智维数据
Intelligent Analytics Platform

灵眸智能运维平台

产品白皮书

北京智维盈讯网络科技有限公司

第一章 运维现状

过多指标和维度导致使用时难以快速上手，重复性工作繁重，人力无法释放是各行业 IT 运维部门的现状。在不同的基础设备和系统配置等不断累积之下，会形成成百上千个监控指标与统计维度，传统的流量监控厂商往往只会将这些指标、维度通过固定化的界面进行呈现，剩下的分析、决策、执行则全部交给了用户的工程师去完成。

据调研机构统计，如果采用传统运维监控产品，从指标解读到后期处置，简单问题分析至少 30 分钟起，而复杂问题分析甚至需要 5 天以上（120 小时）。线上业务数量持续增长但支撑人员并没有随之增长的今天，运维人员的工作压力是巨大的。

把运维人员从重复性工作中释放出来，提高整体运维效率，是各运维团队迫切需要解决的问题。

第二章 产品介绍

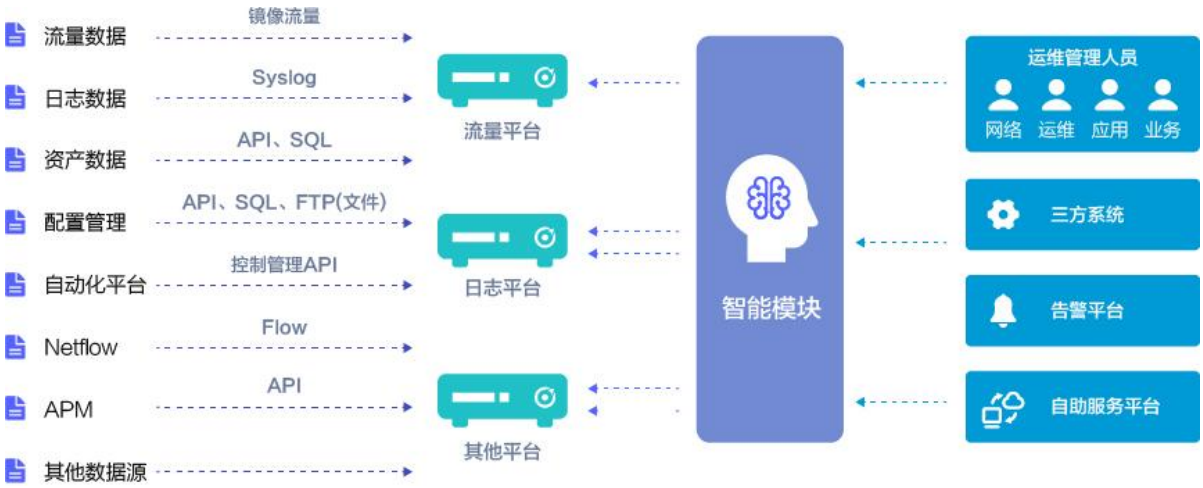
2.1 灵眸智能运维平台简介

智能监控：基于 AI 算法及产品内置的监控逻辑，有效的降低告警策略部署的复杂度，且通过有监督及无监督算法，实现精准告警。

智能分析：基于 AI 算法及产品内置的故障分析逻辑，实现告警事件自动化智能分析，提升故障的响应效率。极其简便的使用方式，让所有人都能自主分析故障。

智能巡检：深层次隐患巡检分析，及时发现业务系统运行中的隐患问题，及时解决，规避严重故障的发生。

AI 知识库：半中文式的 Python 脚本编辑器，让用户可以结合自己的环境、使用场景，定制化智能分析脚本，持续提升产品的智能化能力。



【智维数据流量数据引擎“灵眸”产品架构】

用户使用灵眸智能运维平台,当异常或故障发生时,只需点击智能分析按钮,一分钟内即可得到一份完整的“体检诊断报告”,使用门槛大幅降低而工作效率得到大幅提升。

分析报告由事件描述、体检表格、分析详情、结论、排查建议五个部分组成。自动化分析过程经过数据建模、机器学习、多维分析、AI 算法、专家知识图谱,最终输出完整的分析报告,让一线人员更从容地处理遇到的各种问题。

2.2 方案部署

nCompass 灵眸智能运维平台以虚拟机的形式运行,与其它数据平台互通,能实时获取数据信息,并在本地对数据信息进行二次加工分析。

“灵眸”支持以下主流虚拟化平台的安装:

KVM、vSphere、XenServer、Hyper-V 等。

支持以下主流公有云平台的安装:

华为云、阿里云、腾讯云、百度云、亚马逊云等。

2.3 功能概述

“灵眸”具备强大的多源数据采集、场景化分析、数据统计能力，最新的AI 算法及内置专家知识库，帮助用户拥有零配置的全面监控及一键式的故障分析能力，产品包含“零配置”的数据监控、智能告警聚合、自动化及一键式的数据分析、隐患及合规事件巡检等功能，极大地降低了数据分析产品的使用门槛，是智维数据根据多年服务大型客户复杂应用场景的实战总结，为用户真正实现运维故障“简单、快速，一键输出分析结果”。同时可以根据用户差异性场景，定制化脚本进行匹配，将明确的故障场景转换为自动化分析脚本，可以更加高效且准确的定位网络中的问题，如：策略未开通、配置缺失、线路中断、硬件 BUG 等。同时通过引入多元数据，包括设备配置、日志数据等，解决外联商户的 IP 地址众多难以维护，以及 NAT 地址转换后会话追踪困难等问题，从而有效提升故障分析场景的适配能力。

2.3.1 智能监控：

基于 AI 算法及产品内置的监控逻辑，有效降低告警策略部署的复杂度。同时通过“有监督”和“无监督”算法，实现精准告警。其主要的能力包括下述几点：

针对不同的监控对象，如网络链路、网络设备、应用系统和业务系统，平台预制了监控逻辑，用户无需从几百个监控指标中甄选哪些指标需要监控。对于甄

选出的指标，无需逐个指标的研究历史变化趋势和告警阈值，只需要一键启用监控对象的智能化监控策略，即可完成监控的部署。

监控逻辑

网 络			
网络用量	总吞吐量	网络连接	SYN包数量
	总PPS		新建会话数
	客户端数量		活动会话数
	应用数量	异常连接	服务端Reset
网络质量	丢包率		建连失败数
	网络时延		

业 务			
可用性	业务办理成功率	负载	业务请求量
	业务请求响应率	性能	业务响应时间

应 用			
网络用量	总吞吐量	应用可用性	建连失败数
网络质量	丢包率		服务端Reset
	网络时延		成功率
应用负载	建连请求数		错误响应码占比
	新建会话数	应用性能	TCP建连时间
	活动会话数		重传时延
	访问量		应用响应时间
	客户端数量		应用无响应

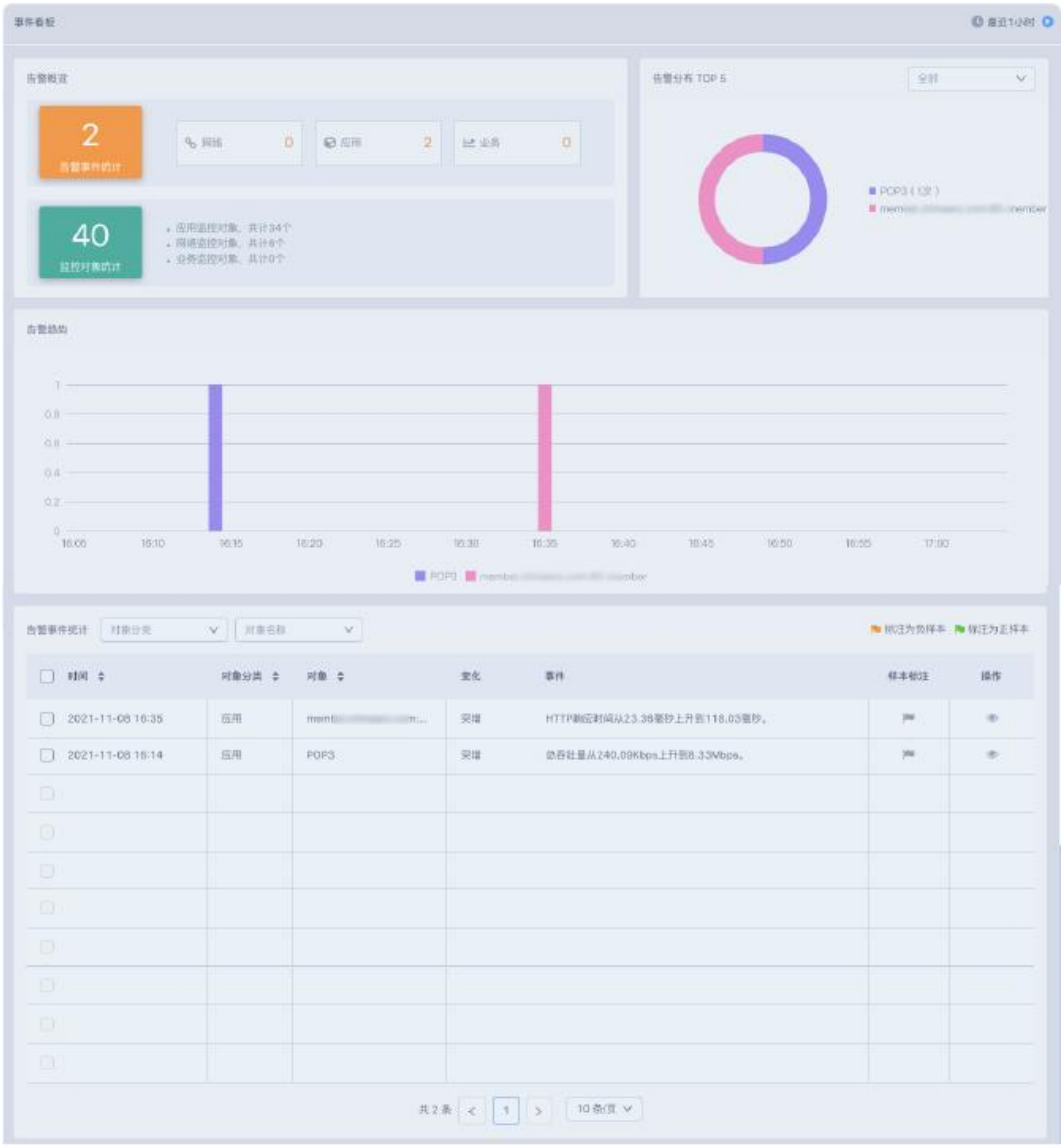
2.3.2 机器学习：

通过机器学习算法和样本数据，实现智能化、精准化的实时监控。当告警启用后，系统会自动化执行异常检测，发现指标的异常突增突降事件。用户可以对告警事件进行人工标注，当数据样本达到一定数量后，系统会再次进行数据训练，持续辅助优化告警策略。

【机器学习算法展示】

2.3.3 告警及收敛：

告警数量太多也是用户头疼的问题之一，“灵眸”在同一时间、同一监控对象、CMDB 同一业务系统等维度上，能够实现自动收敛告警事件。基于多个维度的告警关联与收敛，能够有效降低误报所产生的无效工作。



【告警事件收敛展示】

2.3.4 告警分析：

告警产生后，系统能够自动调用智能分析脚本，给出事件的详细分析报告。包括异常对象、事件现象、分析结论、排错具体命令、后续建议等，同时报告中还会提供详尽的分析过程数据，以支撑分析结论。

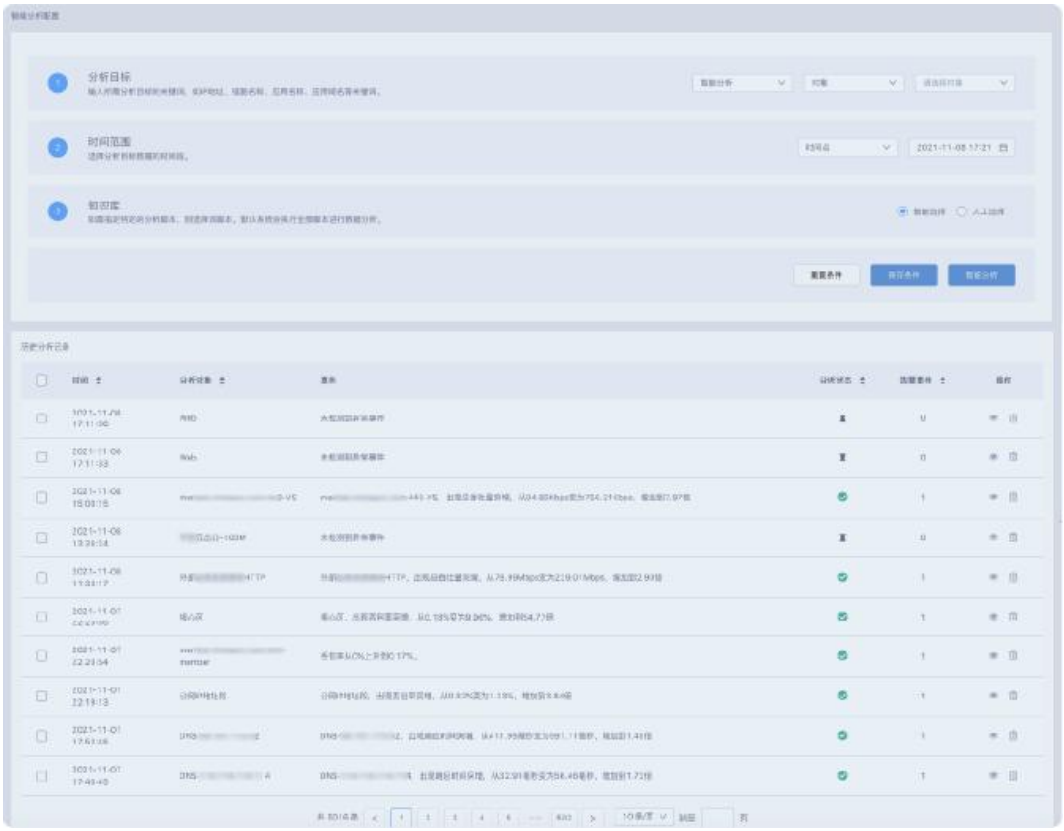
【告警分析报告详情展示】

2.3.5 智能分析：

基于 AI 算法及产品内置的故障分析逻辑，实现一键式、或 API 调用的故障自动化分析。以极其简便的使用方式，支持 IT 运维各个部门本地使用和能力输出。

产品提供界面及 API 接口，用户可在导航式界面中，输入所需分析的数据

目标和分析时间段，系统即可进行智能化分析并给出报告。



【智能分析界面使用示例】

2.3.6 自定制脚本：

用户可基于自己的网络应用架构和独有的分析习惯，针对关键业务系统，自定制数据分析脚本。“灵眸”能够提供图形化的思维导图编辑模式和高级的 Python 编辑模式供用户选择。

【思维导图编辑模式示例】

如用户具备一定编程能力或复杂分析场景需求，产品还提供 Python 编辑器，用户可快速实现自定义的数据分析脚本。

14.Web应用响应时间突增.py > ...

```python
"""
1.HTTP响应时间检测（响应时间/下钻URL），建议应用部门，检查以上URL对应的应用接口是否存在异常。
2.HTTP访问量检测(访问量/下钻客户端IP)，建议应用部门，排查以上客户端IP突发访问是否合理。
3.TCP/IP网络流量检测（总吞吐量/下钻服务端IP）
4.TCP/IP网络质量检测（网络时延/下钻服务端IP），建议网络部门，排查网络是否存在波动。
5.TCP/IP新建会话检测（SYN包数量/下钻客户端IP），建议应用部门，排查前端是否有类似促销活动或疑似攻击行为。
6.TCP/IP主机性能检测（服务端小窗口时延/下钻服务端IP），建议系统部门，排查服务器是否存在性能瓶颈的日志。
"""

from nsmart.framework.script_import import *


class 知识库(Base):
    def 检测前(self):
        if self.分析对象.类型 != "应用":
            self.跳过()

    def 配置(self):
        return {
            "检测规则": "HTTP.响应时间.突增 > 40",
            "自动匹配": True,
            "优先级": 9,
        }

    def 运行(self):
        ####1.HTTP响应时间检测（响应时间/下钻URL），建议应用部门，检查以上URL对应的应用接口是否存在异常。
        HTTP响应时间基础事件=self.检测突变(self.分析对象, "HTTP.响应时间.突增 > 40")
        if not HTTP响应时间基础事件:
            self.日志("应用响应时间检测：正常。")
            self.添加结论("应用的响应时间检测：正常。")

        if HTTP响应时间基础事件:
            self.日志("应用响应时间检测：异常。")
            服务端IP_URL贡献度列表 = self.贡献度分析(HTTP响应时间基础事件, ["服务端IP", "URL"], 5)
            if 服务端IP_URL贡献度列表:
                self.添加报表(
                    "曲线图",
                    标题="HTTP响应时间",
                    数据=服务端IP_URL贡献度列表,
                    指标="HTTP.响应时间",
                    备注="经检测，以上域名-HTTP响应时间指标存在异常。",
                )
                self.添加报表(
                    "贡献度表格",
                    标题="HTTP响应时间",
                    数据=服务端IP_URL贡献度列表,
                    备注="经检测，以上URL-HTTP响应时间指标存在异常。",
                )
                self.添加结论(f"应用响应时间检测：异常。应用的以下域名出现HTTP响应时间突增的情况：", 层级=1)
                for 服务端IP_URL in 服务端IP_URL贡献度列表:
                    self.添加结论(
```

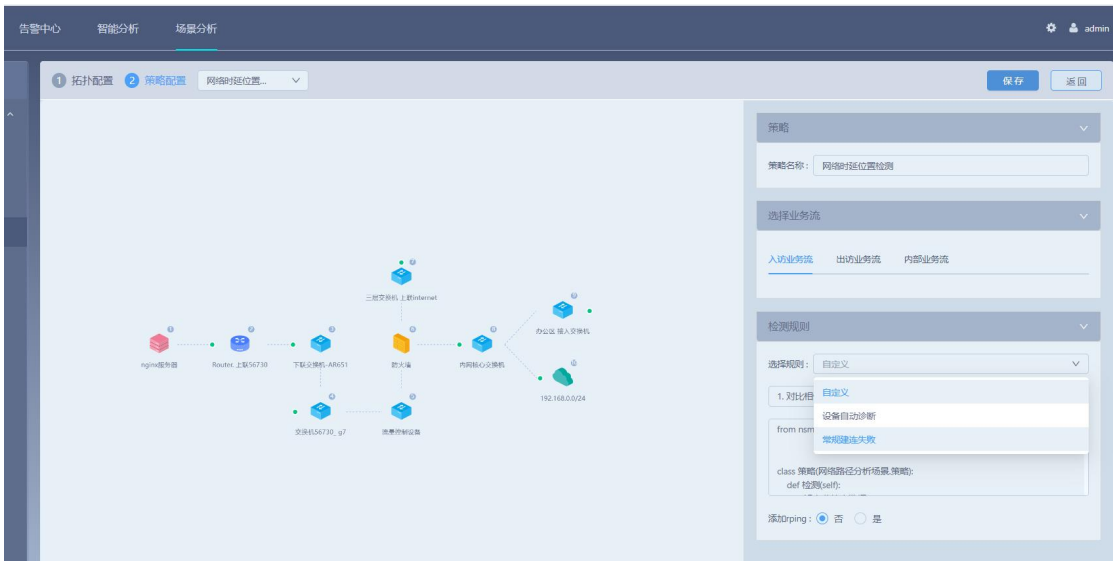
【Python 编辑模式示例】

2.3.7 拓扑配置：

能够针对企业的逻辑拓扑图，进行相关的拓扑配置，如业务流的流向路径、节点信息等，创建相应场景。帮助用户更加直观、方便地了解网络环境。

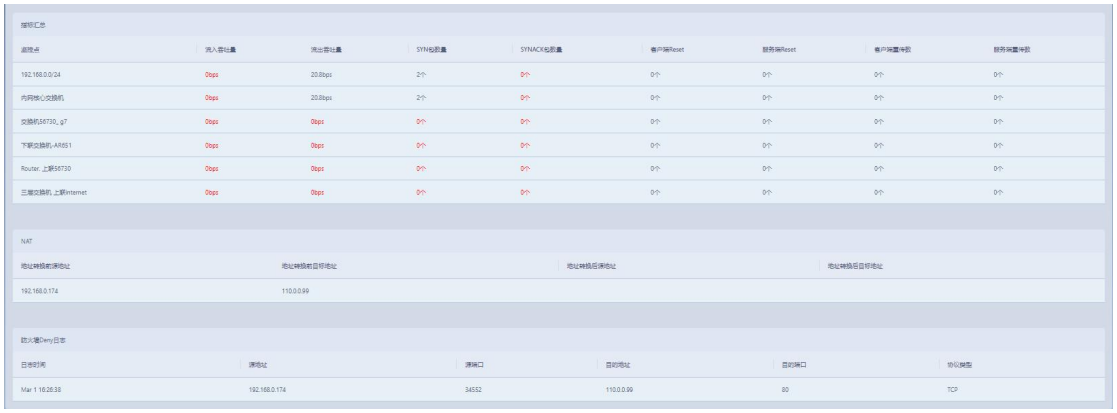
2.3.8 策略配置：

策略配置通过脚本编辑的自定义方式以及系统内置的检测规则，可以匹配多个场景，如：默认场景、建连失败场景、防火墙 Deny、路由器缺少路由、专线中断等，将场景通过 AI 算法进行分析，分析出来的结果以报告的形式展示。


告警中心
智能分析
场景分析
admin
1 拓扑配置
2 策略配置
网络时延位置...
保存
返回
策略
策略名称：
网络时延位置检测
选择业务流
入访业务流
出访业务流
内部业务流
检测规则
选择规则：
自定义
自定义
设备自动诊断
常规建连失败
添加Dping：
否
是

分析报告如下：


n-compass

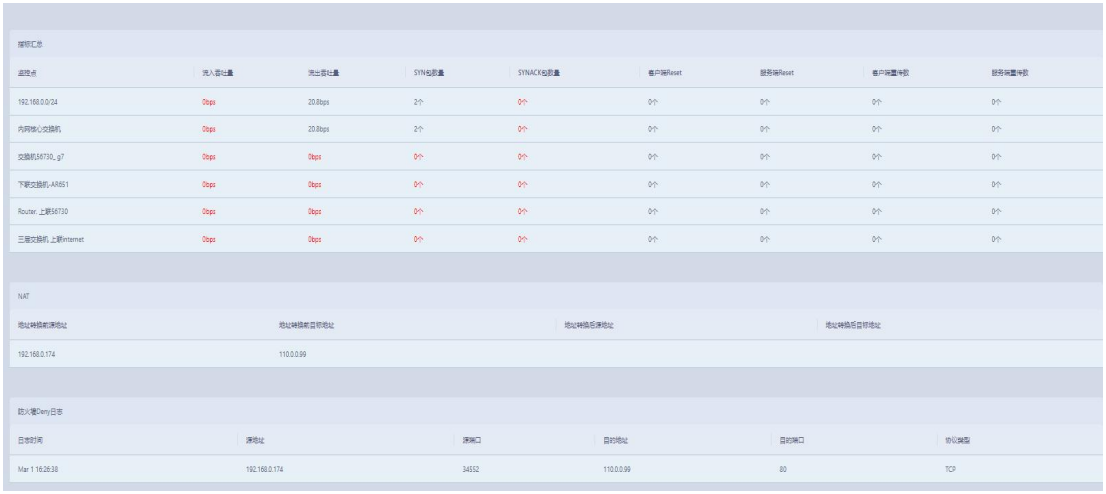


第三章 应用场景

灵眸智能运维平台，内置大量分析场景知识库，常规分析场景可参考下表所示。平台还具备前后事件关联分析，例如：查找连续两次请求 DNS，第一次失败，第二次成功的事件，关联 NAT 防火墙前后数据指标对比等定制化场景分析。

流量突发	链路抖动	链路中断
扫描类行为	促销活动	访问不通
部分区域访问不通	访问卡顿问题（汇总）	部分区域访问卡顿
应用无响应类	并发会话类问题	异常中断类
HTTP访问类	DNS访问类	SSL协商类
更多场景可详询……		

通过场景化分析，灵眸智能运维平台可以针对专线链路中断、路由器缺少路由、防火墙 Deny、交换机缺少路由等场景匹配相应的检测规则，并产生相应的报告。通过报告可以了解到分析对象在什么时间发生了哪些异常现象，并给出相关的建议与结论。



指标汇总

监控点	流入吞吐量	流出吞吐量	SYN包数量	SYNACK包数量	客户端Reset	服务端Reset	客户端重传数	服务端重传数
192.168.0.0/24	0bps	20.8bps	2个	0个	0个	0个	0个	0个
内网核心交换机	0bps	20.8bps	2个	0个	0个	0个	0个	0个
交换机S6730_g7	0bps	0bps	0个	0个	0个	0个	0个	0个
下联交换机-AR651	0bps	0bps	0个	0个	0个	0个	0个	0个
Router_上联S6730	0bps	0bps	0个	0个	0个	0个	0个	0个
三层交换机_上联Internet	0bps	0bps	0个	0个	0个	0个	0个	0个

NAT

地址转换前源地址	地址转换前目标地址	地址转换后源地址	地址转换后目标地址
192.168.0.174	110.0.0.99		

防火墙Deny日志

日志时间	源地址	源端口	目的地址	目的端口	协议类型
Mar 1 16:26:38	192.168.0.174	34552	110.0.0.99	80	TCP

第四章 产品价值

“灵眸”作为新一代更“聪明”的企业级智能运维平台，用户体验友好，使用简单，无需高深的技术功底，人人可用。再也无需繁杂的操作和数据解读，无需漫长的等待和人员消耗，一杯咖啡的休息时间，即可得到一份简洁易懂的分析报告。

【与传统监控产品对比，“灵眸”让用户体验和工作效率都大幅提升】

第五章 公司介绍

公司简介

智维数据，全称是北京智维盈讯网络科技有限公司，成立于 2015 年，智维数据是一家使用全新智能分析软件技术，改变企业对网络流量数据的消费场景，提升用户在 IT 网络运维及安全上的响应能力的企业服务公司，致力于打造技术领先的智能流量数据分析平台。

核心产品 nCompass **网络流量分析平台**可以接纳流量，Traffic log 等各种数据源，通过规则引擎进行动态数据分析与展现，通过流数据采集，策略检索，AI 智能算法，知识图谱，可视化一体化平台，帮助用户清晰了解流量中应用及业务流的不同维度的状态，将故障与隐患在从事后排障提升到了事中预警，为用户实现机器的问题机器处理，帮助用户快速提升智能运维、安全、业务数据分析的能力、效率和准确性。

该能力已经被全球领导厂商和各行业头部认可并完成数据对接与合作。公司从 15 年成立至今，服务于金融、电力、医疗、政企、互联网等多行业，服务客户包含中国银行 、民生银行、浦发银行、华夏银行、中信证券、中国人寿、银联商务、中金集团、中石油、中石化、国家电网、中国联通、中山医院、海尔集团、上海韵达等，累计合作头部客户超过百余家，得到客户的一致认可。

第六章 nCompass 产品系列

作为国内**率先实现全流量数据源智能分析的大数据公司，智维数据以流量数据作为切入点，结合日志、配置、CMDB、拨测、Netflow、Telemetry等多种数据源，通过系统内置的AI算法库，分析海量运维数据，准确发现问题，进而从决策层面进一步提高运维效率。**从根本上改变了传统IT运维管理依靠工具+人工经验的模式，为服务企业提升数据挖掘及应用创新能力。

智维数据的产品系列可服务网络、安全、应用、业务等多类别场景。

nCompass产品系列

第七章 联系我们

北京总部：

地址：北京市朝阳区八里庄西里 99 号住邦 2000 二号楼 807

电话：400-666-8216

上海办事处：

地址：上海市静安区大宁中心广场三期灵石路 718 号 A7202

电话：400-666-8216

广州办事处：

地址：广州市天河区天河北 906 号高科大厦 A 座 1906

电话：400-666-8216

深圳办事处：

地址：深圳市南山区高新科技园南十二路九洲电器大厦 B 座 3 层 F 室

电话：400-666-8216

公司网址：

www.ncmps.com

邮箱：

技术支持：support@ncmps.com

市场或合作渠道：marketing@ncmps.com