告。管理者可通过日历视图快速识别异常日期，运维人员可直接下钻隐患明细，实现从"被动响应"向"主动发现"转变。

8.2.4 互联网业务路径梳理

输入互联网业务域名，系统自动呈现从互联网接入区到 DMZ 区的关键访问路径与业务地址，贯通 DNS 解析、负载均衡 VS、防火墙 NAT 等配置，帮助运维人员快速理解业务对外暴露面与端到端链路，并可一键导出配置。

8.2.5 内网调用关系与影响分析

系统结合高速日志与 CMDB，自动描绘内网业务模块间的调用关系。当某服务故障时，可直观评估其上下游影响范围，支撑微服务架构下的变更评估与故障研判。

8.3 行业实践方向

灵眸的多源数据融合与智能分析能力，可广泛应用于对网络稳定性与业务连续性要求较高的行业：

行业	典型应用方向
金融（银行、证券、保险）	核心交易系统网络质量保障、外联链路监控、秒级故障感知、等保合规审计
政府 / 公共事业	电子政务外网、数据中心网络可视化、国产化环境智能运维
能源（电力、石化）	跨地域广域网链路质量监控、关键业务保障（如供电局网络性能分析）
大型企业 / 制造	集团多分支机构链路巡检、数据中心与多云环境统一监控
运营商 / 数据中心	多租户流量分析、应用交付可视化、容量规划与成本分析

平台支持**大屏可视化**集中展示网络运行态势，并可针对行业客户需求进行定制化交付，灵活适配差异化运维场景。

九、产品参数规格附录

9.1 数据模型规格

模型	默认颗粒度	说明
TCP/IP	分钟级（60 秒）	建连、吞吐、时延、丢包等核心指标
TCP/IP 秒级	秒级（1/60 秒）	秒级流量监控
HTTP	秒级	请求响应、响应码、慢响应
HTTPS	秒级	加密站点可用性与性能
DNS	秒级	域名解析可用性与效率
ARP	分钟级	地址解析异常
NFlow	分钟级	流记录分析
链路管理	分钟级	链路状态与质量
Oracle	分钟级	数据库访问性能

9.2 告警事件类型

支持 6 类事件自动识别与分类：

1. 指标突增
2. 指标突降

3. 基线上偏离
4. 基线下偏离
5. 阈值上越限
6. 阈值下越限

9.3 建连失败 7 类根因

1. 服务端无响应
2. 服务端重置
3. 源端口复用
4. 客户端重试不足
5. 异常 SYN
6. 异常 SYNACK
7. 服务端队列不足

9.4 时延 5 维拆解

1. 建连时间
2. 应用响应时间
3. 网络 RTT（客户侧 / 服务端）
4. 重传时延
5. 小窗口时延

9.5 拨测任务类型（8 类）

Ping、端口探测（Telnet）、HTTP、HTTPS、DNS、Traceroute（ICMP/UDP）、UDP、WebSocket。支持 1 秒 ~ 1 小时频率配置、可用性判定、告警压制、智能分析关联与拓扑关联。

9.6 通知渠道

邮件、企业微信、钉钉、飞书、Kafka、Syslog（TCP/UDP）、HTTP/Restful API、短信（平台扩展）。发送类型支持持续、触发、聚合。

9.7 认证方式

本地认证、企业微信、第三方协议（RADIUS、TACACS、LDAP）、单点登录 SSO。安全能力含验证码、密码强度检测、最大登录次数、IP 黑白名单、登录日志审计。

9.8 智能能力特性

能力维度	特性说明
大模型接入方式	采用业界主流标准化接口，支持接入公有云大模型服务、国产大模型或私有化部署模型，可平滑切换与升级
模型兼容性	模型无关设计，不绑定特定厂商或版本；具体兼容清单以最新版兼容性说明为准
交互方式	支持自然语言多轮对话与流式输出，分析结论实时呈现
分析触发	告警一键分析、拓扑视图嵌入分析、对话中心主动提问、定时巡检
智能体管理	提供创建、编辑、删除与卡片化管理，内置多类网络场景预设智能体，支持AI辅助优化分析口径
分析技能	支持技能的对话式创建、在线编辑、规范校验、能力评测、发布与版本回溯、导入导出及启停
分析脚本	自然语言生成平台分析脚本，覆盖突增检测、基线对比、维度下钻、贡献度分析等常见场景
脚本安全	生成脚本自动进行语法、结构与安全性检查，在受控环境内运行，拦截危险操作
内置分析能力	告警根因分析、网络诊断、IP/应用/站点/VLAN分析、负载均衡虚拟服务与成员分析等
数据安全	分析所用拓扑与指标由平台统一整理后提供，AI不直接访问底层数据库
能力扩展	支持以标准化方式接入客户环境中的外部工具与服务，持续扩展分析边界，调用均在授权范围内进行

灵眸智能监控系统 NSMART

数据驱动·智能感知·分钟级定位

北京智维盈讯网络科技有限公司

本白皮书内容基于灵眸智能监控系统V2.5版本实际功能编写，所述能力均有相应功能代码支撑。