智维数据
Intelligent Analytics Platform

智维数据行业案例集

北京智维盈讯网络科技有限公司

目录

1、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，是立足于中国本土的智能运维大数据公司，通过布局关键数据节点，为服务企业快速建立业务交互数据地图和完整的监控视角，提供安全、高效、可观测性强的运维管理及安全响应解决方案。

公司的系列产品通过机器学习及缝合算法自动绘制企业实时业务交互数据动态地图，利用独有的智能算法自动发现数据异常，提升用户在IT网络运维及安全上的响应能力，改变企业IT监控与业务相脱离的现状。智维数据目前是业界唯一一家能够提供全访问流程监控与分析产品的公司，为未来场景算法提供更强的可扩展空间。

该能力已经被全球领导厂商和各行业头部企业认可，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。

2、产品简介

2.1 nCompass 产品系列

智维数据的产品立足于通、断、调中的每一个节点交互数据与配置数据的分析，在兼顾每一个节点安全、快速、高可用的同时，通过智能分析引擎进行实时节点间缝合帮助用户形成业务交互数据地图和完整的监控视角，并建立数据运营基础，推动运维部门向运营部门的进化。

2.1.1 nCompass 流量数据分析平台

应用交互路口监控，从南北向东西推进，快速搭建、升级全流量可视化自服务分析平台。

产品优势

- **全量采集：**多元数据全流量采集，提升数据统一管理及关联计算能力。指标、维度丰富，可根据分析目标，定制化输出结果。

- **智能基线：**基于历史流量特征，自主学习生成动态基线。
- **自服务平台：**智能算法结合自服务查询方式，实现了运维和分析能力的输出，提升企业整体运维效率。

产品原理

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。

典型场景

- 内置指标与智能分析引擎快速定位故障，界定责任
- 控制安全隐患风险，提升紧急事件处理能力
- 跨部门服务自查询
- 为不同场景提供定制化服务

重点功能

2.1.2 灵眸智能运维平台

完成智能数据缝合，形成业务交互地图，零配置全面监控与一键式故障分析。

产品优势

- **业务交互地图：**通过关键节点的数据获取和缝合，形成业务交互的关联基础数据，自动绘制动态业务交互地图，支撑业务及安全场景的综合分析。
- **场景分析：**基于不同网络区域、业务特点来进行可编排的智能分析。
- **AI赋能：**基于最新AI算法及内置专家知识库实现故障自动化分析，1-5分钟一键输出报告。
- **规避风险：**零配置动态告警，规避严重故障发生。

产品原理

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。

典型场景

- 配置的数据监控
- 智能基线精准告警
- 1-5分钟一键快速输出故障分析结果

重点功能

2.1.3 防火墙策略管理平台

对海量防火墙策略进行策略优化，消除隐患策略，加固防火墙策略漏洞。

产品优势

- **业内唯一：**通过全数据采集加配置分析给出精准策略优化建议的产品。
- **防火墙性能零影响：**旁路部署方式，不开启防火墙日志，对防火墙性能与业务零影响，高效率自服务，可一次收敛所有策略。
- **采购灵活：**软件订阅服务或软硬件一体买断方案均可提供。

产品原理

通过7*24采集防火墙前后流量加读取配置输出优化方案。

典型场景

- 符合等保2.0要求，策略快速收敛
- 自服务查询查询访问路径中的策略

- 对异常跨区访问做精准统计分析
- 替换前后的配置对比
- 识别不合规策略，给出优化建议

重点功能

2.1.4 灵珑应用交付管理平台

应用交付全面监控与分析，精准业务路径梳理，优化配置提升效率，业务场景分析，业务故障快速定责。

产品优势

- **业内唯一：**分钟级故障定位与业务画像，可自助查询的应用访问路径与业务访问关系画像，明确提示业务状态，精准定位故障影响范围。
- **全面监控与分析：**360度设备监控，提升故障的处置效率，规避潜在业务风险。
- **专家级赋能：**可根据需求自定义检测时间与范围，准确输出应用与设备自动巡检结果。

产品原理

通过主动的API获取和被动的日志及遥测数据接收的方式获取相关信息，输出应用交付设备高效管控方案。

典型场景

- 消除应用交付监控盲区，快速了解业务状态
- 一键式操作，输出业务故障分析结果
- 智能识别应用交付设备隐患
- 直观展示访问质量变化情况
- 自动绘制业务路径画像，支持自助查询服务，有效核实业务变更
- 自动梳理不合理的配置信息

重点功能

3、客户案例

3.1 金融行业

某大型股份制银行

1、项目背景

某大型股份制银行，营业网点总数近千家，并建立境内外代理行近两千家，建成了覆盖全球主要贸易区的结算网络。随着业务发展，需要建设更加完善的网络监控系统，提升运维效率，保障国内及国际业务稳定持续。

2、用户痛点

缺乏细微到业务级的带宽占用分布统计；对于性能指标阀值的设定，欠缺一套基于链路特征的动态基线告警策略，以完善现有监控系统；偶尔出现无法访问、获取数据慢及交易失败等问题，交易监控只能发现业务成交量下降和失败率上升，网络部门为监测专线网络连通性和网络抖动情况，借助 SLA 跟踪等方式实现，却很难在业务层面实现监控，缺少辅助手段分析出现异常的根本原因。

3、应用场景

场景 1：主动发现故障

对全互联网业务进行梳理，深度剖析互联网流量的组成，针对各业务单独计算占用带宽百分比。统筹全局站在数据中心全业务整体高度，7*24 小时不间断监测关键业务用量、质量及运行状态。出现异常时发送故障告警短信，第一时间将信息反馈给业务系统负责人，缩短故障被动发现的时间差，实现快速恢复生产。

场景 2：链路管理

nCompass 流量分析平台让数据以可见和可读的方式呈现，大大的提升了互联网和专线链路的用量及质量管理能力，量化业务状态及数据传输效率。

场景 3：智能分析

nCompass 流量分析平台与网管平台实现数据对接，从网管平台收取一份专线链路带宽和质量的统计数据，对数据进行二次分析，通过私有算法自动生成智能动态的性能告警基准线，结合业务特点产生偏离智能基线的告警。

场景 4：多元数据接入

nCompass 流量分析平台采用主流的 API 开放式接口，更容易与第三方平台实现数据互通，融合的统一管理平台对运维管理者更加友好，实现辅助决策和集中呈现。

场景 5：外联第三方业务全局监控

实时监控外联第三方全业务，借助客户侧/服务侧相关位置指标，精准判定导致业务异常的原因。通过网络流量、网络质量、网络连接、应用性能、主机性能五类指标组，分析异常是因网络、应用、主机造成的。

场景 6：一键生成故障分析报告

nCompass 业务监控通过颜色的变化，精准快速的定位异常节点，大大缩减人工盲目排查的时间。选中异常节点，一眼知晓曲线的异常变化。结合海量场景分析模块，一键生成故障分析报告，大大降低用户使用成本。

某城商行 A

1、项目背景

某城商行 A 现阶段不能整条业务流程串联分析，也无法直观显现对本地业务可用性、性能评测、故障分析排查方面有待优化，同时无法监控外联第三方单位业务状态，不可主动发现现网中潜在的隐患问题，只能被动的等待业务部门的反馈。因此急需建设一套完善的网络流量监控分析系统，实现网络质量和应用系统性能可实时监测、并提供事前，事中，事后的问题分析手段。

2、用户痛点

缺乏细微到业务级的带宽占用分布统计；网络运维人员对于应用或者业务系统无法做到有效监控，问题排查的效率低；缺少一个涵盖交易层、应用层、网络层这样完整的可视化监控系统，如果某一层面出现问题无法快速的扩展到其他层面进行分析；网络区域较多、网络规模庞大、网络设备众多以及人员的变更会导致网络架构信息缺失，致使出现问题时很难判断问题出现在具体哪个网络区域，网络运维效率低；现有的大屏可视化监控无法对当前业务系统的“好”与“坏”进行直观展示，缺少像互联网监控、网联交易监控这样宏观的供监控中心人员使用的可视化监控系统。

3、应用场景

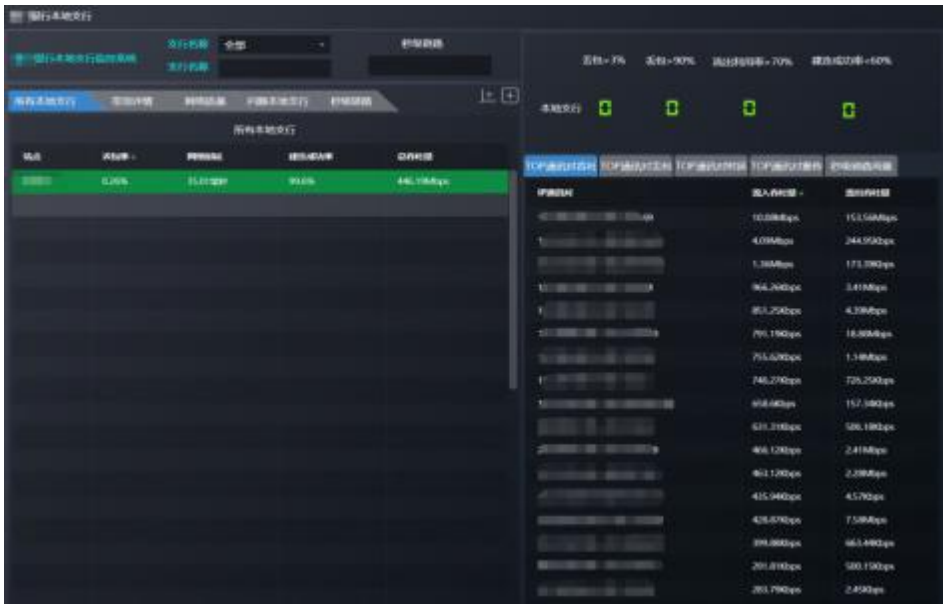
通过上述部署方案将每一个关键节点的流量镜像过来，做到对整个网络区域的全流量监控，再针对用户的上述需求完成了链路监控、应用端到端监控、网联协议解析、智慧网络、对接 zabbix、定制可视化监控大屏等场景。

场景 1：广域网链路监控

镜像数据中心互联网区、外联区的流量，针对镜像的流量数据进行精细计算，统筹全局站在数据中心整体高度，7*24 小时不间断检测各链路用量、质量以及运行状态。出现异常发送故障告警邮件时，可快速进行下钻分析定位故障。通过一个分析模板监控各链路的实时运行状态，如实时的吞吐量、丢包率、网络时延、建连成功率等重要指标。同时关联系统内置的分析模板，遇到问题能有一个快速的分析界面，提高了运维的效率。

同时针对链路问题常见指标设置了问题链路栏，哪条链路丢包率 > 3%、流出利用率 > 70%、建连成功率 < 60%等隐患一目了然，选中任一链路即可进行下钻分析。某条链路下哪个业务出现了问题，哪个通讯对流量突发等都可通过下钻的方式查看，为故障排查提供了便利。根据用户的实际情况对各链路的流量突发、网络时延等加入了告警功能，一旦触发告警就会根据提前设定好的知识图谱自动导出一份智能分析报告，来告诉用户告警的原因是什么，怎么解决，大大提高了问题排查

的效率。



针对各链路加入了定时生成的报表，比如在报表中列出了每条链路中流量最大的 IP 通讯对以及带宽利用率较大的链路，便于周期性的对各链路的运行情况有一个宏观的了解。此外还可根据报表中长期没有数据的链路和相关部门核对该链路是否在使用，及时排除不在使用的链路，减轻运维负担。

场景 2：业务端到端可视化监控

通过一张自动的端到端视图展现业务系统各节点的访问关系以及运行状态，做到实时监控，而且视图中的数据支持灵活的编辑、深度钻取等功能。

对各核心业务系统进行业务逻辑梳理，如网上银行、手机银行等，并通过 nCompass 平台产品的自动端到端模板，形成各业务系统的端到端可视化监控。通过一张视图完整呈现某个业务端到端的监控，当故障发生时可通过指标颜色或曲线趋势的变化快速锁定故障区域，判断都有哪些用户受到影响，故障是由哪个节点发生，故障节点哪些指标异常等。

而且用户可以通过点击快速链接到系统中内置的分析模板，便于分析和排查问题。

场景 3：协议解析与第三方数据对接

通过协议解析将网联的监控做到交易层面，与前面的核心系统业务梳理结合从整体的角度将交

易层、应用层、网络层的数据串起来，监控每一个层面的状态，因为任何一个层面出问题都会导致交易失败。此时再遇到交易问题就可以通过流水号或是其他维度从交易层、应用层、网络层来分析到底是哪一个环节出现了问题，是银联那边的问题还是行内自己的问题，若是自己行内的问题可快速查看是哪个节点，哪个指标的问题，使问题的排查更加精细化，快速定位问题。

针对用户的痛点，通过 API 的方式对接了 Zabbix 的告警信息，使 Zabbix 的设备告警信息更能可视化的展现，与其他各个层面的信息相关联，实现了信息的整合，使监控更全面，更能从全局的角度分析问题。

场景 4：数据中心可视化监控

当数据中心的网络结构越来越复杂，网络设备越来越多的时候，即使是网络管理员也很难清楚地知道每个流量过来到底经过哪个区域哪些哽备，而通过智慧网络视图就能轻松解决这些问题，比如网络信息缺失，以及出现故障是哪个区域哪个业务出现了问题。

在 nCompass 定制的智慧网络视图中用户可以通过搜索 IP 或 IP 通讯对的方式来查看其经过了哪些区域以及哪些网络设备，也可通过下钻来查看这个区域下承载了哪些业务。

场景 5：可视化监控大屏

用户通过 nCompass 定制化的方式，定制了互联网监控、网联交易监控和超网交易监控视图，

为运维人员高度概括互联网以及核心交易状态的大屏。这些视图能更加美观、直观的呈现各环节的运行情况，使不具备丰富网络知识的人员也能及时发现问题，及时通知运维人员来处理。

某城商行 B

1、项目背景

某城商行 B 是其省内大型综合银行。随着业务的不断发展，该银行网络、应用系统自身的复杂度日益提升。同时，数据中心与分支机构，以及外部机构的流量与业务交互量也日益增长。当有故障发生时，时间往往被耗费在低效的排查工作中，该银行此前的现网网络性能管理平台系统上线已经三年时间，该系统已经无法满足行内现网运行需求。

2、用户痛点

核心业务系统的可视化监控不够直观，难以管理，无法定位故障至具体节点；业务系统之间的前后访问关系难以梳理；业务系统出现故障后，无法快速定位问题；生产和灾备双中心互联网链路及专线链路的用量及质量难以评估；基于核心区域、电子银行区域，需要每天统计每台交换机接口

的流入流出流量大小，评估是否存在超负载情况；行内数据量较大，很难做到原始数据包保留 7 天；缺乏通过巡检发现数据中心存在隐患的有效手段；对于全局监控缺乏清晰、直观与美观并存的大屏展示。

3、应用场景

场景 1：基于该银行核心系统定制可视化分析视图

每套可视化视图都从公网入口至后端 APP Server，每一个节点均可独立下钻分析(网络层、应用层、主机性能层)，用户在发生故障时可快速直观地定位出故障域。以下为手机银行的端到端分析视图演示图片：

场景 2：流量采集分析

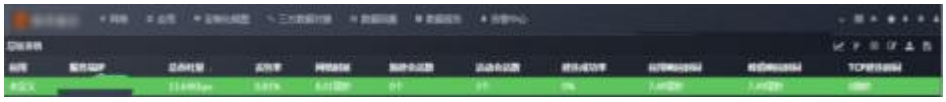
能够对该银行通过真实业务访问产生的流量进行采集与分析，输入单个业务 IP 即自动得到应用调用逻辑和性能变化，解决了在应用梳理、应用变更等场景下快速精确变更和解耦业务。

场景 3：针对突发故障快速定位

以某业务系统故障示例：

该业务相关同事反馈业务办理出现故障，点击查看该业务响应趋势图：

对其后端调用的数据做关联分析，未发现异常现象。



向上关联分析，查看该相关业务所属的接入交换机该时段流入流量分支峰值，同时发现该交换机中存在另一相关业务的大量流量占用带宽，由此可得到结论为：此次该业务响应时间较长为所属交换机网口带宽不足导致，通知同事调整策略后解决。该银行此类问题，从发现到解决，总体耗时控制在半小时内，大大缩短了排障时间。

场景 4：网络链路质量监控

评估行内互联网及分支行网络链路用量和质量监控不单单是指标类问题，nCompass 流量分析平台能够应对指标做历史数据的判断并生成“基线”，判断出此次突发是否为在基线以内，且可直接分析出突发时请求的业务应用 IP，从而避免将由于业务特性产生的特定时间吞吐量的上升误定位为故障，消耗时间与人力成本。

场景 5：定制日报

为该银行定制核心区域和电子银行区域日报，每日凌晨发送最近一天核心区域流量变化趋势，用户上班第一时间即可对内部流量冗余做出判断。

场景 6：优化数据存储

基于该银行重点区域优化了生产和灾备共多台设备数据压缩优化存储，服务器存储资源量提升 4 倍以上，且可留存提取 7 天以上的原始数据包、半年以上指标类数据，便于事后回溯。

场景 7：隐患事件记录与场景知识库

在未显现明显故障时，提供当前隐患事件记录，增加行内运维人员学习业务知识的渠道，建立体验指标库，形成分析优化机制目标，如：是否有服务开启高位端口、是否存在疑似端口扫描行为等隐患，在未形成故障时及时发现并优化。

另外为该银行配置故障分析场景知识库，定时巡检可能存在的故障场景，如：业务流量突发、网络丢包、应用响应时间过长等。

场景 8：IT 质量监控大屏

大屏是能够非常好的体现当前运维质量状况的途径。智维数据针对互联网链路、分支行链路为该银行定制可视化大屏，全网实时监控 IT 质量，所有监控指标均关联告警，一旦触发告警，会有明显的颜色变化提示。

某股份制银行信用卡中心

1、项目背景

某股份制银行信用卡中心，隶属于一家从事货币金融服务的全国性股份商业银行。随着该行人员更换，交接不完整，部门对自身业务访问关系变得模糊。出现问题排查十分麻烦，网络不了解应用调用关系，应用总认为是网络问题，只能各部门去检查自身问题，因此急需建设一套完整的可打通各部门统一数据分析的可视化系统，协助各部门人员去解决问题。

2、用户痛点

该信用卡中心网络部门工作人员较少，无法实时监控网络及判断网络是否影响业务等问题；故障感知迟缓，只能通过前端的用户投诉或者业务部门反馈才能知道故障已经发生；现有的网络工具可粗略回溯数据但无法精确排查问题；突发事件发生后，缺少精准故障现场数据，故障根因定位纯靠运维人员的经验，效率得不到保证；故障发生快，解决慢，后续查因难，责任难界定；业务系统众多，各业务系统之间的调用十分频繁，同时缺乏对关键应用状态的展示与应用调用关系的自动发现能力，随着人员更换，交接不完整，部门不了解自身业务访问关系；多套独立的监控系统造成信息孤岛，系统间数据孤立，无法有效联动分析。

3、应用场景

场景 1：定制大屏

互联网链路可视化；外联第三方单位链路可视化；分支单位链路可视化；同城中心链路可视化

针对数据中心整网链路分析，定制分析大屏，可展示分析链路下的网络状态，并设置告警，做到早发现，快定位。

场景 2：业务系统

目前核心业务系统随着人员更换，很多部门都不了解自身业务访问关系。首先梳理核心业务访

问关系，其次对应业务制作前端后端视图。

例如：手机 app 业务梳理

前端：“用户访问我的用户体验如何？”

自身：“网络及应用的端到端各节点的运行状态如何？”

后端：“我依赖的后端服务的运行状态如何？”

制作对应定制化视图，实时监控观察自身业务状态，对自身业务更加了解，监控每层运行状态。快速故障定位，通过前后层对比判断发生故障时的位置。

场景 3：交易监控

可直接使用卡号、流水号等信息搜出对应 IP 地址的同一笔交易进行关联，对其中涉及到的相关交易能够进行筛选。

监控内容：监控应用会话、延迟、卡号、交易流水、交易状态。

某大型金融服务企业

1、项目背景

某金融服务大型企业是一家集财富管理、信用风险评估与管理、信用数据整合服务于一体的综合性现代服务业企业。随着互联网产业发展和日益完善的网络环境，越来越多的业务办理由线下转移到了线上，线上飞速增长的用户交易量加深了该公司运维部门的压力。因此用户体验监控与核心业务的实时状态监测就显得尤为重要。

2、用户痛点

故障感知迟缓，只能通过前端的用户投诉或者业务部门反馈才能知道故障已经发生；突发事件发生后，由于缺少故障现场数据，故障根因定位纯靠运维人员的经验，效率得不到保证；业务系统众多，各业务系统之间的调用十分频繁，同时缺乏对关键应用状态的展示与应用调用关系的自动发现能力；信息孤岛，多套监控系统处于独立状态，系统间数据孤立，无法有效联动分析。

3、应用场景

场景 1：前端用户的监测

nCompass 流量分析平台可以实时展示不同维度用户的使用体验，同时支持智能告警，实时感知前端用户体验。该公司的运维从此由被动变为主动，用户体验迅速感知(通过智能告警或者地图的颜色标记)，在用户反馈之前即可解决问题，降低运维的投诉率。

场景 2：故障的快速定位

通过应用端到端可视化监控分析，实现可视化关键应用在数据中心各个节点的实时运行状态。各层面的指标数据均可展示在一张图表之中，在该公司复杂应用架构下，出现故障可快速定位，缩短故障定位时间，降低故障造成的损失。

场景 3：关键业务状态监控大屏展示

能够呈现每个业务详情，如成功率、访问量、响应时间等。实时掌握业务的响应状态。该公司工程师无需任何操作，通过大屏即可得知重要业务的状态是否正常。

场景 4：一体化展示平台

nCompass 流量分析平台融合了该公司现有的所有监控系统，可进行一体化展示。支持将多个来源的数据统一展示在一张视图里，并进行二次计算，展示其智能基线。工程师无需依次登录每一个平台单独进行查看，无需联系相关业务人员即可了解该系统是否异常。

某金融科技公司

1、项目背景

某金融科技公司致力于运用人工智能、云计算等技术，赋能金融、医疗、房产、汽车、智慧城市五大生态圈。该公司当前网络对信息系统的依赖程度越来越大，网络遭受内部攻击、违规操作、信息泄露等安全威胁也在不断增加，组建可视化网络迫在眉睫。为此，该科技公司在数据中心网络中部署了众多的旁路监测系统来组建业务可视化网络。

2、用户痛点

网络规模庞大，但是运维人员少，几个人管理几千条链路及数个数据中心的网络运行，网络人员处于疲于奔命的救火工作模式，难以保证高效进行网络管理工作；集团的促销活动频繁，比如双十一、双十二等，这类活动一天的营收都是数以亿计的，如果中间因 IT 故障导致交易异常，将给集团造成巨大损失；数千条网络链路，扩容缺少有效的运行数据支撑，难以合理的做出扩容方案及预算。

3、应用场景

场景 1：全球机房整体的链路质量与流量详情

宏观上，呈现全球机房整体的链路质量与流量用量详情，通过一张监控视图能够快速的了解各个机房的流量大小丢包时延等信息。

场景 2：定制所有机房的数据流入路径图

包括经过的一些关键的节点如防火墙、F5 等。通过关键节点的丢包、时延、会话状态、吞吐、等指标的对比，如出现故障可以进行快速定位，并且能够明确的找到故障区域以及出现问题的指标。

场景 3：对各机房出口运营商线路进行监测

呈现各机房任意运营商的网络丢包与流量吞吐的实际情况，出现故障时可以快速呈现并进行告警。

场景 4：为重要促销业务定制可视化监控大屏

通过数据包分析，我们可以实时查看业务的前端用户体验是否正常、数据中心内部的网络链路的丢包时延是否处在合理范围、业务的关键 url 响应时间是否变慢等，结合高亮值告警，做到业务的全面监控，保障促销业务的正常运行。

场景 5：通过拨测显示各地的网络延时与丢包情况

通过定制化监控视图的高亮值可以实时查看丢包率高或者时延长，快速精准定位链路问题。

场景 6：实现 netflow 的数据分析

可以实时查看各职场的流入流出吞吐大小，并展示吞吐量 TOPIP 通讯对，若出现链路带宽占满，可以快速识别并告警；可以为带宽占用最高 IP 通讯对提供数据支撑快速解决问题。同时生成周报月报年报，呈现链路带宽利用率曲线图，并给出合理的链路带宽优化建议。

场景 7：确认安全设备的状态

通过部分安全设备前后的数据对比(数据包数量、吞吐量等)来确认安全设备的状态，以防火墙为例：数据包数量(数据吞吐量)经过防火墙的过滤会有一定的减少，但是整体的数值对比应该是稳定在一定的比例之间。对比前后的数据，若出现较大幅度的波动，则需要对火墙进行排查。

3.2 政企机构

某省铁路局

1、项目背景

按照电子客票业务使用需求，涉及客票网络的通信、信息系统维护单位要以优化网络架构、挖掘既有资源为主，综合考虑设备使用寿命、发展趋势、可扩展性、可维护性等确定扩容方案。网络设备要补充流量监测功能，实现对网络端口流量的持续监测。

2、用户痛点

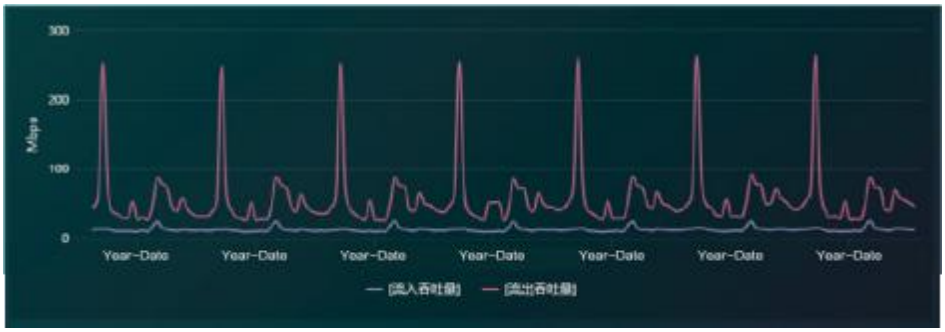
缺少票务段和车站到数据中心的专线链路的网络监控，缺乏监控相关业务专线的网络带宽使用情况、使用趋势、业务占比等的有效手段；电子客票系统出现故障后，无法快速定位问题；没有了解全部应用之间的调用关系的有效手段；缺少原始流量回溯能力；相关系统出现异常事件时，缺少

原始流量数据的留存和提取功能；缺乏在未发生故障时通过巡检发现数据中心可能存在的隐患，做到主动运维的有效手段；缺乏对相关业务网络状态进行实时、精确告警的有效手段。

3、应用场景

场景 1：链路监控

某铁路局缺少有效的手段了解相关专线链路的网络质量及用量，nCompass 流量分析平台可以帮助用户呈现所有专线链路的运行状态和详情。



场景 2：内网网络问题发现

相关线路采用 Span 方式采集数据，并且通过精细的根因指标评估当前链路的网络质量，在发生网络异常时，快速定位出故障区域。若某应用丢包率较高，可以通过 nCompass 流量分析平台生成的数据表格，快速发现客户侧丢包较高对应用访问造成影响，基于该现象定位排查方向和故障范围，如：主机网络或配置问题造成异常。通过 nCompass 流量分析平台可以快速发现并定位问题节点，大大提升运维人员工作效率。

场景 3：应用调用关系展现

该铁路局通过真实业务访问产生的流量，输入单个业务 IP 即可自动得到的应用调用逻辑和性能变化，帮助该铁路局在应用梳理、应用变更等场景下做到快速精确变更业务。

场景 4：数据库监控

相关系统后端数据库的运行状态是该铁路局重点关注的部分。通过 nCompass 流量分析平台能够实时监控相关 oracle 数据库的运行状态，查询最耗时的语句。能够提升该铁路局核心区部署的分析设备的存储能力，且可留存提取 7 天以上的原始数据包、半年以上指标类数据，便于事后回溯。

场景 5：隐患排查

在未显现明显故障时，提供当前隐患事件记录，增加行内运维人员学习业务知识的渠道。并建立体验指标库，形成分析优化机制目标，如：是否有服务开启高危端口、是否有疑似端口扫描行为等隐患的存在。在未形成故障时，发现并优化。

场景 6：专线详情监控

实现相关业务专线的网络带宽使用情况、使用趋势、业务占比等进行全面的可视化展示，并实现精确的告警帮助该铁路局对相关业务网络通道进行实时的监测。

按照相关系统业务的流程，实时监控票务关联服务器间的应用状态包括网络用量、网络质量、网络连接、应用性能等，出现异常时，如：响应变慢、流量突增、访问量突增等情况，可实现主动告警。

相关专线链路以及关键数据库应用的流量分析是该铁路局主要关注的部分。nCompass 流量

分析平台能够做到当相关专线链路以及关键数据库应用的网络出现问题时，及时触发设置的警报规则，进行邮件提醒。下图为 oracle 数据库告警统计：

当触发告警时点击即可查看告警详情，以及告警关联的数据波动情况。锁定故障范围之后，若发现发现当前时段 APP 服务应用响应时间如上图一样出现明显上升。

某政务服务平台

1、项目背景

某政务服务平台是为政府行业提供基础设施支撑软件、应用系统、信息资源、运行保障和信息安全等综合服务平台。该平台需要满足大量相关部门正常办公的同时确保内部数据的安全稳定运行，保证提供完善安全的云服务。用户目前没有完善的运维监控平台，还是靠人员登录各个产品界面进行运维工作。

2、用户痛点

缺乏网络链路用量与性能的可视化能力，当发生异常情况，无法准确定位出是哪台设备或者应

用出现问题；缺乏对业务系统进行端到端访问关系的梳理，无法准确的掌握内部业务之间运行情况；缺乏日常工作以及事件场景化定制。

3、使用场景

场景 1：内部流量管控

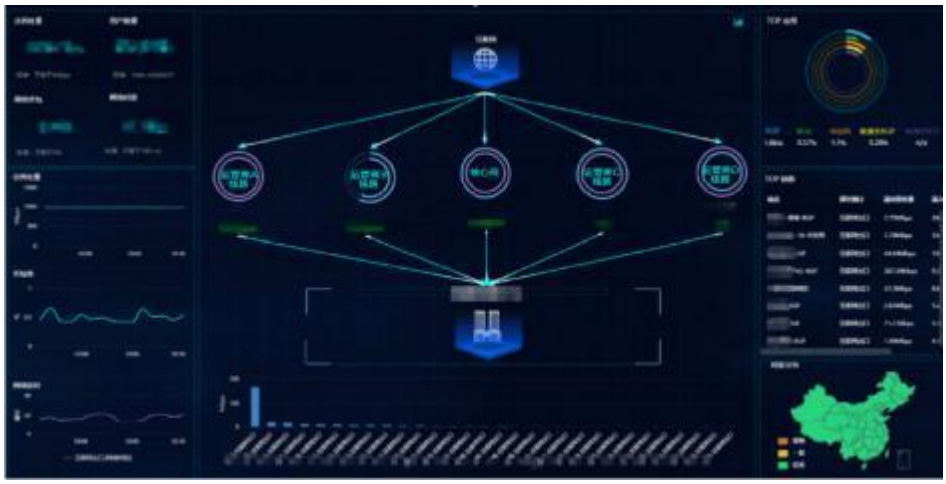
针对重要业务系统内部架构复杂的现象，通过对内部资源的梳理，整合出关键的几套业务系统。以某主站为例，用户就可以监控到该主站有多少的访问情况，各个部门访问主站的通畅情况、每个节点之间的访问量大小以及数据传输之间的性能好坏都可以一目了然的展示出来。并且能够展示各个部门之间协同办公的效率情况，能够有效的做到主中心对访问的部门一目了然，很好的帮助用户解决对内部流量管控不足的问题，合理的规避链路堵塞风险。

场景 2：运营商链路监控

加强对运营商链路可视化能力的提升，加强对各个下属节点监控能力。

nCompass 流量分析平台通过在关键节点交换机进行镜像，能够对节点设备的变动做到准确掌握。通过梳理一定时间内的访问关系，快速的展示内部资源的上线或下线情况。而且针对用户内部存在多部门设备协同办公的情况，通过关系梳理能够发现较为常用的组合模式，一方面能对组合模式进行监控；另一方面用户能够根据真实使用情况，对资源进行二次分配，有效合理地解决协同

办公模式下带来的办公环境复杂的问题，提升用户对网络链路精细化管理的能力。



场景 3：隐患监察

针对用户安全管理范围低，故障常常在发生之后才能被发现的现象，提供有效解决手段。

nCompass 流量分析平台通过智能化模块，时刻分析用户当前数据中心状态。能够做到及时发现数据中心内部存在的隐患行为，如：CC 攻击、肉鸡攻击、DDOS 攻击等攻击行为；还能排查出网络内部存在的一些安全隐患，如：高危端口、端口扫描、负载分配不均、防火墙策略漏洞等现象；并且提供安全漏洞排查、新业务上线前后对比,、重大业务环比同比等功能。帮助用户减少安全隐患，提高网络安全预警范围。而且还能通过数据回溯回放,针对已经发生的攻击事件进行后续的问题分析，帮助用户进行事故责任调查，增加日后安全防范方法。

场景 4：重大事件监控

针对重大事件保障以及日常运维中可视化能力较差的现象提供有效解决手段。nCompass 流量分析平台支持可视化视图自定义功能，用户可通过内部搭载的 dashboard 功能来进行可视化视图的自定义，有效地提高了客户针对重大事件的保障以及日常工作的数据可视化能力。

nCompass 流量分析平台通过回溯以及报表功能，能够将这段时间内使用资源情况进行自动输出，明显地减少了用户日常工作内容，帮助用户提高工作质量。并且还能输出整体数据中心内部运行报告，方便向用户进行展示。

3.3 互联网&媒体行业

某大型媒体平台

1、项目背景

随着海外业务日益增多，该媒体平台现如今在欧洲、美国、亚太、非洲等地区设有分部，通过专线链路连接总部数据中心；数据中心作为业务核心，在日常运营管理中面临巨大运维压力和挑战。网络部门为保障业务的稳定运营，计划逐步建立和完善网络可用性告警等专业监控系统，以实现相对独立的专业化监控和关键数据指标的集中展现。

2、用户痛点

如何实时监控不同网络区域的网络用量以及网络质量；业务系统之间的前后访问关系难以梳理；关键业务出现问题时，无法快速定位是网络问题、主机问题、系统问题还是应用问题；缺少原始流量回溯能力，当业务系统出现异常事件时，缺少原始流量数据，无法回溯；缺少用户体验感知能力，该媒体平台的多媒体云为众多媒体机构提供服务，需针对云上的最终用户的体验进行监控；如何在未发生故障时通过巡检发现数据中心存在的隐患。

3、使用场景

场景 1：网络集中监控大屏

基于监控各个机房与数据中心专线的网络状态，详细展示了该机房和海外专线的网络用量及质量情况，包括流入流出吞吐量、丢包率、网络延时等，可以实时查看各机房与数据中心专线的网络用量和质量排名。

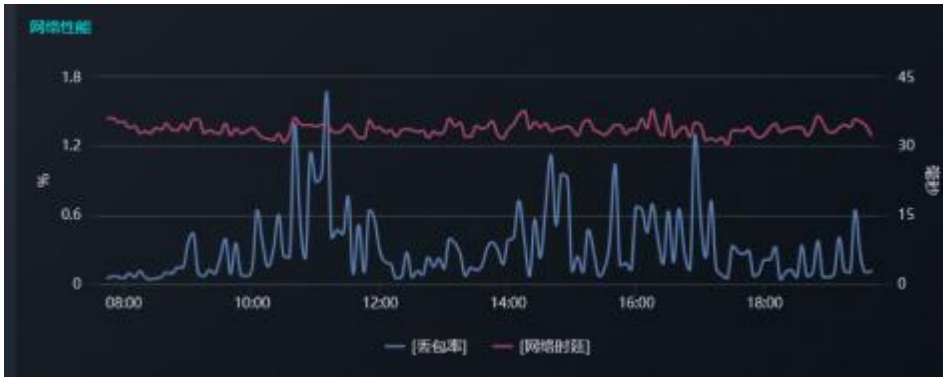
场景 2：云环境下的关键应用访问关系梳理

通过采集与分析该媒体平台真实业务访问产生的流量，可以实现输入单个业务名称即自动得到应用调用逻辑和性能变化。解决了在应用梳理、应用变更等场景下快速精确解耦业务。

实现了自动可视化网络中业务系统之间的访问调用关系的可视化展示，为故障排查、安全合规检查、变更比对分析、机房搬迁、重大业务变更等场景提供数据支持。

场景 3：故障快速定位

以某业务定位问题示例：运维相关同事反馈某应用经常出应用访问异常，但不知道具体原因是什么。



通过针对该应用监控可以清晰看到该应用的网络状态以及应用自身响应的运行趋势，通过曲线图看到当日该应用的网络丢包较严重，通过数据包回溯分析，可以看到用户访问该业务时客户侧丢包率很高，导致 TCP 三次握手失败，很快排除了数据中心内部的原因，确定了需联系运营商查找

链路问题。快速定位出现问题的节点，大大提升了运维人员的工作效率。

场景 4：周期性网络运行自动化报表

为机构定制相关应用周报，方便用户了解相关应用一周的流量变化趋势，为运维人员做工作总结提供便利。

场景 5：各个海外专线链路的网络情况监控

当发现某区域的网络通信出现异常时，可及时发出告警，并快速定位故障域。通过监控，发现某海外子机构出现较为严重的网络丢包，快速定位故障点：子机构的哪个设备出现异常？访问的是数据中心的哪些服务器?

场景 6：隐患记录

在未显现明显故障时，提供当前隐患事件记录，增加机构内运维人员学习业务知识的渠道，建立体验指标库，形成分析优化机制目标。如，是否有服务开启高危端口，是否存在疑似端口扫描行为等隐患存在。在尚未形成故障时，发现并优化。

另外为该媒体平台配置故障分析场景知识库，定时巡检可能存在的故障场景，如及时发现业务流量突发、网络丢包、应用响应时间过长等故障存在，并及时处理，提升运维效率。

某央媒机构

1、项目背景

经过不断地发展，现如今，该机构已拥有数十家分社和数家分支机构，用户遍布全球 200 多个国家和地区。随着国家信息的不断发展，机构本部的数据中心与国内分社、国际分社的信息交互日益频繁，当国家有重大信息交互时，数据中心与分社之间的网络用量、链路的质量、应用性能的稳定就显的尤为重要。

2、用户痛点

针对国内/国际分社的网络链路，实现 7*24 小时的链路用量、链路通信质量、网络连接状态的监控；对国际链路实现端到端的通断检测，链路异常/主备链路切换时，主动发出告警信息并提示故障节点；具备用户流量数据的可追溯、可分析能力；在重大事件中，提供快速、便捷的监控界面定制及高精度的实时监控、告警及分析能力等。

3、使用场景

场景 1：数据可视化

在 A 数据中心以及 B 数据中心的互联网区、核心区等关键区域部署 nCompass 的数据采集设备，利用集中管理器进行统一设计和数据管理。同时在移动通信车中，部署移动终端设备，用于重大事件保障工作的移动。在 A 数据中心与 B 数据中心，互联网区、核心区、生产办公区等关键节点做镜像点，镜像流量经过 TAP 设备统一整合后，由 nCompass 设备负责数据的采集并分析。

通过互联网区监控视图，可以全面地看到每条链路实时的状态。以链路的流入、流出吞吐量、丢包率、建连成功率，以及各出口链路流入、流出吞吐量的区域图、链路丢包的折线图的方式进行呈现。从下图可以明显看出，A 运营商两条出口链路状态发生明显抖动，同一时间链路的流量突然下滑，丢包率明显上升；反观 B 运营商两条链路的状态是非常平稳的。

基于机构关键核心业务，定制可视化业务端到端视图。从用户接入区、核心区、互联网区三个关键网络区域来监控，用户在发生故障时可快速定位故障出现在哪一个网络区域。如下图是专线上网端到端视图，真实的反应客户专线上网的各个区域的网络状态。从下图可以看到互联网出口流量有明显下降，服务侧丢包有明显增高。

场景 2：核心系统访问慢

通过系统的多项指标分析评估模板，可以快速分析故障是网络问题、应用问题还是主机性能问题。下图中可以看到该系统的用户数量、流量、丢包、网络连接在故障时间点，没有明显

的突增。但是应用性能在 9-11 点时有明显幅度的增加。

场景 3：主备线路无法区分

该机构全球有多个重要分社，各国际分社到总部有专线链路，以通过总社镜像流量的方式获取的数据的方式无法检验链路的实时状态。针对该问题，智维数据的方案采用了主动拨测结合 Netflow 的方式监控各分社链路的状态。通过以下拨测视图可以实时查看各分社链路的通断、质量、丢包状态，同时，还能结合 Netfolw 数据进行关联分析。

通过 Netfolw 的数据分析，可以实时查看各分社链路的流入、流出吞吐大小，并展示吞吐量 TOPIP 通讯对。当链路切换时，用户可快速感知并及时做出响应。

场景 4：重大事件保障

国家 70 周年国庆期间，某央媒机构作为国家通讯社，向海内外播发各种形式报道累计上万条，创历史新高。在此期间，智维数据提供了专业的技术支持和全力的配合,并在报道中进行了后方现场保障，持续监控移动报道网络平台，保障了流量监控系统的运行稳定。

场景 5：数据报告

为机构定制相关链路详情日报、周报、月报、以及一次性报表，用户可根据自身部门需求选择适合的报告模板。

场景 6：告警联动

基于指标的历史数据，系统支持通过对历史数据的学习预测未来数据的区间，可用于智能告警场景。当告警触发的时候，nCompass 流量分析平台将告警信息推送给第三方平台，再由第三方平台将告警信息推送给相关部门人员。

3.4 医疗行业

某大型综合医院

1、项目背景

该医院随着信息化的发展，部署了多个医疗信息系统，如：HIS、CIS、LIS、PACS、电子病历等系统。该医院欠缺的是应用可用性方面的监控，无法对本地业务可用性、性能评测、故障分析排查等方面进行直观显现。

2、用户痛点

现有的监控系统只能实现设备级链路异常流量的感知可用性监控，无法实现应用级、数据级的监控；由于数据中心的访问来自各个分院、大楼以及不同楼层的线路，当有故障发生时，无法快速判断故障是发生在客户端还是数据中心内部；目前只是对设备的可用性进行监控，缺少应用可用性方面的监控；业务监控、故障定位完全依赖人工，缺少智能化的分析平台与经验知识库支撑。

3、应用场景

场景 1：业务梳理

当应用系统出现异常需要排障，或是应用需要变更进行影响分析时，一份准确、真实的应

用拓扑图，往往能让工作效率得到极大的提升。如果通过人工维护拓扑信息，则需要极大的人力资源，并且极可能出现维护信息不准确的情况。

nCompass 流量分析平台基于真实流量数据，可快速生成应用系统的访问关系画像。支持多层级的扩展、聚合、过滤、检索、回溯、钻取等功能，可快速形成目标应用节点的实时、历史画像。并且能够把这些业务画像保存为基准画像，进行对比、分析和检测，及时发现新增或者是减少的业务访问节点。并且可通过保存业务的基准画像，制定对比分析和异常检测规则，为应用端到端追踪分析、渗透后的内网横向及纵向移动行为分析，提供真实、准确的数据支撑。平台会针对设置的监控策略，对业务系统进行对比分析，检测是否存在异常的访问行为，再根据这些信息进行进一步的验证。

场景 2：网络全局可视化监控

可视化能力是运维的核心能力，因为只有看得到才能谈管理。nCompass 平台提供全面的数据可视化能力，可集中呈现数据中心各个监控点的指标状态，也可基于网络拓扑定制出网络全局可视化监控，实时监控、呈现各关键网络实时运行状态，包括各客户端站点的用户体验、业务可用性、业务负载等关键状态信息。

只需要通过输入一个 IP 会话或者选择一个过滤条件，便可以清晰的看到这些数据流会经过哪些节点，通过对比节点的指标判断丢包或者网络时延大是在哪个节点发生的。在清晰的看到访问的数据流向的同时也可以看出这个数据流在数据中心内部有没有丢包。

场景 3：应用端到端监控

通过应用的端到端视图展现业务系统各节点的访问关系以及运行状态，做到实时监控。而且视图中的数据支持灵活的编辑、深度钻取等功能。对各核心业务系统进行业务逻辑梳理，形成各业务系统的端到端可视化监控。

能够通过一张视图完整呈现某个业务端到端的监控，当故障发生时可通过指标颜色以及数值的变化快速锁定故障节点，判断都有哪些用户受到影响、故障是由哪个节点发生、故障节点哪些指标异常等。而且用户通过点击可以快速链接到系统中内置的分析模板，便于分析和排查

问题。

场景 4：隐患排查

nCompass 流量分析平台能够主动找出异常事件，发现数据中心中即将发生的故障或者潜在隐患点，如异常跨区访问、高危端口触发流量、恶意扫描行为、主机违规外联、异常 DNS 请求、数据库错误码突增等行为。做到主动发现、及时解决。

场景 5：智能巡检

网络流量作为业务的载体，蕴含极其丰富的价值。nCompass 流量分析平台提供自动化的数据巡检能力，基于采集的数据，定期对数据中心进行全方位的数据巡检服务。能够主动发现数据中心的异常流量及隐患问题，如：内网中存在开启的高危端口、主机性能持续下降、应用服务错误率升高、内网存在高危域名访问、链路出现突发异常流量等问题。运维及安全人员通过事前的定期巡，发现隐患并及时处理，从而规避不必要的故障出现。

3.5 地产行业

某地产集团

1、项目背景

目前，该公司智慧服务已进驻全国多个城市，服务上百万户业主，数据中心作为核心保障部门面临着巨大挑战和压力。该公司目前运维处于工具化的阶段，注重基础设施的监控，对基础硬件设备采用基础网管、动环等手段监控；对应用内部程序的监控，采用 APM 作为主要监控手段。

2、用户痛点

在排查故障时往往需要各部门各自查看自身的监控，缺乏一体化监控，难以界定问题点出

在哪里；针对互联网及分支办公区专线访问数据中心网络链路质量的评估和管理，现阶段只能通过基础网管查看流量状况，无法评估流量质量以及突发的业务定位；公有云内部虚拟机之间互访关系和应用质量难以评估，出现故障无法快速定位。

3、使用场景

场景 1：统一监控分析视图

为实现统一监控、集中展示，该公司在数据采集方面收纳包括网络流量、基础网管、应用性能等数据，通过原始网络数据包及 API 获取相关数据进行分类管理入库。通过可视化界面配置现有监控工具 API 完成解码，其中包含网络层、应用层、主机资源层等指标的计算。通过对数据中心各区域进行多类别指标分析，对从数据中心入口途径的每个节点做统一分析，最终为该公司形成统一监控分析视图。

应用层：建连时间、响应时间、成功率等

网络层：流入吞吐量、流出吞吐量、丢包率、网络时延等

会话层：建连请求数、建连失败率、服务端 rest 等

主机层：CPU 使用率、内存使用率、磁盘 IO 使用率等

统一监控视图为该公司拟缩短了排查故障域的时间，节省了人力资源的消耗。

场景 2：链路质量监控

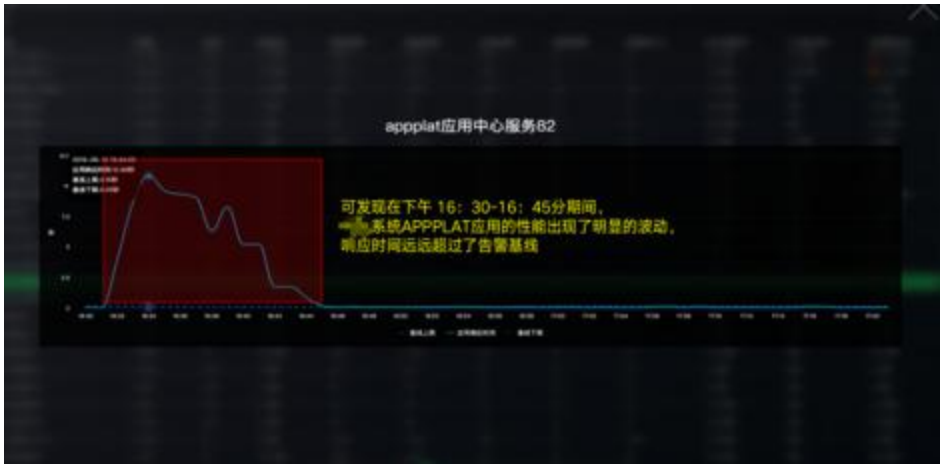
相关线路采用 Span 方式采集数据，并且通过精细的根因指标评估当前链路的网络质量，在发生网络异常时，快速定位出故障区域。监控指标不限于流入流出吞吐量，还包含客户侧延时、服务侧延时、客户侧丢包、服务侧丢包、连接状态、响应时间等。链路用量及质量能够做到设定自动生成报告，报告中包含峰值指标及波动趋势，实现精细化管理。

场景 3：全局调用关系视图

该公司阿里云内部监控采用安装 agent 的方式进行分析，重点做端到端分析，解决了难以

快速定位故障域的问题。

上图为该公司全局调用关系视图，网关服务、底层服务、微服务集群等各服务节点区域健康状态清晰可见，各服务节点均关联告警信息，当节点触发告警时，可以直观的看到颜色变化。



当触发告警时点击即可查看告警详情，以及告警关联的数据波动情况。锁定故障范围之后，若发现发现当前时段 APP 服务应用响应时间如上图一样出现明显上升。

nCompass 流量分析平台能够针对响应时间突增问题进一步分析，并得出如上图的结论“此问题为自身应用响应慢导致，不受网络和主机影响”。

由此可见，该公司基于 nCompass 排查此类问题，小于五个步骤即可完成问题定位。

3.6 物流行业

某大型物流集团

1、项目背景

该大型物流集团已建成整体网络架构。各类信息系统分散部署在各个数据中心。通过 F5DNS 产品做到全局流量分发，异地容灾。应用数据接入类型分为 VPN 接入和互联网接入两大类，以上传各类业务应用数据及业务。为实现网络质量监控、业务性能监控，提高故障定位效率，保障业务系统连续工作，急需引入先进、有效的网络及应用性能管理产品，帮助提高运维人员日常运维工作及故障响应的效率。

2、用户痛点

实现多套关键应用质量监控。包括多条运营商线路监控与专线链路监控；全局负载 GSLB 监控看板、互联网接入链路监控大屏、关键应用监控分析大屏、双十一监控大屏；建立完整的网络分析平台，提升事件分析能力；将原本简单的脚本式应用监控升级成为全量用户访问数据分析的应用监控方式。

3、使用场景

场景 1：互联网接入区网络性能监控看板

互联网接入区网络监控看板内容，为互联网接入区提供常态监控数据。

提供各条运营商链路监控指标数据，展示链路使用情况以及时延、丢包等链路质量数据。

为每条运营商链路展示各个 IP、TOP 各条链路内每个 IP 的网络吞吐量数据，提供完整的 IP 流量分析数据。

场景 2：GSLB 监控看板

对于互联网应用，全局 DNS 域名解析和流量调度，对保障客户端体验，应对突发状况有着重要作用。通过实时分析 DNS 应用数据，展示关键应用全局域名解析访问量、成功率等数据。同时区分不同客户端所在地域，以及客户端运营商信息，量化 DNS 应用质量。

通过全局 DNS 分析可帮助用户提供原始 DNS 应用访问性能数据。快速发现全局 DNS 质量较差地域或运营商 IP，通过数据分析帮助用户优化 GLSB 策略。最终达到提高客户体验的目的，提高 IT 服务质量。

场景 3：HTTP 关键应用监控分析

通过对各个应用全量数据实时分析，获取真实客户访问性能数据。

通过真实客户访问数据：成功率、访问量、响应时间等指标，量化应用质量情况。

系统内置“应用评分”指标，可以直观的展示当前应用质量情况。

3.7 IT 服务行业

某云计算及人工智能科技公司

1、项目背景

某云计算及人工智能科技公司，急需进行两方面提高：一方面是在高速扩张的过程中保障现有业务的稳定；另一方面提升现有客户的服务质量，建立良好的口碑效应。但该公司现有链路管理手段单一，希望寻找到一款产品能够帮助云服实现流量可视化，通过多维度全面监管业务流量。

2、用户痛点

网络内全流量无法量化，只能通过查看流量大小来进行监控；云平台用户的带宽占用情况无法进行有效划分；网络工程师对于应用或者业务系统无法做到有效监控；现有的大屏视图无法对当前业务系统的“好”与“坏”进行直观展示。

3、使用场景

场景 1：监控系统视图

下图中左侧展示目前业务系统的总体情况；右侧显示四条专线带宽质量；中间视图展示网络用量；下方展示业务系统好坏。能够清晰直观地反应出目前总体业务的真实情况。

场景 2：F5 监控视图

nCompass 流量分析平台能够与 F5 负载均衡厂商进行业内唯一的深层次数据互动，客户通过简单配置 F5，即可从 F5 上收集数据进行展示。

场景 3：链路监控视图

能够展示各专线链路质量，以及网络资源使用情况。

场景 4：各业务系统监控视图

nCompass 流量分析平台通过深层次的分析以及处理，把各业务系统的流量进行有效划分，实时展示各个业务系统的情况。

3.8 日用快消行业

美国某快销企业

1、项目背景

美国某快销企业，提高企业大中华地区数据中心网络的可视性和直观性，继而提升技术团队对各种应用问题，网络问题排错的用时和更规范的收集分析数据中心网络数据，进而更好更敏捷地支撑业务部门的促销活动，因此急需搭建一套数据中心网络可视化监控系统。

2、用户痛点

每次促销活动中，关键指标的关联与展示，提升运维团队应对各种网络问题，应用问题的排查效率，同时能为领导小组的营销决策提供全面的数据参考；数据的可视性，直观性，作为一个高度重视 IT 投入的高科技企业，也急需一批能与其 IT 水平相当的可视化大屏展示视图。

3、使用场景

场景 1：用户体验可视化监控

下图为 nCompass 设计的用户体验监控视图，其中主体的地图用来体现用户的分布，在线人数越多的区域地图亮度越高。顶栏主要提供总体用户体验值，体验较差中断用户的占比，在线用户数，实时下单数等概览指标。主视图两边根据实际情况，显示体验最差的 TOP 城市，单数最多的城市等信息。

通过该数据视图，业务部门领导在促销活动时，能直观的掌握交易活跃及潜力较大的城市群，为广告及宣传资源投放提供参考依据。同时，运维部门能直观的掌握每个地方用户访问体验。一旦发现某地区访问质量下降，即可快速结合主动拨测页面，快速诊断是远程运营商网络问题，还是 CDN 问题或是数据中心问题。为故障快速分诊，定位调度提供统一、便捷的监控中心。在促销过程中，通过用户体验可视化监控中心，一旦发生故障，可快速分诊、定位。当问题范围划定在数据中心时，运维人员需要及时进行排查。下面一场景将展示如何实现数据中心网络可视化监控。

场景 2：数据中心网络可视化监控

在促销期间，一旦发现故障，则运维人员需要快速进行排查。而一般情况下，网络组会首先关注互联网链路的使用情况，关键设备的使用状态(CPU、内存、告警等)。而这些信息一部分已经通过网管设备以及日志采集平台进行收集。

nCompassTDA 通过与网管设备的 API 以及日志平台的 API 进行对接，实现数据的集中采集与关联。下图是相关链路与设备状态的监控视图。左侧条框动态轮播每个设备的当前状态，包括 CPU、内存、吞吐量、连接数等信息。一旦设备状态出现异常就会触发告警。主体拓扑的相关图例会通过变红，变橙等方式显示告警的严重程度。

3.9 教育行业

某教育机构

1、项目背景

作为全国性质的考试及相关服务单位，面对集中式的高并发访问，容易造成系统压力过载，从而引发一系列的连锁“故障”。目前的监控系统无法满足对 F5 设备的数据和应用转发进行有效监控。为了保证日益增多的考试系统能够平稳安全可靠地运行，急需引入能够快速部署的、可以对 F5 设备所承载业务监控、可以对网络及应用性能进行管理的产品。

2、用户痛点

业务自身调用其他系统或接口越来越多，业务系统之间的前后访问关系难以梳理；无法对业务和用户使用的情况进行精确监控，无法直观的显示业务的运行状态，并快速的定位问题节点；系统出现故障时，缺乏溯源手段，无法对发生过的问题进行回溯分析；如何在未发生故障时通过自助巡检发现数据中心存在的隐患，将问题扼杀在萌芽状态。

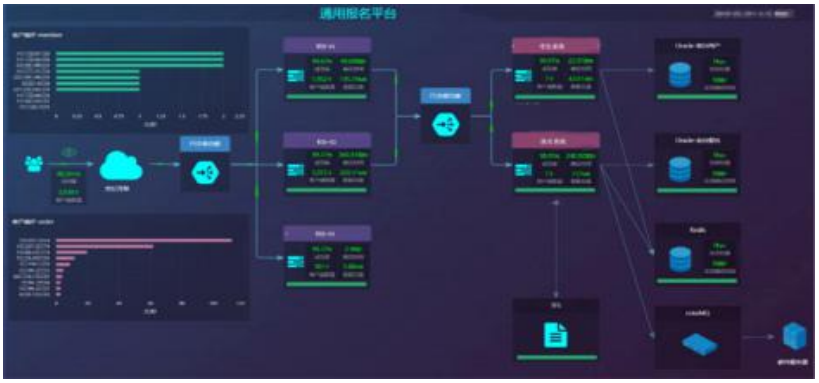
3、使用场景：

场景 1：相关平台业务梳理

通过应用梳理功能，基于某平台系统在外层 F5 上 VS 的地址，自动发现并梳理出了系统内部及外部的访问关系，完成了跨地址映射的数据关联。

场景 2：相关系统大屏展示

基于几套关键考试系统定制可视化分析视图，每套可视化视图皆为从公网入口至后端 APPServer 的每一个节点均可独立下钻分析(网络层、应用层、主机性能层)，用户在发生故障时可快速直观的定位出故障域。



场景 3：用户全国分布及各区性能状态图

通过监控平台，可以很直观的发现该相关业务系统发生性能异常，严重影响业务办理。通过数据下钻，我们发现有部分 URL 的响应延时达到了 10 分钟。通过 Tomcat 问题修复和服务器扩容以后，业务性能明显提升，业务平均处理时间在毫秒级。

场景 4：相关查询系统监控-查询系统怀疑有攻击

查询系统访问量突增，上午查询的 QPS 高峰保持在 2k 左右，下午从 4kQPS 一直飙升到 7kQPS，并且单 IP 高达 3kQPS。怀疑有攻击行为。查询 QPS一直飙升，通过和 TOP3 的客户端进行对比发现查询曲线基本一致。