n-compass

nCompass

产品介绍

www.ncmps.com

400-666-8216

目录

第一章 运维现状

“业务正在不断的驱动着 IT 运维管理朝着以应用及数据为中心发展，与此同时，应用也变得越来越难于管理。”

—Gartner

“关键复杂应用不具备高性能和高可用性将直接给业务生产力，业务收入和 IT 效率造成负面影响。”

—Forrester 咨询机构

时至今日，各个企业 IT 建设的规模与复杂度与日俱增，信息化标准水涨船高，IT 应用模式日新月异，基础架构及应用模式的革命性变化给 IT 管理带来了巨大的挑战。IT 运维管理不仅要对传统基础资源的运行状况负责，更要对承载于其上的应用、业务运行的性能与质量负责。数据的可视化展示及智能化分析的能力，尤其是基于 AI 算法的自动化运维能力，已经逐渐成为各个企业 IT 运维管理的重要研究课题。

【业务模式逐渐从线下走到线上，这对 IT 系统的高可靠及稳定性提出了更大的挑战】

国内各行业的 IT 信息化建设正处于高速发展阶段，业务量与日剧增，伴随着数据大集中，及越来越多的业务系统陆续上线，信息部门作为业务核心保障部门面临着巨大挑战和压力。由于各种关键业务和应用都被承载在基础架构、WEB 应用、中间件和数据库上，同时业务系统上线需实现快速、灵活、按需的可插入式部署能力，这使得业务的复杂性和维护难度大幅增加。如何对这些复杂的业务系统进行有效监控和风险防范，保障关键业务的高性能和高可用性，以及如何对现有的运维流程进行优化，不断提升管理和运维水平已经成为目前数据中心急需探索和解决的重要问题。

目前用户主要面临的问题如下：

1. **运维管理被动，运维人员长期处于救火的工作模式中**：经过多年的努力，基础架构层已经具备了一定的监控能力，比如硬件的工作状态、系统的资源使用分布、进程的运行状态等。但是当用户访问出现问题或者即将出现问题时，现有的监控体系还是难以及时发现问题，故障出现往往是用户或业务人员先发现，运维人员

后知后觉疲于奔命的解决。缺乏事前的隐患消除及异常事件的预警机制是导致运维被动的主要原因。

2. **IT 建设发展迅速，现有的人力资源跟不上 IT 建设的步伐，需提升自动化运维的能力**：随着业务需求的多元化，业务部门对网络、应用提出了更高的要求。新系统上线的频率及网络和应用的变更频率越来越高，设备数量越来越多、应用数量越来越多、应用的架构也越来越复杂，如何在现有人力资源的能力范围内，通过自动化的工具，协同应对这种变化，成为众多企业正面临的难题。

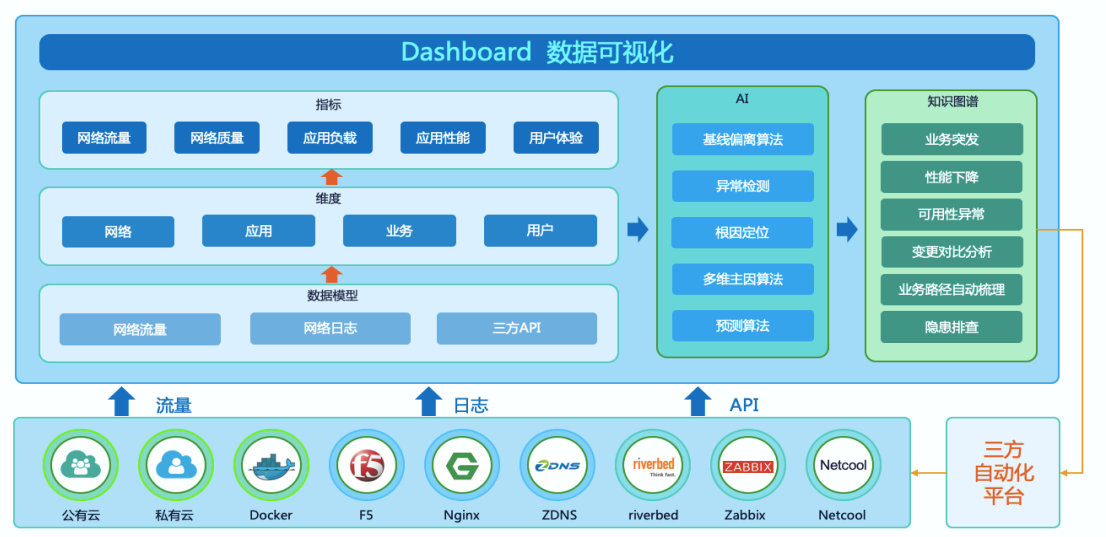
3. **突发异常事件处理效率不足：**信息系统架构随着业务需求不断变化，应用节点的数量及应用系统之间逻辑调用关系越来越复杂，所需运维的环节众多。而监控系统相对独立，一旦出现问题，网络、主机、系统、中间件、数据库、存储等部门人员分头查找原因各自为战，出现取证难、效率低，甚至互相推诿的问题。突发事件处置缺少明确方向，一方面需要付出较多沟通和定位问题的时间成本，另一方面导致事件处理时间过长，影响被放大。

鉴于以上情况，北京智维盈讯网络科技有限公司的 nCompass 数据可视化分析平台帮助客户实现运维从工具化向自动化、智能化方向的演进。从用户的实际情况出发，以数据作为切入点进行面向业务的数据可视化分析，解决目前运维管理中面临的一些实际问题。达到提升业务连续性管理水平，提升运维管理水平，从而最终提升 IT 服务质量及用户满意度。

第二章 产品介绍

2.1 nCompass 数据可视化分析平台介绍

nCompass 数据可视化分析平台，可实时采集分析网络中的流量数据及应用系统的日志数据，实现主动式隐患巡检分析、用户访问体验监控预警、基于 AI 智能算法的故障根因分析等功能。从而实现全面的运维自动化，自动化巡检、自动化的异常监控、自动化的故障分析定位、自动化的运行报表，通过数据及计算能力，释放人力资源、提升工作效率。



【nCompass 数据可视化分析平台架构】

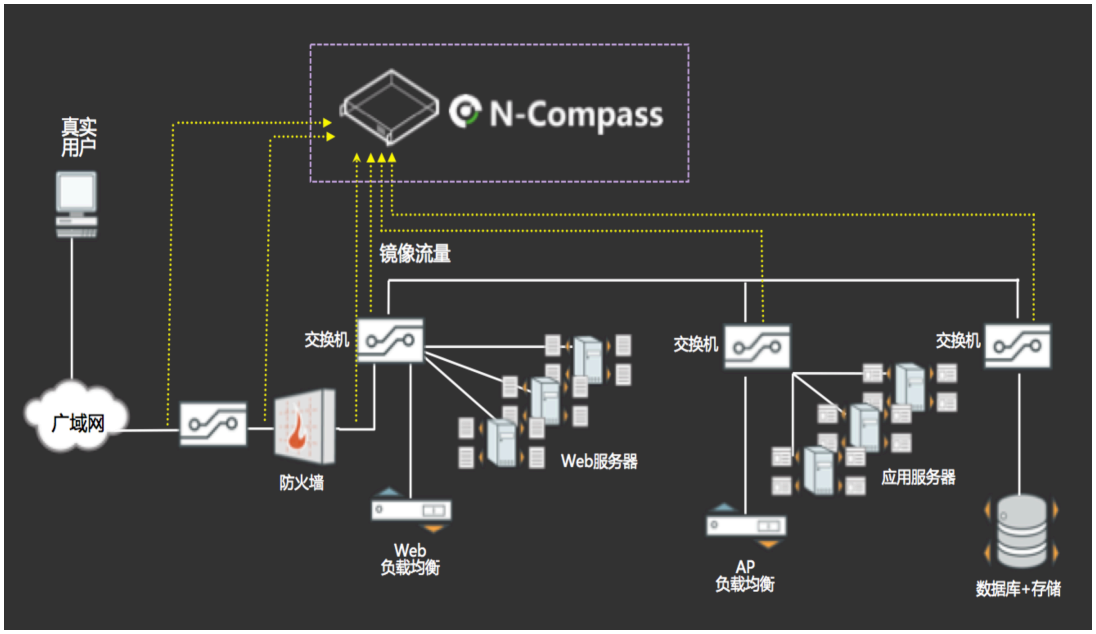
2.2 方案部署

nCompass 数据可视化分析平台以硬件或软件的形态部署在用户的数据中心，基于采集网络中的流量及日志数据，实时监控、分析数据中心出现的异常事件。

基于用户数据中心环境不同，主要分为以下几种部署方式：

2.2.1 数据中心物理环境部署

在非云化数据中心，nCompass 可以用软硬一体化设备的方式部署，通过从物理交换机获取网络流量数据并对流量进行实时分析，用于发现及分析网络中出现的异常事件。



【nCompass 物理数据中心部署架构】

2.2.2 私有云环境部署

nCompass 可部署在用户的私有云环境，不论是 Vmware 还是 KVM 等私有云环境，均可通过虚拟交换机采集流量数据。

1. VMware VSS 环境：

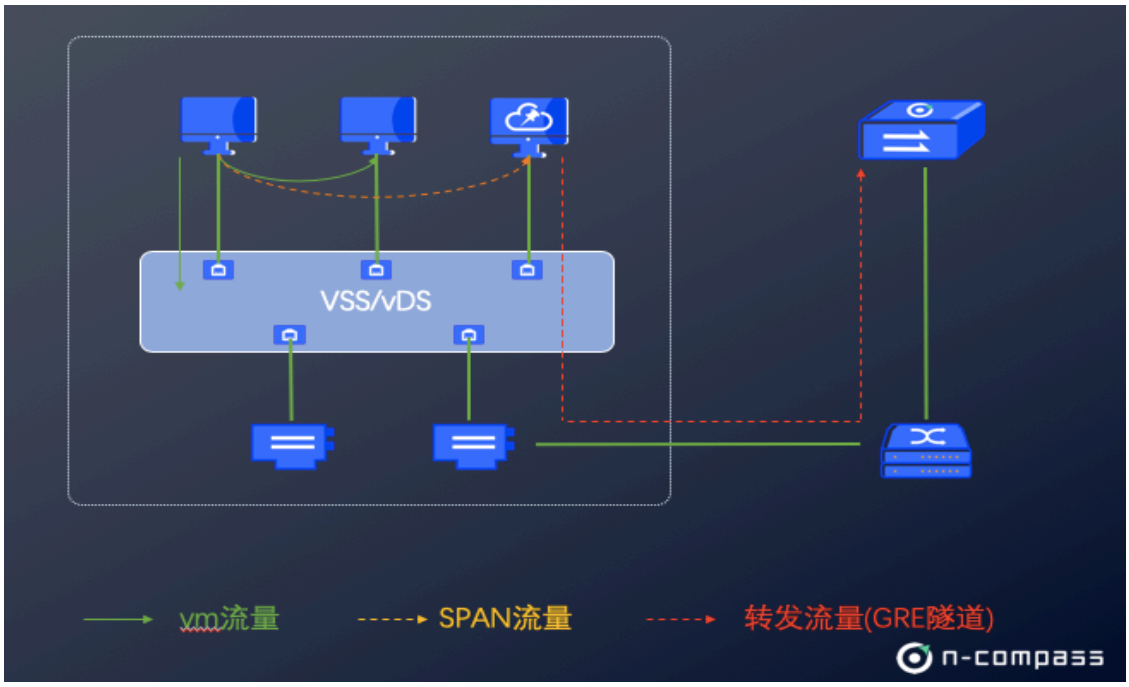
- 可以通过创建 VGT 端口组采集流量。VGT 端口组设置混合模式可以接收所有 VLAN 数据，不需要更改每个 VLAN 的工作模式。

- 在每台宿主机上安装一个云探针虚拟机采集 VGT 端口组流量，即宿主机上所有虚拟机的流量，然后通过 GRE 封装原始流量，转发到 nCompass 探针节点解封装、存储、分析和可视化。

2. VMware VDS 环境：

- VMware 虚拟机使用分布式交换机支持镜像功能，可以通过创建端口镜像采集流量。

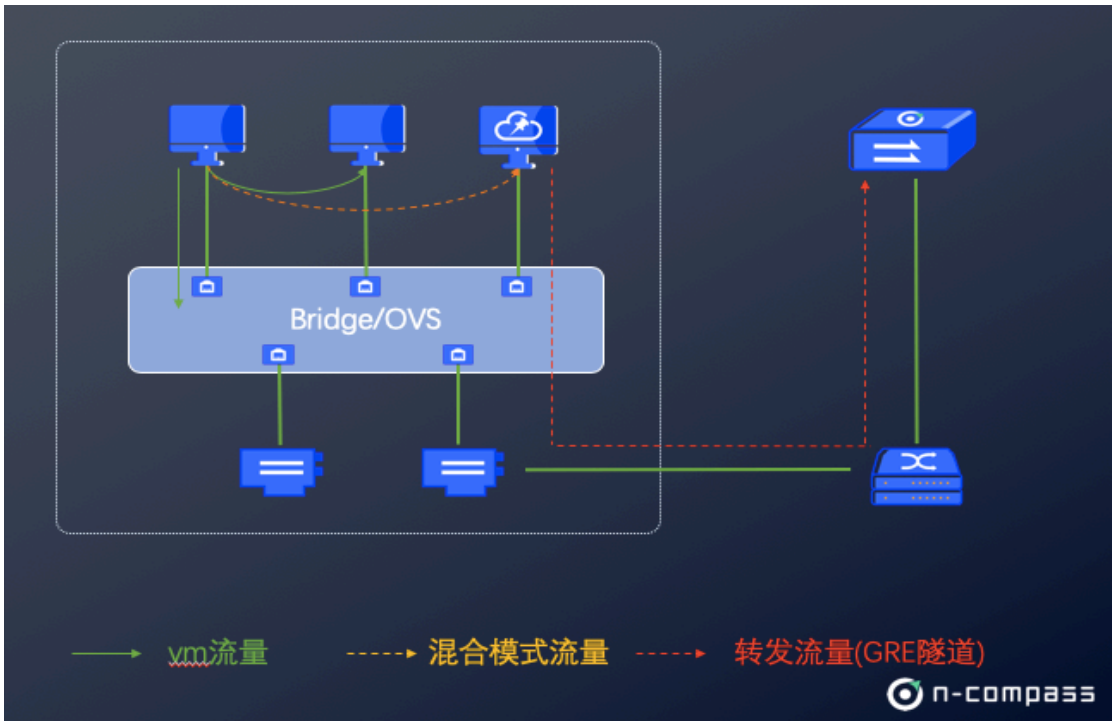
- SPAN 模式需要在每台 esxi 上安装一台虚拟机接收其它虚拟机的流量，并在这台虚拟机上安装云探针，采集所有虚拟机流量并转发。



【nCompass VMware 私有云环境部署架构】

3. OpenStack 环境：

- OpenStack 平台采用 KVM 虚拟机化，使用 Linux bridge 模式，类似 VMware 的 VSS，但是不具备类似 VGT 的端口组模式，需要在物理网卡设置混合模式，在每个 KVM 上创建一个虚拟机用来安装云探针，采集其它虚拟机流量并转发。
- OpenStack 平台采用 KVM 虚拟机化，使用 OVS 模式，类似 VMware 的 VDS，也具备端口镜像功能。SPAN 模式和 VMware 的 VDS 一样。

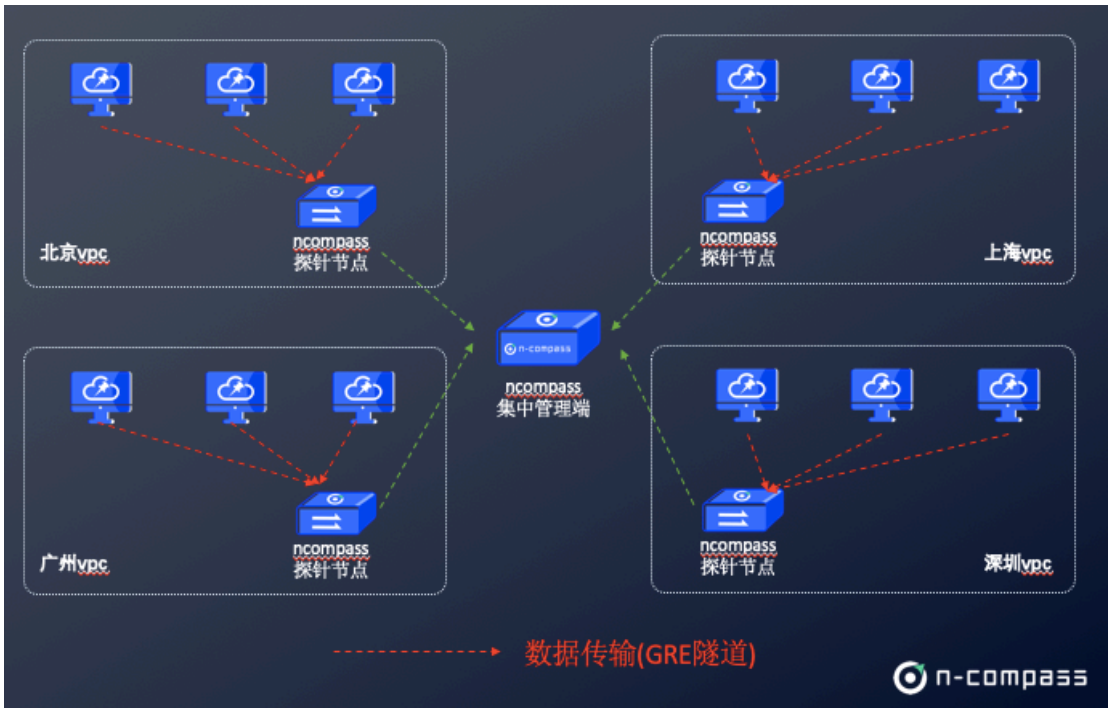


【nCompass OpenStack 私有云环境部署架构】

2.2.3 公有云环境部署

当前阿里、腾讯和百度的公有云目前暂不支持流量镜像，所以公有云部署需要在每个公有云 VPC 中安装一套管理端，并在每个 VM 中安装 Agent 用于采集 VM 的流量。

- 在每个 VPC 的虚拟机上安装 nCompass 云探针;
- 每个 VPC 里创建虚拟机安装一套 nCompass 探针节点，接收来自云探针的流量；
- 如果有多个 VPC，需要再安装一套 nCompass 集中管理系统。



【nCompass 公有云环境部署架构】

2.3 平台所支持的数据类型

nCompass 数据可视化分析平台支持多源数据采集及实现数据整合分析、呈现的能力。主要支持的多种数据源包括网络镜像流量、Netflow、主动拨测、网络设备的访问日志，以及三方平台的 API 接口的时序、告警或配置数据。平台目前已支持的数据类型如下：

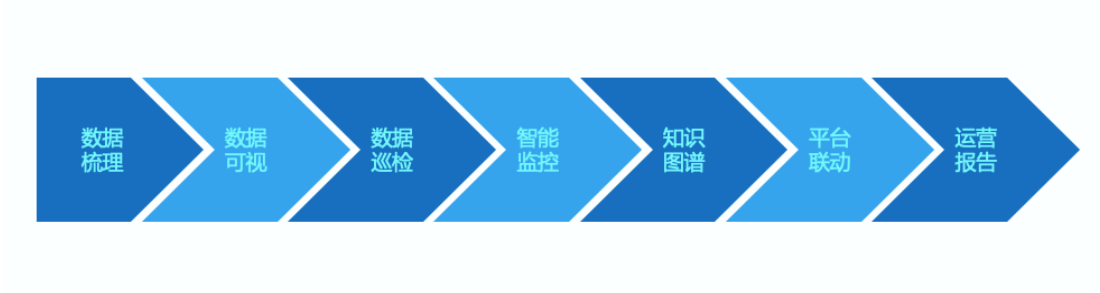
- 物理交换机镜像流量
- SDN 虚拟交换机镜像流量
- 公有云虚拟机云探针采集流量
- Netflow 数据
- 主动拨测数据
- F5 iControl 配置管理数据及 HSL 会话日志
- Nginx 日志
- HAProxy 日志
- ZDNS 日志
- Imperva 告警事件日志
- 山石网康防火墙及 VPN 日志
- Juniper telemetry 日志
- Zabbix 告警日志

- 博睿 SDK API
- 博睿 Server API
- 微步威胁情报
- CMDB 资产管理信息

nCompass 数据可视化分析平台已支持的数据采集类型详情，请参见 6.1 章节

2.4 功能概述

nCompass 的解决方案主要包括如下 7 个重点功能：



2.4.1 数据梳理

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。用户的数据中心运行着几十、上百套应用系统，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 基于真实业务调用访问数据，自动生成各应用系统的真实、准确的应用拓扑图。并且当应用出现变更，如新增应用节点或访问关系

发生变化时系统可自动更新拓扑。nCompass 主动感知应用的变化情况，为应用端到端追踪分析提供真实、准确的数据支撑。

2.4.2 数据可视

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。如何消除可视化盲区，是众多用户的需求所在。nCompass 平台提供全面的数据可视化能力，既可集中呈现用户访问数据中心的用户体验状态，也可基于应用梳理结果定制出应用端到端可视化监控，实时监控、呈现各关键应用系统的实时运行状态，包括各应用节点的用户体验、业务可用性、业务负载等关键状态信息。同时 nCompass 数据可视化模块支持接入三方数据，可以接入用户现有运维工具的数据，实现运维数据大集中，完成数据的统一治理、统一分析、统一监控、统一呈现、统一报表等功能，从而为运维自动化、智能化提供坚实的基础。

2.4.3 数据巡检

网络流量作为承载业务的载体，流量中蕴含极其丰富的价值。nCompass 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。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检，发现隐患并及时处理，从而规避不必要的故障出现。

2.4.4 智能监控

目前众多用户主要的监控方法，还是基于基础架构层的硬件、资源监控，如各机房的设备实时运行效率。这类监控系统可以针对我们肉眼可见的设备运行状态进行细粒度的监控，但是对于设备所承载的业务系统的服务质量、用户体验缺少监控能力。这就使得业务访问异常时，监控系统并未发现，而是业务部门率先发现。从而说明目前的监控体系仍然存在盲区，运维部门往往非常被动。IT 是技术支撑部门，服务的对象是企业内部员工及广大互联网用户，nCompass 的监控理念是:搭建一套以用户为核心的监控体系。nCompass 借助网络承载应用、业务及用户访问的特性，从网络流量中实时抓取用户的每一次访问，通过解析网络数据，得到全量的用户体验数据，通过用户的真实访问数据，来监控数据中心关键应用系统的运行状态，当真实用户访问出现异常时，运维人员可以及时的感知到，可以及时处理，降低故障的影响。

2.4.5 智能分析

当出现故障需要分析时，较为依赖运维人员的能力、经验，但是随着应用节点的数量及应用系统之间逻辑调用关系越来越复杂，监控系统也相对独立，出现问题后涉及众多部门，网络、主机、系统、中间件、数据库、存储等人员分头查找原因，各自为战，出现取证难、效率低，甚至互相推诿的问题。突发事件处置缺少明确方向，一方面需要付出较多的沟通和定位问题的时间成本，另一方面导致事件处理时间过长，影响被放大。nCompass 支持 AI 算法库及知识图谱，系统内置机器学习、异常检测、多维主因素、事件关联分析、预测等智能算法，同时内置覆盖众多故障场景的知识图

谱，当系统产生告警事件后，系统可进行自动的智能分析，并提供分析结论报告，自动定位故障的根因，提升异常突发事件的处理效率。

2.4.6 平台联动

运维自动化的最终目标是实现故障的自愈。nCompass 平台脚本化的多平台联动能力，当数据中心出现异常事件时，可远程调用相关设备或系统，实现故障的自愈。

2.4.7 数据报告

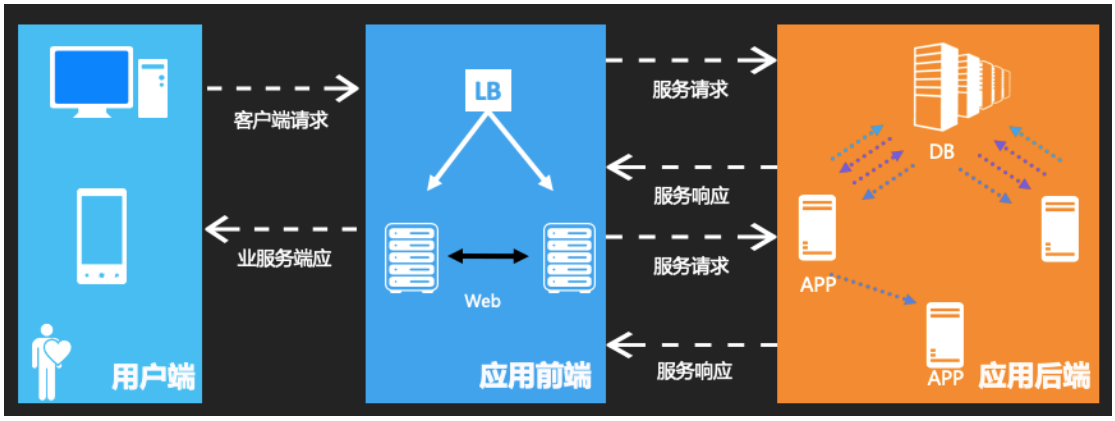
nCompass 平台支持自定制的数据报告功能，同时内置常用模板以及灵活的自定义报表系统，可以按照不同客户、不同人员、不同场景实现灵活多样化的报表，如定期生成基于应用服务质量排名及优化监控报告等。同时支持按计划自动生成可归档的短期、中期、长期报告（日报、周报、月报），并提供生成报告的类型及报告的格式和主体内容。

第三章 用户使用场景

3.1 重大事件保障

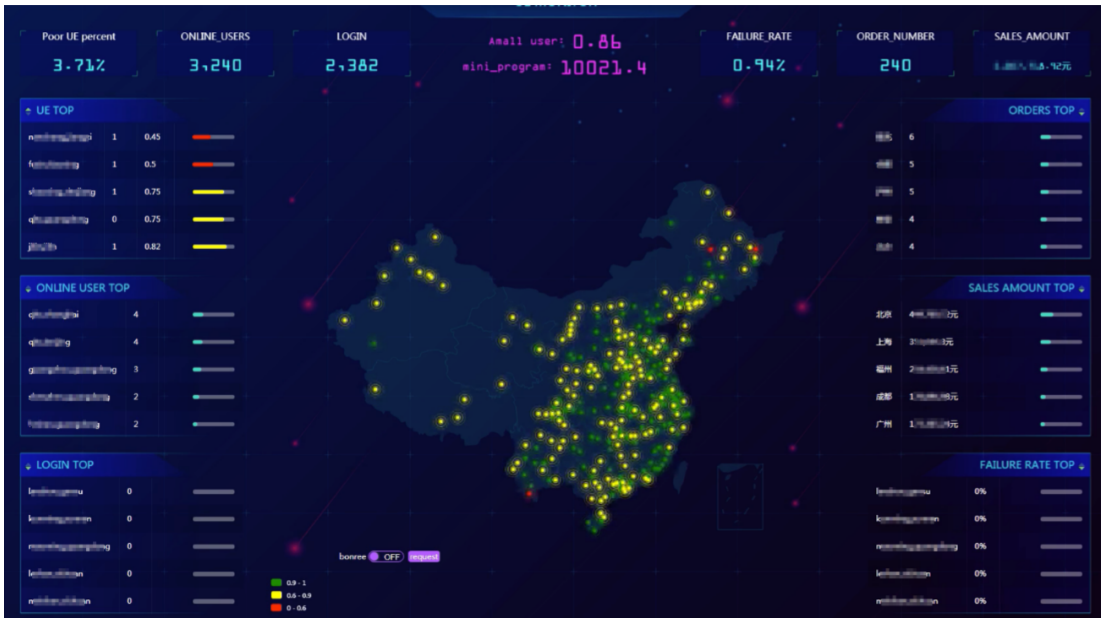
用户体验正逐渐成为各行各业 IT 运营部门领导最为关心的问题，因为用户体验的好坏可能直接决定企业的生存问题。业务从线下走到线上，最终用户可以足不出户的完成各种交易。那么当 IT 系统的稳定性、性能达不到用户的要求时，往往就会产生大量的用户流失，而这个损失的挽回往往是需要花费很大的成本。

nCompass 解决方案借助网络承载最终用户访问的特性，对用户访问应用所产生的网络流量数据进行深度分析，可实时监控用户访问数据中心各应用系统的实时用户体验状态。



【用户发起一笔业务的流程示意图】

nCompass 通过在网络的关键节点部署监控点，通过对网络流量的解码分析，实时计算出用户访问业务系统的可用性及性能等指标，并基于多个指标综合计算出用户体验 Apdex 值。下图为某快销行业的用户体验监控大屏，其中界面中间主体部分是一张用户体验热力图，通过不同的指标和维度实时查看用户分布及用户体验情况。



【nCompass 业务交易及用户体验监控大屏】

在业务促销、秒杀等活动中，IT 运营部门往往最为关注业务可用性及用户体验，上图的业务交易及用户体验监控大屏，可提供高精度的指标计算，如：

- 实时在线用户数
- 用户体验 Apdex 值
- 用户分布
- 关键业务可用性
- 关键业务负载
- 关键业务性能
- 实时交易金额

在重大活动中，该界面可实时呈现 IT 运营部门关注的各个维度的信息并提供高精度的实时刷新能力。一旦发现某地区访问质量下降可快速诊断并修复问题，提升突发事件的响应处理效率，规避因 IT 故障导致的企业金钱损失及用户损失。

同时 nCompass 通过与用户现有网管平台、日志平台对接，实现多源数据的集中分析与展现。不仅可以对最终用户体验进行监控也可以对多数据中心基础架构进行实时监控。下图则是基于某企业的 IT 基础架构，端到端的呈现各关键节点设备的实时运行状态。包括：互联网链路的用量及数据传输质量，互联网区核心网络设备的硬件及资源负载状态，防火墙设备的实时负载及资源使用状况，负载均衡设备的实时负载及资源使用状态等。一旦设备状态出现异常就会自动触发告警并及时通知运维人员快速处理。

【数据中心关键设备监控界面展示】

通过数据中心网络可视化视图，运维人员能第一时间直观的看到每个设备以及每条链路当前的运行状态。在业务大促争分夺秒的场景下，能将用户体验监控视图与数据中心架构监控视图结合起来进行分析，快速定位问题大大提升了突发故障响应效率。

作为监控大屏，不同用户有自己的审美标准。所以固化的监控界面是不能满足所有用户的需求。nCompass 提供一个快速 Dashboard 创建的功能，让 IT 运营人员可通过鼠标的拖拽等操作快速完成所需的视图，满足不同用户的审美。同时还可以支撑任意场景下的大屏监控需求。

【nCompass 视图编辑界面】

在 nCompass 的视图编辑功能中，系统预制了 80 余种 2D/2.5D 可视化控件供用户选择，实现监控大屏级别的视图快速定制。

秉承基于角色的数据场景化分析， nCompass 为用户提供了美观且灵活的数据可视化功能。基于 nCompass 专业工程师们常遇到的数据可视化场景，系统内置了数百套可视化模板界面。用户无需过多的配置或者定制可直接使用数据进行监控或分析。

【nCompass 视图中心】

视图提供两种呈现方式，上图为简版呈现。nCompass 针对每个视图的使用场景、包含的数据内容等信息都进行了详细描述，这样用户使用视图时可通过关键词检索，快速找到适合的分析视图。

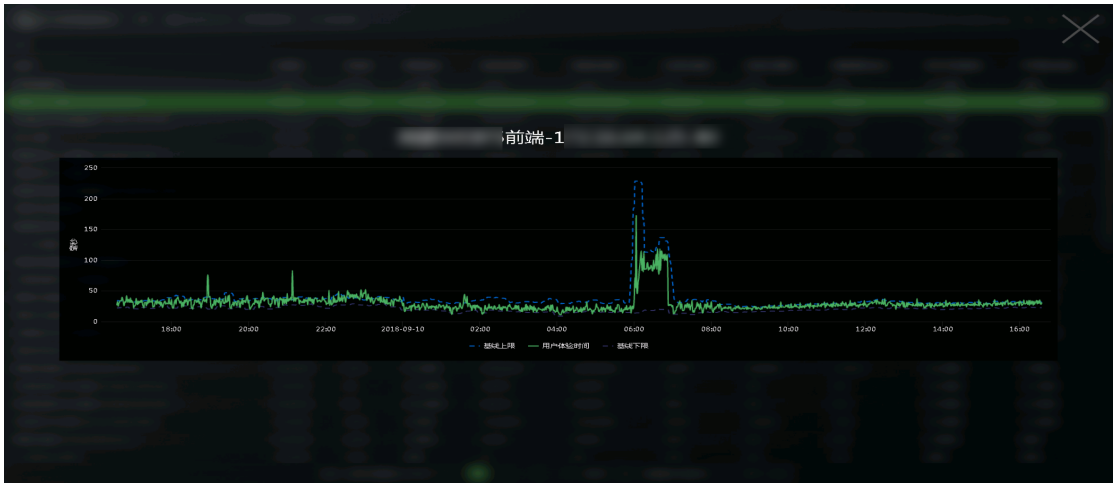
【通过视图描述关键词快速检索对应的视图】

基于 nCompass 灵活、便捷的监控视图编辑器，可快速帮助用户完成监控大屏的绘制，满足各个用户的个性化需求。

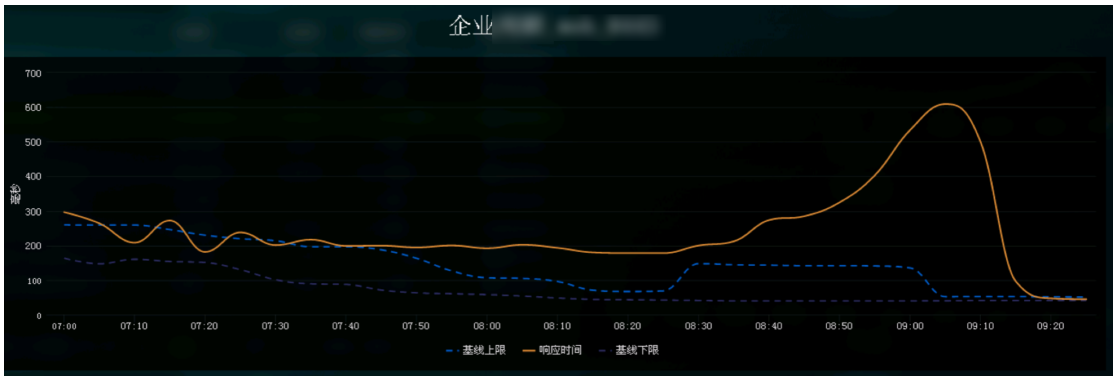
【nCompass 部分监控界面展示】

3.2 日常监控

nCompass 数据可视化分析平台拥有众多的监控维度及监控指标，提供灵活的告警。首先从监控机制上，nCompass 采用了基于机器学习的智能监控方式，所有的指标统计完成后会进行自学习，基于历史数据自动形成告警基线，避免了告警策略人工配置工作量大、不准确、误报率高的问题。

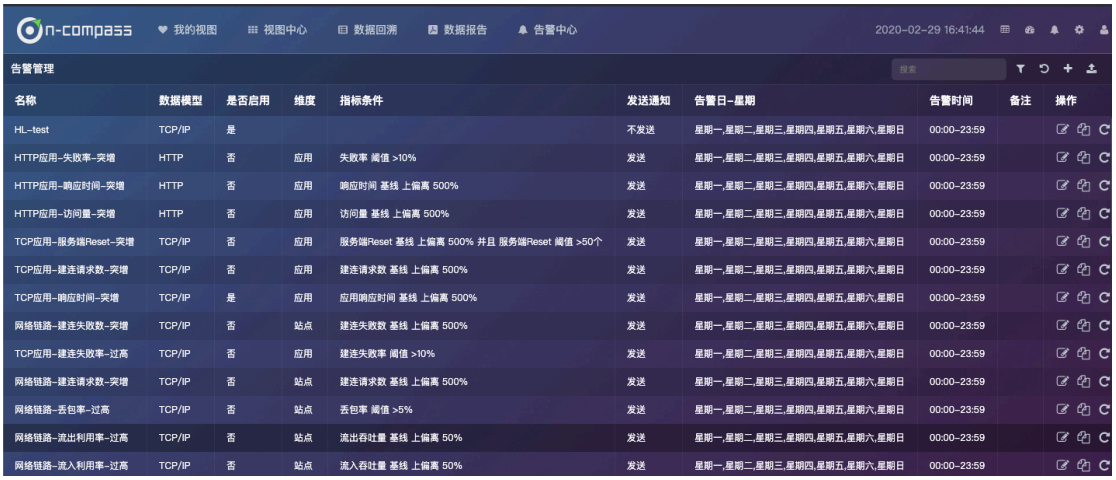


【nCompass 机器学习算法可识别正常的突发，并自动调整告警基线】



【因真正故障所导致的突发，nCompass 会精准识别】

用户可基于不同指标的基线上、下的偏离度设定告警，进一步提升告警的准确性。同时，nCompass 数据可视化分析平台针对主流的监控场景预置了常用的告警，如：链路流量突发/突降、链路传输质量异常、链路网络连通性异常、Web 应用可用性异常、Web 应用突发访问、Web 应用性能下降等。同时针对 DNS、Oracle、Mysql、SQLServer 等主流应用均预设告警。nCompass 所支持的监控指标，详见 6.2 章节。



名称	数据模型	是否启用	维度	指标条件	发送通知	告警日-星期	告警时间	备注	操作
HL-test	TCP/IP	是			不发送	星期一,星期二,星期三,星期四,星期五,星期六,星期日	00:00-23:59		
HTTP应用-失败率-突增	HTTP	否	应用	失败率 阈值 >10%	发送	星期一,星期二,星期三,星期四,星期五,星期六,星期日	00:00-23:59		
HTTP应用-响应时间-突增	HTTP	否	应用	响应时间 基线 上偏离 500%	发送	星期一,星期二,星期三,星期四,星期五,星期六,星期日	00:00-23:59		
HTTP应用-访问量-突增	HTTP	否	应用	访问量 基线 上偏离 500%	发送	星期一,星期二,星期三,星期四,星期五,星期六,星期日	00:00-23:59		
TCP应用-服务端Reset-突增	TCP/IP	否	应用	服务端Reset 基线 上偏离 500% 并且 服务端Reset 阈值 >50个	发送	星期一,星期二,星期三,星期四,星期五,星期六,星期日	00:00-23:59		
TCP应用-建连请求数-突增	TCP/IP	否	应用	建连请求数 基线 上偏离 500%	发送	星期一,星期二,星期三,星期四,星期五,星期六,星期日	00:00-23:59		
TCP应用-响应时间-突增	TCP/IP	是	应用	应用响应时间 基线 上偏离 500%	发送	星期一,星期二,星期三,星期四,星期五,星期六,星期日	00:00-23:59		
网络链路-建连失败数-突增	TCP/IP	否	站点	建连失败数 基线 上偏离 500%	发送	星期一,星期二,星期三,星期四,星期五,星期六,星期日	00:00-23:59		
TCP应用-建连失败率-过高	TCP/IP	否	应用	建连失败率 阈值 >10%	发送	星期一,星期二,星期三,星期四,星期五,星期六,星期日	00:00-23:59		
网络链路-建连请求数-突增	TCP/IP	否	站点	建连请求数 基线 上偏离 500%	发送	星期一,星期二,星期三,星期四,星期五,星期六,星期日	00:00-23:59		
网络链路-丢包率-过高	TCP/IP	否	站点	丢包率 阈值 >5%	发送	星期一,星期二,星期三,星期四,星期五,星期六,星期日	00:00-23:59		
网络链路-流出利用率-过高	TCP/IP	否	站点	流出吞吐量 基线 上偏离 50%	发送	星期一,星期二,星期三,星期四,星期五,星期六,星期日	00:00-23:59		
网络链路-流入利用率-过高	TCP/IP	否	站点	流入吞吐量 基线 上偏离 50%	发送	星期一,星期二,星期三,星期四,星期五,星期六,星期日	00:00-23:59		

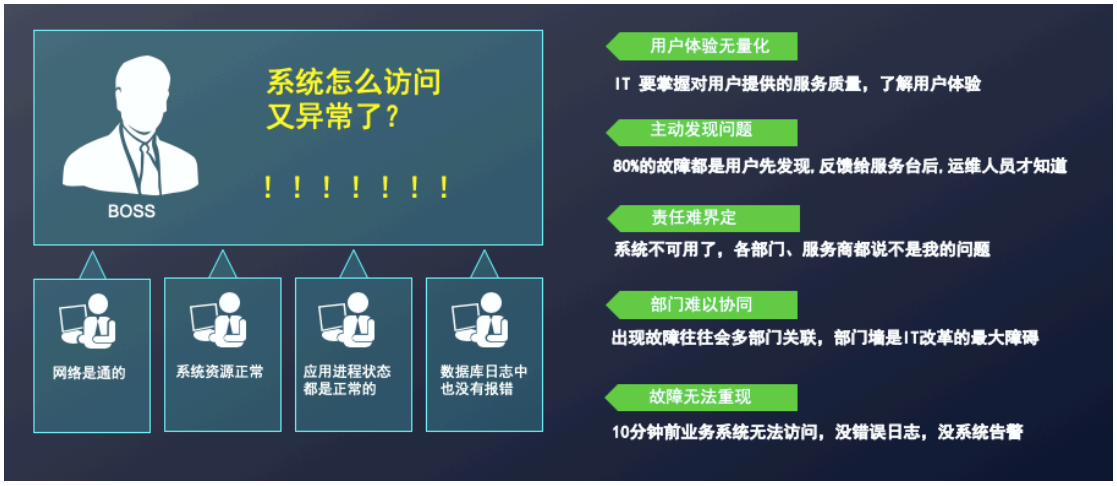
【告警策略管理界面】

告警的准确性随数据学习周期的累加不断提升。基于此 nCompass 提供了告警回放功能，以便在告警设置初期尽量保证告警的准确度。在告警配置完成后，立即在历史数据中运行一遍并将结果呈现给告警配置人员，用于判断当前告警设置的基线、阈值是否会出现过多的误报。

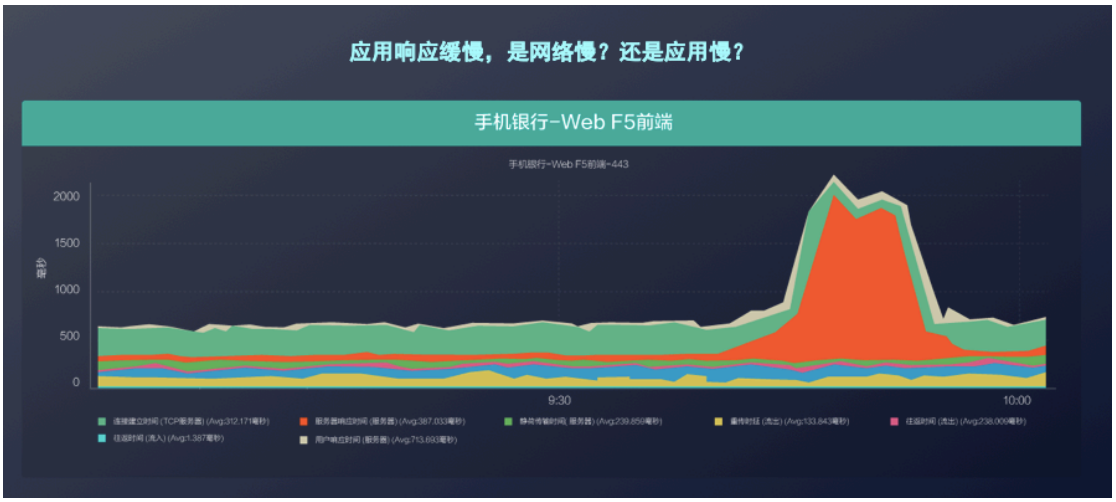
【告警模拟测试界面】

3.3 故障责任快速界定

在当今复杂的应用架构下，当业务系统运行异常时往往需要多个部门的专家组成“WarRoom“来共同分析故障。房间内可能不仅有用户方的网络、应用、系统、安全等多个部门的人员，同时还可能有服务商、软件开发商、各设备厂商的人员。如何快速进行故障责任界定、快速定位出是网络导致业务异常还是安全攻击事件，是众多用户关注的问题。对于网络部门来说，在这个场景中往往很容易成为背锅侠，只要业务出问题就是网络问题已经成为很多 IT 人员的惯性思维方式。

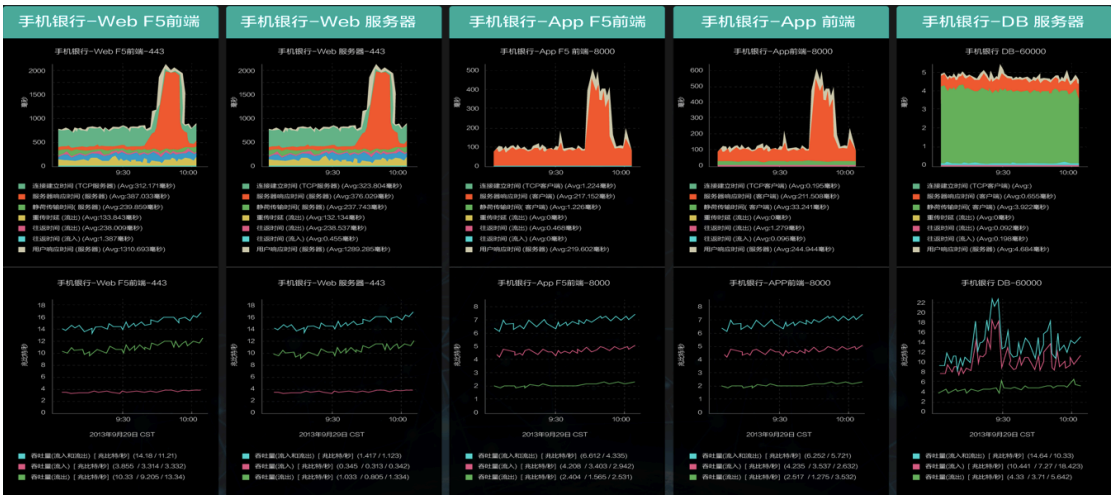


nCompass 数据可视化分析平台可以帮助用户通过数据说话，快速进行责任的界定，定位故障的根因，从而避免责任推诿现象的发生。如下图示例，业务系统响应缓慢，通过系统内置的性能可视化分析控件，可快速定位是网络原因、还是应用原因。图例中展示了手机银行应用的实时性能状况，nCompass 通过性能切片技术，对应用交互的各个阶段的时间进行切包，包括网络建链时间、丢包重传时延、客户端主机时延、服务器主机时延、应用响应时间，每种指标对应下图中的不同颜色。当性能异常时，我们只需要看时延分布在哪个指标所对应的颜色上，即可定位故障。



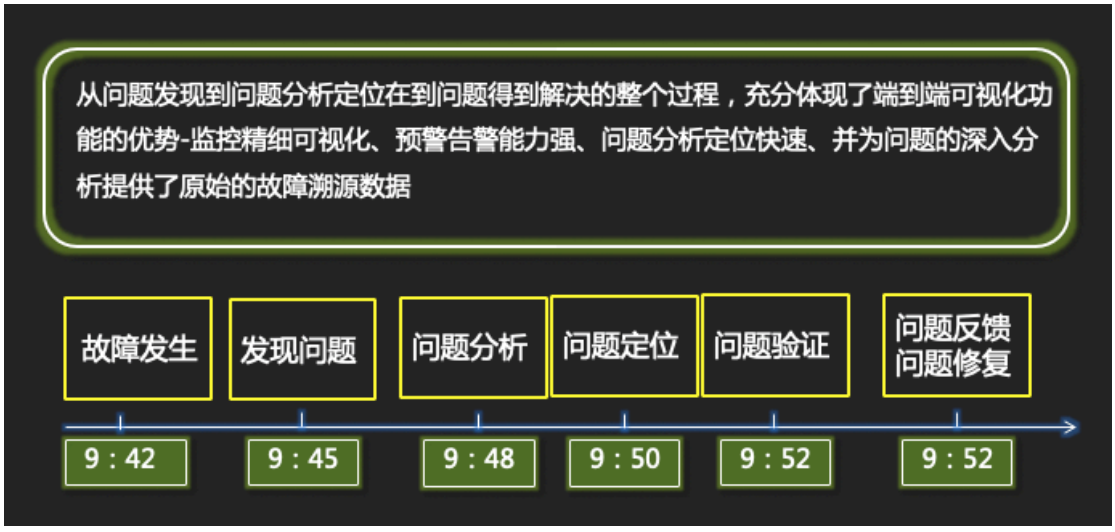
【性能可视化分析控件】

下图中清晰的展现应用性能下降是红色部分时延上升导致，而红色对应的指标是图例中的应用响应时间。代表网络性能的网络连接时间、丢包重传时延则没有明显变化，客户端性能及服务器主机性能也未出现明显变化。所以本次故障是由应用自身导致的与网络无关。应用部门还需要针对该问题继续分析，应用哪里出现了问题，手机银行 Web F5 节点性能下降，那么是不是 F5 导致的呢？我们可以继续看下面的视图。



【应用端到端可视化控件】

上图是 nCompass 为手机银行业务系统提供的应用端到端可视化视图，图中从左到右的节点分别为： 手机银行 Web F5 -> 手机银行 Web 集群->手机银行 APP F5 -> 手机银行 APP 集群-> 手机银行数据库，全流程的呈现了应用的各个节点各维度的运行状态，其中视图的第一行是性能分析视图，呈现了不同时间段该系统各应用节点的实时性能状态。从上图可以看出，除了数据库性能平稳运行外，其他节点均在故障时间点出现了较大的波动。性能分析的原理是后端节点性能下降，必然导致前端节点性能下降，所以我们可以快速定位到本次故障是手机银行 APP 响应缓慢导致 Web 应用、F5 负载设备均受到了影响。最后通过对所有版本的手机银行 APP 服务器做分析，定位到 IOS、Android 版本均性能异常。在分析手机银行 APP 的后端时，发现最终是短信网关性能异常导致手机银行 APP 性能异常，修复短信网关后服务得到了修复。在整个分析过程中，避免了网络背锅、避免了 F5 厂商背锅同时也避免了手机银行团队背锅。基于数据分析快速定位到是短信网管系统，影响了手机银行系统。



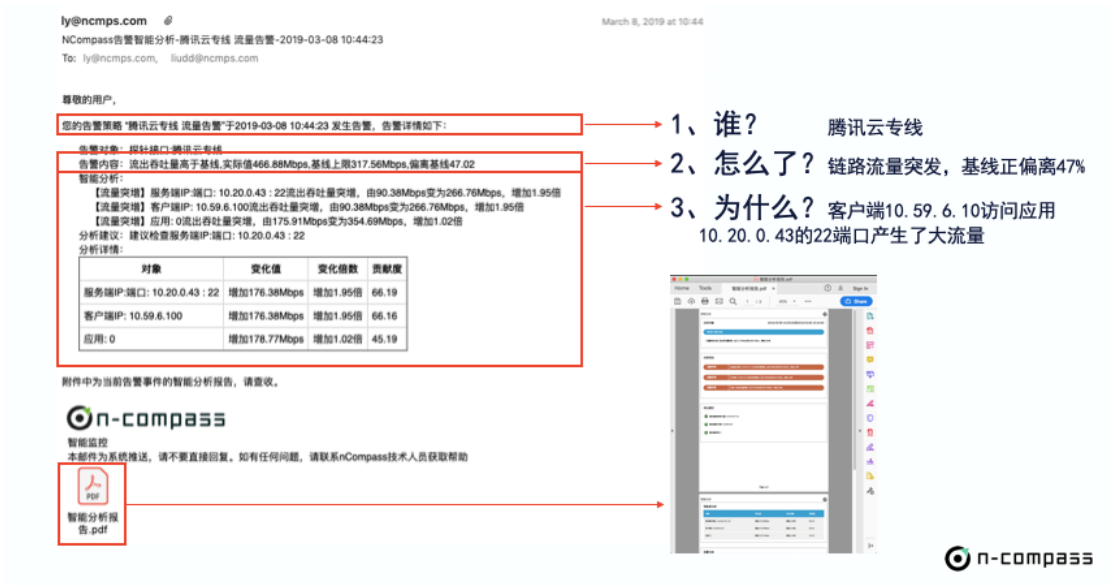
【故障分析步骤回溯】

3.4 突发故障的秒级定位

在复杂的网络及应用架构下，故障定位往往费时费力。很多故障从分析到定位的时间往往是以小时甚至部分疑难杂症问题的解决周期是以天、周为时间单位的。故障分析周期如此之长的主要原因有如下几点：

- 架构复杂，涉及部门众多。一个业务问题往往要涉及众多的网络及应用节点，分析人员需要登录多台设备获取数据整合后进行分析。
- 严重依赖 IT 人员的技术能力及经验。分析人员越专业排障的效率就越高，故障产生的影响就会越小。不过技术过硬且经验丰富的数据分析人员往往被各个领域的头部客户瓜分，想招到这种级别的人非常困难。
- 业务访问逻辑复杂。分析人员往往不熟悉业务，熟悉业务的过程则消耗的很多时间。
- 缺少数据支撑。不少故障是偶发性或间歇性的，进行分析时问题没有发生需要等下一次问题出现。

面对这种情况，nCompass 解决方案，借助系统内置 AI 算法库以及故障分析知识图谱，实现当出现告警后的故障智能分析及定位功能。实现了从故障感知、故障分析、故障定位、故障解决的全流程闭环。下面我们来看一条 nCompass 数据可视化分析平台发出的告警信息：



【智能告警及分析内容展示】

nCompass 的告警内容，不会如传统告警一样只通知用户某指标超过阀值，而是会借助系统内置的 AI 智能算法及故障分析知识图谱，自动对告警的异常事件进行分析，并在几秒钟内，将分析结论与告警通知一并发送给用户。

上图的示例中，nCompass 通过实时监控模块，发现数据中心和腾讯云的专线链路中出现突发流量。告警产生后系统立刻调用告警关联的智能分析脚本，对链路用量进行分析，快速发现突发流量是客户端 10.59.6.10 访问服务端 10.20.0.43 的 22 端口产生了大流量。因此运维人员在收到这条告警后，省去了登录设备、获取数据、人工分析的环节，直接可以看到导致链路突发流量的原因，极大的缩短了故障的平均修复时间（Mean time to repair，MTTR）。

上述案例是一个相对简单的分析场景，nCompass 数据可视化分析平台内置了数百种数据分析图谱，可对数据中心常见的网络连通性异常、应用可用性异常、应用性能异常、IP 行为异常等场景，实现秒级的故障诊断分析。

【系统内置的故障分析知识图谱】

数据智能分析需要高级算法的支持。比如一个指标出现变化，那么变化的幅度、速率达到多少算是异常？nCompass 的内置机器学习、异常检测算法、多维主因素分析、根因定位等算法，可以让系统具备一个数据分析专家的能力。所有的智能分析脚本均是通过 Python 语言编写，分析逻辑、数据消费、智能算法，均可在脚本中配合使用，脚本几乎可以取代一个专业的人员在 nCompass 平台中进行的所有数据分析。

```
def run(self):

    # 检测1:  判断是否网络丢包导致
    self.packetloss = self.helper.report.datasource()
    self.tcpconnecttime = self.helper.report.datasource()
    packetloss = self.helper.case.detect(self.target, self.target.model, '{丢包率}', '{突增}', time = [self.case.start_time, self.case.end_time])
    if packetloss:
        reason = Reason()
        reason.obj = self.target.obj
        reason.case = packetloss
        reason.category = '网络性能异常'
        reason.suggestion = '故障时间段，网络丢包率突增，可通过网络端到端可视化视图，定位丢包的节点'
        self.add_reason(reason)
        self.packetloss.add(self.target.obj, self.target.model, '{丢包率}')

    # 检测2:  判断是否网络时延导致
    tcpconnecttime = self.helper.case.detect(self.target, self.target.model, '{TCP建连时间}', '{突增}', time = [self.case.start_time, self.case.end_time])
    if tcpconnecttime:
        reason = Reason()
        reason.obj = self.target.obj
        reason.case = tcpconnecttime
        reason.category = '网络性能异常'
        reason.suggestion = '故障时间段，应用的网络连接时间变长，该问题主要由网络丢包或应用负载过高导致，请检查网络丢包率及应用系统的负载'
        self.add_reason(reason)
        self.tcpconnecttime.add(self.target.obj, self.target.model, '{TCP建连时间}')

    # 检测3:  判断是否网络连接数变多导致
    self.newconnect = self.helper.report.datasource()
    self.table_newconnect = self.helper.com.table()
    newconnect = self.helper.case.detect(self.target, self.target.model, '{新建会话数}', '{突增}', time = [self.case.start_time, self.case.end_time])
    if newconnect:
        self.table_newconnect.add_row(["对象", "变化值", "变化倍数", "贡献度"])
        pca_result = self.helper.algorithm.pca(self.target, newconnect, ["{客户端IP}", "{服务端IP:端口}"])

        for item in pca_result:
            reason = Reason()
            reason.obj = item.obj
            reason.case = item.case
            reason.category = '新建连接数突增'
            reason.suggestion = '故障时间段%s的新建连接数突增，请确认其行为是否为正常' % (reason.obj.format())
            self.add_reason(reason)
            self.newconnect.add(self.target.obj, self.target.model, '{新建会话数}')
            self.table_newconnect.add_row([item.obj.format(), item.case.format_delta(), item.case.format_delta_times(), item.score])

    # 检测4:  判断是否主机性能不足导致
    self.tcpwindowdelay = self.helper.report.datasource()
    self.table_tcpwindowdelay = self.helper.com.table()
    tcpwindowdelay = self.helper.case.detect(self.target, self.target.model, '{服务端小窗口时延}', '{突增}', time = [self.case.start_time, self.case.end_time])
    if tcpwindowdelay:
        self.table_tcpwindowdelay.add_row(["对象", "变化值", "变化倍数", "贡献度"])

        pca_result = self.helper.algorithm.pca(self.target, tcpwindowdelay, ["{服务端IP:端口}"])

        for item in pca_result:
            reason = Reason()
            reason.obj = item.obj
            reason.case = item.case
            reason.category = '服务端小窗口时延突增'
            reason.suggestion = '建议检查%s的系统资源' % (reason.obj.format())
            self.add_reason(reason)
            self.tcpwindowdelay.add(self.target.obj, self.target.model, '{服务端小窗口时延}')
            self.table_tcpwindowdelay.add_row([item.obj.format(), item.case.format_delta(), item.case.format_delta_times(), item.score])

    # 检测5:  判断是否应用所依赖的后端服务导致
    self.topo = self.helper.com.topo()
    self.responsetime = self.helper.report.datasource()
```

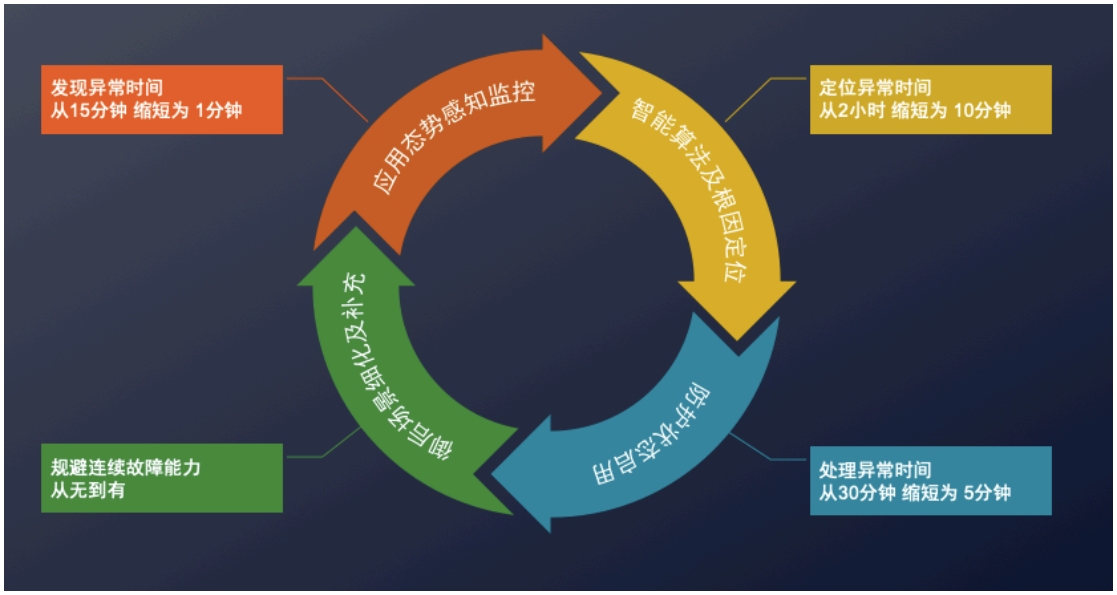
语法检测　确认　退出全屏

【智能分析脚本源码示例】

用户基于自己的网络及应用架构，通过可视化的图形界面，编辑自己的监控及智能分析脚本。为了提升脚本编辑的应用性，nCompass 提供了一套可视化配置形式的 Python 脚本编辑器。用户无需掌握 Python 语法，通过界面的选择、配置，即可完成智能脚本的编辑。

【支持用户自己创建知识图谱】

- 通过 nCompass 的智能故障分析模块，可以让用户的运维更智能：
- 通过 nCompass 平台的机器学习及异常检测算法实时感知应用运行态势，让故障发现时间从 15 分钟缩短为 1 分钟。
- 通过 nCompass 平台的多维主因素及根因定位算法，让故障定位时间从小时天缩短为分钟级。
- 通过 nCompass 的多平台联动能力，处理异常时间从 30 分钟缩短为 5 分钟。
- nCompass 平台帮助用户不断完善知识图谱，搭建智能化运营体系。



【nCompass 系统智能分析模块的核心价值展示】

3.5 自动化平台联动实现故障自愈

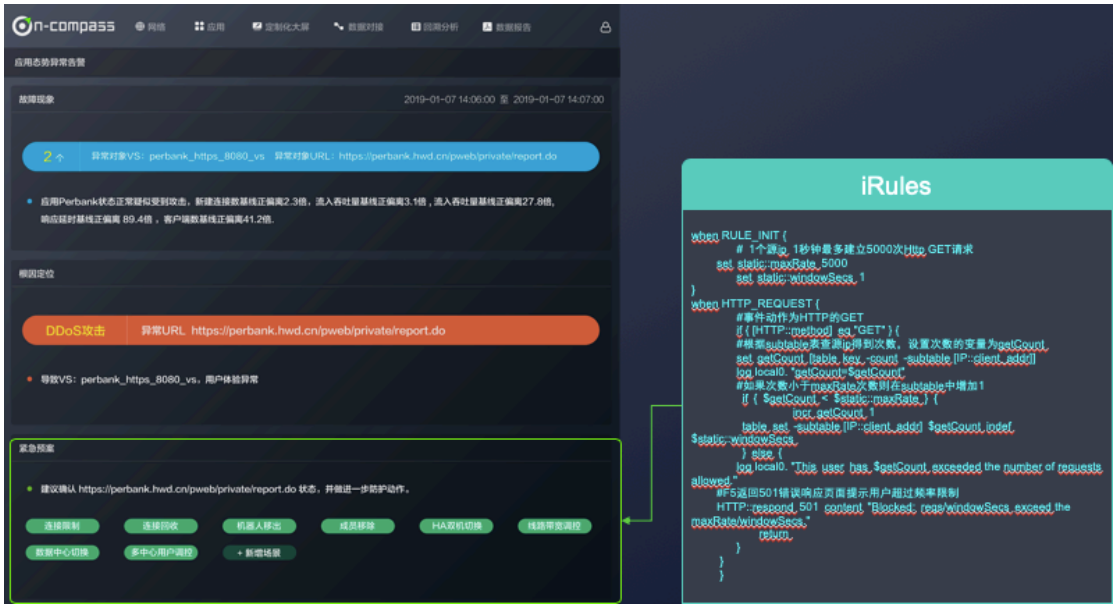
nCompass 数据可视化分析平台具备与自动化平台联动的能力，感知故障后可进行智能分析定位故障根因，并由 nCompass 下发配置命令，自动修复故障。

下图为 nCompass 与某股份制银行共同实现的广播风暴故障自愈案例。该银行网络采用大二层的架构，并且网络中有一批型号较为早期的网络设备，所以偶发性的会出现广播风暴，针对该问题 nCompass 提出的解决方案是：

- 在每个网络区域中接入 nCompass 采集节点，采集该区域的广播、单播、组播的数量;
- 提供秒级精度的监控;
- 当某类数据包数量远偏离基线时，发出告警;

- 基于告警信息内的 VLan ,查询资产系统 ,找到该区域的所有接入层网络设备清单;
- 调用自动化平台的脚本，遍历设备清单内所有设备的广播包变化情况，定位广播风暴源端口;
- 自动化平台直接关闭源端口;
- 整个过程从故障感知到故障修复，仅需 7 秒.

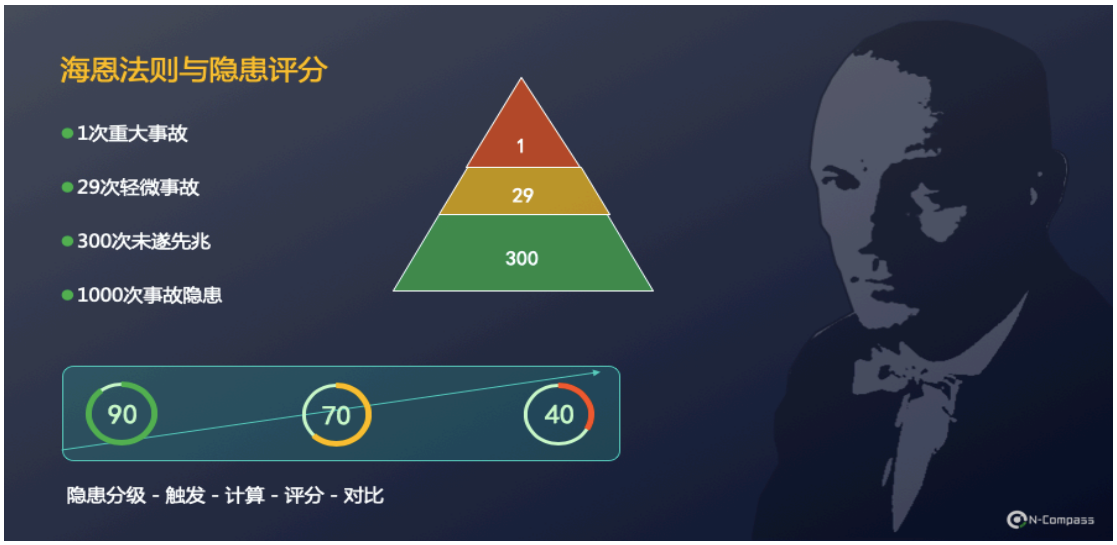
针对相对复杂的故障，通常用户不放心让自动化直接作出操作动作，nCompass 提供智能分析及基于分析结论的一键自愈功能。即在上述分析的自动化执行脚本下发命令的步骤，暂不执行。而是将该操作放到 nCompass 分析结论报告中，用户看完分析报告确认无误后，可点击脚本执行按钮，针对故障进行修复。



【一键故障自愈流程图】

3.6 隐患巡检分析

德国人帕布斯·海恩经过对飞行事故研究和统计后，提出了安全生产管理领域的重要法则——海恩法则。法则指出:每一起严重事故的背后，必然有29次轻微的事故、300起未遂的先兆以及1000起事故的隐患。法则强调两点：事故的发生是量积累的结果；它说明任何一起事故都是有起因的，有征兆的，而且绝大多数完全是可以避免的。



【海恩法则】

海恩法则同样适用于 IT 运营管理领域，隐患的问题是每个数据中心领导关注的问题，隐患越多则未来遇到的故障越多。如何快速找出隐患及时消除，需要建立一个隐患排查体系。通常用户通过人工巡检的方式，来定期检查设备硬件状态、设备日志，找到设备级的隐患。但是如何保证人工巡检的质量？同时应用级的隐患、安全隐患这类隐藏较深的隐患该如何查找？也是急需解决的问题。

用户可在 nCompass 数据可视化分析平台中，通过定期任务的方式，自动分析系统所采集的所有数据。主动找出其中的异常事件，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。实现主动发现，及时解决。

【隐患巡检结果展示界面】

针对系统巡检检测出的隐患数据，系统可提供数据回溯及智能分析，协助用户的网络、应用、安全人员，快速定性隐患问题，并通过数据对下一步动作进行数据支撑。

3.7 应用优化分析

应用的服务质量作为 IT 运营管理部门价值的一个重要体现 ,用户对系统满意度高，系统运行快速、安全、高可靠，是每一个 IT 运营人员的目标。

但是业务需求变化越来越快，不少应用会面临仓促上线的尴尬情景，应用运维人员需要掌握应用上线后的运行细节，如：哪些页面有错误？哪些页面访问量高且页面性能响应缓慢？应用中的大文件是否及时发布到 CDN 节点？

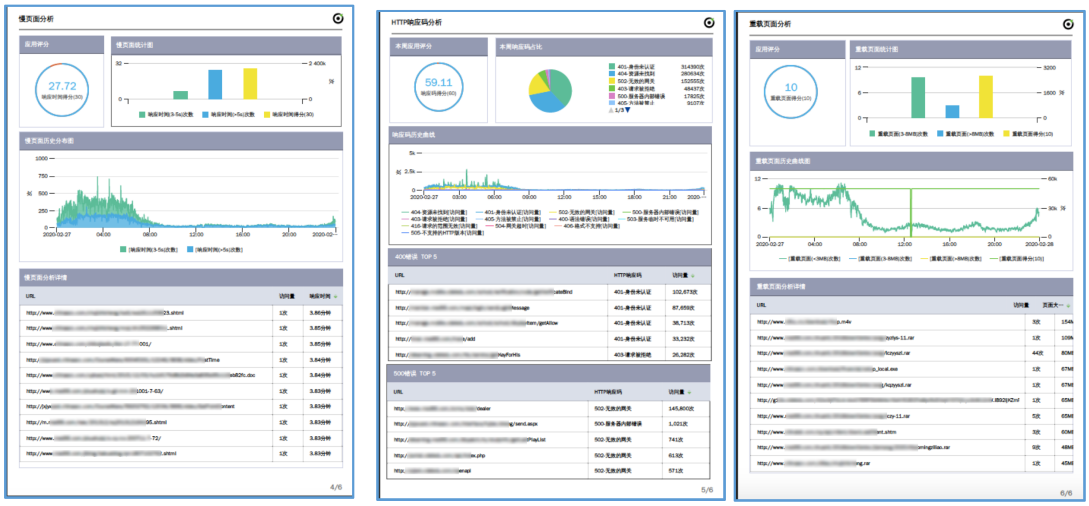
面对上述问题，nCompass 通过数据统计分析报表功能，可以帮助用户掌握应用的运行细节，帮助用户通过历史数据，持续的发现应用存在的隐患、为优化应用提供数据指引。

Web 应用优化统计报表：是 nCompass 系统内置报表中的一种，该报表默认设置为周报，每周统计数据中心内关键 Web 应用系统的服务质量评分以及找出应用运行过程中出现的问题。

下图为报告的应用运行分析概述，量化 Web 应用的服务质量并进行评分，报告呈服务质量未到达 100 分满分的原因，如存在应用报错、慢页面及重载页面（Heavy URL）。同时将本周应用评分与上周进行对比，能够看出应用服务质量的趋势，是不断提升还是不断下降。

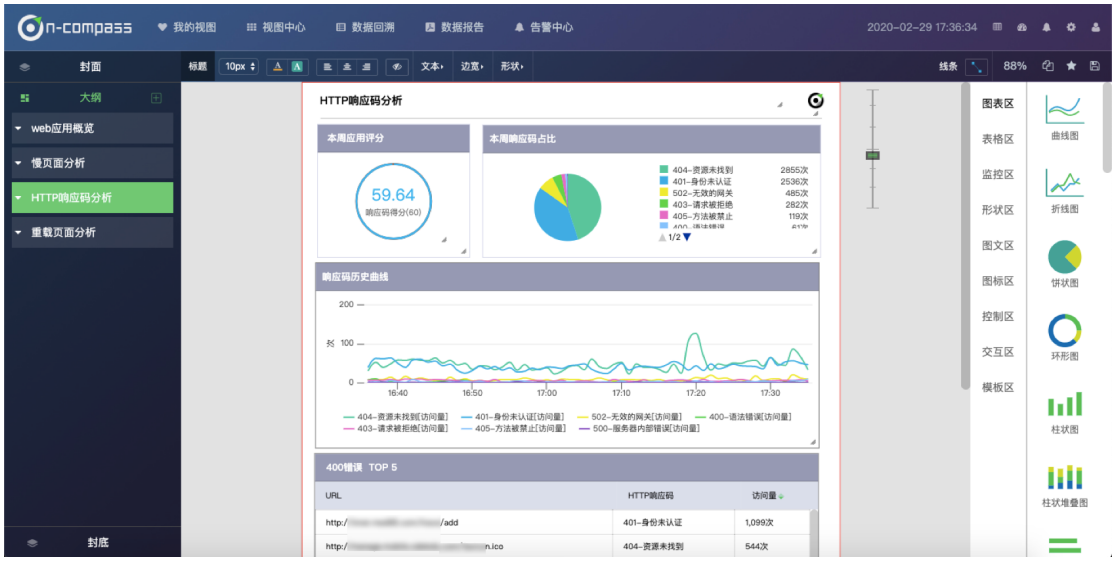
【Web 优化统计分析 概述】

下面三张图，分别针对应用错误、慢页面及重载页面，进行了异常信息的展示。通过查看优化统计报告，应用人员可直观的知道在应用运行过程中，哪些页面存在 400 或者 500 的错误，哪些应用的响应缓慢，哪些页面存在尺寸较大文件，需要尽快发布到 CDN 节点。



【Web 优化统计分析详情】

nCompass 的报表模块，与 Dashboard 类似。提供一套类“Word“模式的报表编辑控件，用户可以同定制视图一样，快速形成所需的数据统计报表。下边可呈现部分系统内置的统计报表，用户可以基于自己的实际环境及具体需求，通过报表可视化模块定制属于自己的数据分析报告。



【数据报表编辑界面】

用户可以在 nCompass 报告管理界面或者在邮箱中，查看、下载最新及历史报告。

【数据报表管理界面】

3.8 梳理复杂的应用访问依赖关系

- **适用部门： 网络运维、应用运维、安全运维**
- **适用场景： 应用关联梳理、业务变更、机房搬迁、安全溯源分析**
- **价值收益： 帮助网络及应用人员快速梳理应用间的服务依赖关系，提升复杂环境下的应用可视性，帮助安全部门快速追溯恶意行为的攻击链**

随着业务系统架构越来越复杂，一次用户的业务请求可能要经过网络节点、安全节点及应用节点甚至外联单位才能完成。所以当业务出现不可用、性能下降时，用户往往难以快速定位到故障域，是哪个节点异常导致的业务受到影响。这时一张清晰、准确且自动化生成的业务路径图，则非常关键。

nCompass 可以通过网络流量数据与资产数据、关键网络设备配置文件的结合，以网络流量或应用日志数据为基础，配置及资产数据为辅助，快速生成某用户或某应用的访问关系拓扑图。

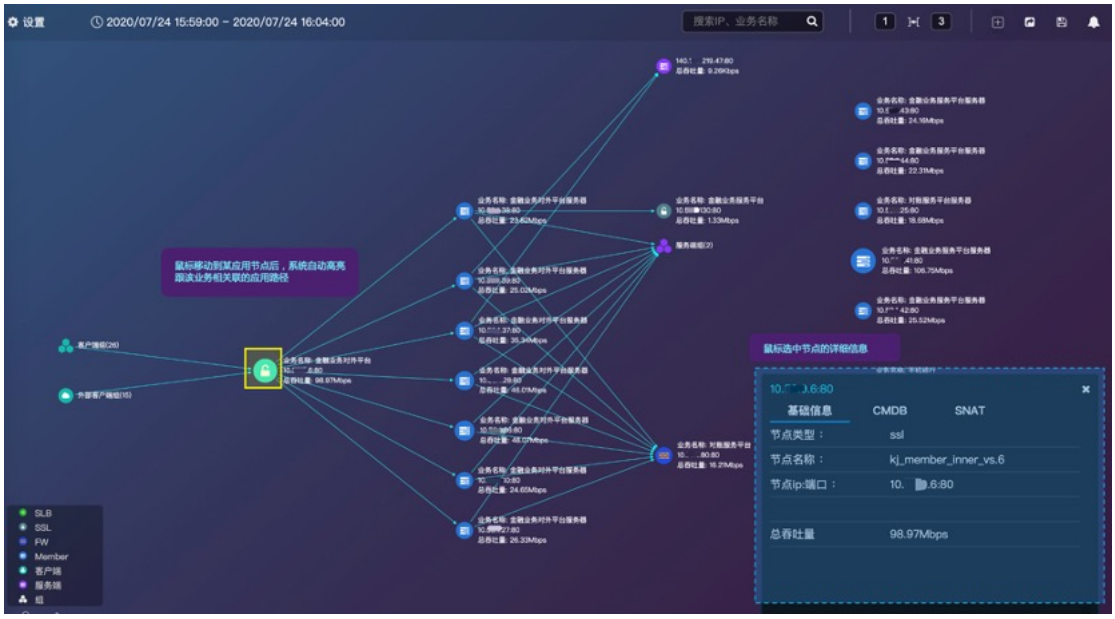
应用数理模块，可基于用户指定的检索条件，自动完成画像的生成，检索规则可灵活组合，同时提供了便捷的噪点过滤算法，快速消除画像中的噪点数据。

【画像生成配置说明】

通过自动梳理整理出一段时间内各设备互访情况，并且根据 CMDB 设备资产管理表来进行流量区域，数据中心的区分，标明业务的走向以及流经节点和应用架构，方便我们系统人员进行资产梳理，网络人员进行网络规划，让用户能够对自己内部资源有更高的掌控。

【业务画像效果呈现】

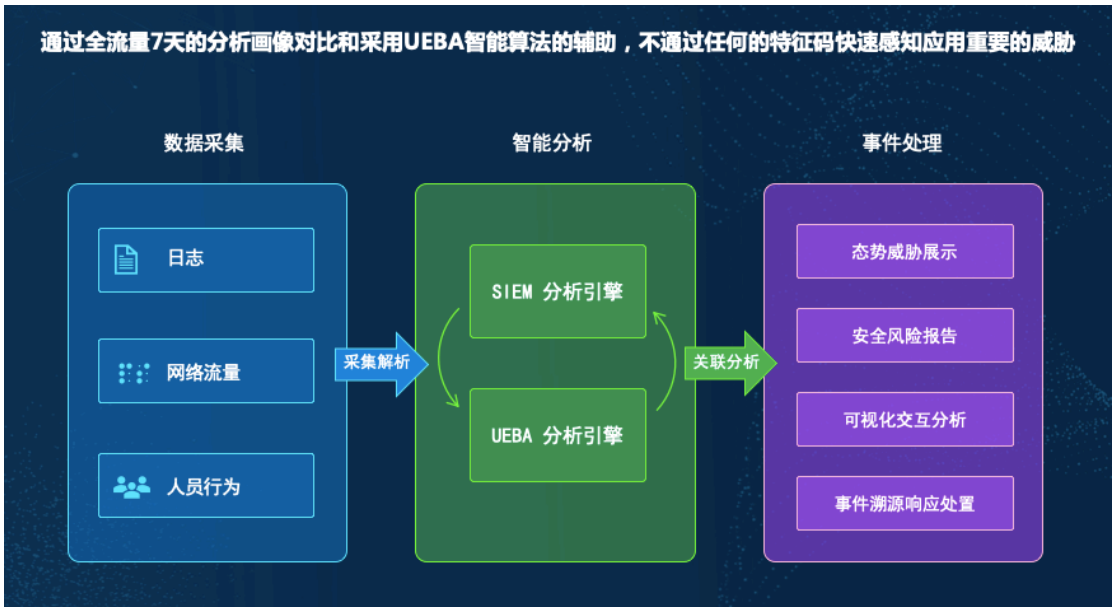
基于应用的访问无限层级的前后延展画像，最终完成整个业务路径的发现。



【业务画像效果呈现】

3.9 攻击溯源取证分析

目前用户的安全防护，主要依赖于基于“数据特征”的检测技术，如IDS、IPS、WAF等，当流量中出现明显的威胁特征时，安全设备可主动做出防护动作，保障数据中心的高可用及信息安全。但是这类安全检测设备存在一定的局限性，无法完全应对现有的安全形势。例如传统检测产品都是面向攻击的检测，对于已攻陷的攻击行为无法进行检测发现。另外设备的安全特征库更新周期较长，无法满足当前快速发展的高级攻击行为。传统检测产品仅仅保留告警的流量数据，溯源需要更多的流量上下文，导致溯源分析很难开展。

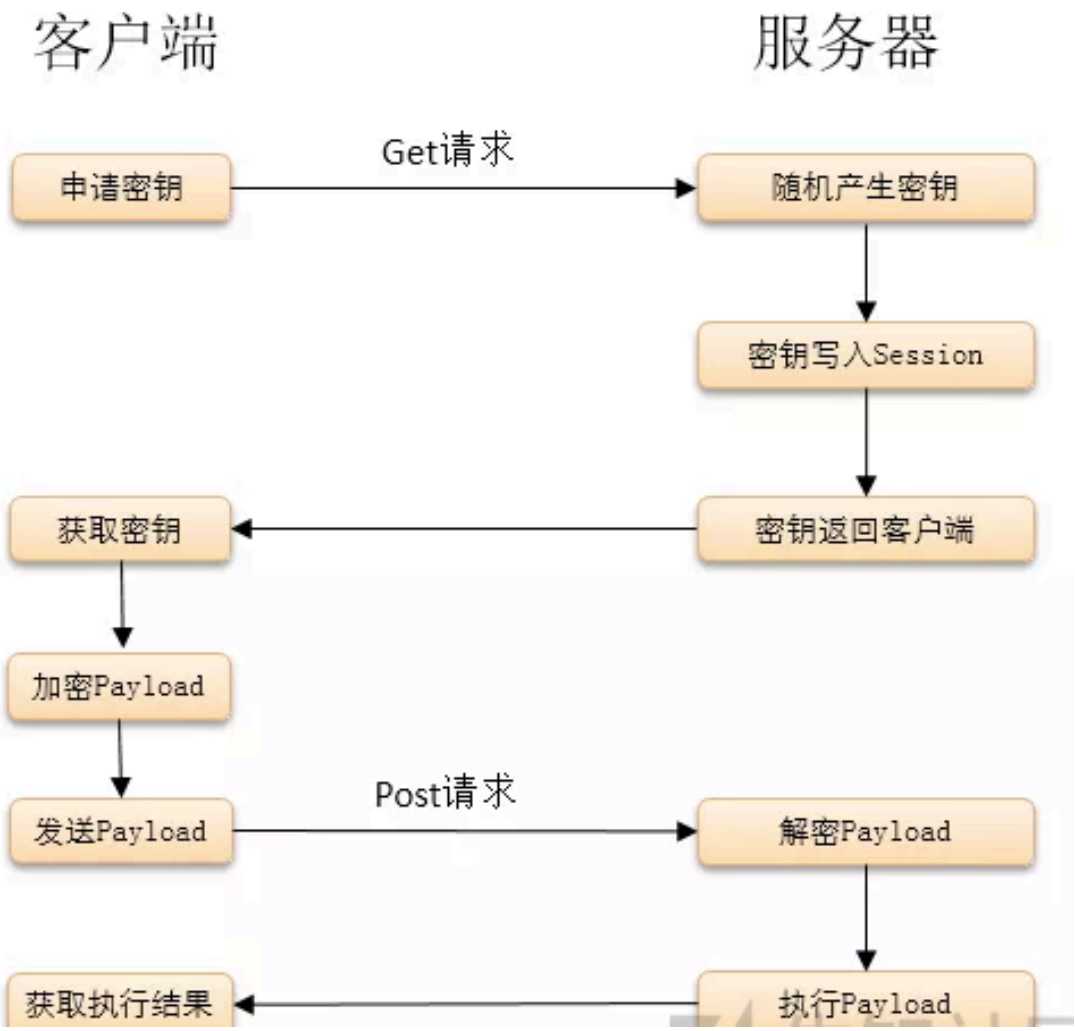


【基于全流量的安全威胁检测模型】

再高级的攻击，都会留下痕迹。nCompass 平台基于实时采集的全网流量数据，及时帮助安全分析人员通过灵活的检索规则，实现数据的快速回溯，对异常事件定性作出相应的安全处理动作，帮助企业止损。

nCompass 安全检测机制并不完全依赖于数据内容特征，而是基于用户或主机的行为特征，结合机器学习、行为关联分析等算法。帮助用户具备弱特征防护能力，密目现有监控体系的不足。

例如最近比较难以防护的恶意木马程序“冰蝎”，其攻击行为通过动态二进制加密的方式完成。传统的安全设备完全无法检测这类流量，给传统安全防护带来了极大的挑战。



【冰蝎攻击行为】

从过程上来看，大概分为下述几个步骤：

- 首先客户端以 Get 形式发起带密码的握手请求，服务端产生随机密钥并写入 Session。
- 客户端将源代码，如 assert|eval("phpinfo();”)利用 AES 加密，发送至服务端，服务端收到之后先进行 AES 解密，得到中间结果字符串 assert|eval("phpinfo();")
- 服务端利用 explode 函数将拆分为一个字符串数据，索引为 0 的元素为字符串 assert，索引为 1 的元素为字符串 eval("phpinfo();")。
- 以可变函数方式调用索引为 0 的数组元素，参数为索引为 1 的数组元素，即为 assert("eval("phpinfo;")") 。

nCompass 则可基于冰蝎木马的行为特征，设定检测规则，快速检测出冰蝎木马攻击。冰蝎密码的行为特征如下：

- Shell 的访问频率明显低于正常的业务页面，所以该 Shell 的访问频率很低；
- 冰蝎木马的加密秘钥为 16 位，所以当用户发起加密请求访问 shell 时，服务端会返回一个 16 字节长度的秘钥；
- 同时 shell 的路径是以 asp、php、jspx 为后缀。

可以实时分析全网流量中每日新增加的低频访问 URL，并且 URL 后缀为 asp、php、jspx，HTTP 请求类型为 GET，并且服务端返回内容长度为 16 字节行为，当出现这类行为，nCompass 可以主动发出告警，安全人员可通过 nCompass 回溯数据，对事件进行定性分析。

nCompass 系统内置的行为监测引擎及全网流量回溯能力，帮助用户具备了弱特征的防护能力及在安全事件定性过程中，提供数据回溯能力，帮助用户更精准、更高效的分析安全事件。

nCompass 的底层数据中，有丰富的数据索引，可以通过灵活的数据检索规则，快速从 TB 甚至 PB 级的存储中，找出所需的数据。

【nCompass 数据检索规则展示】

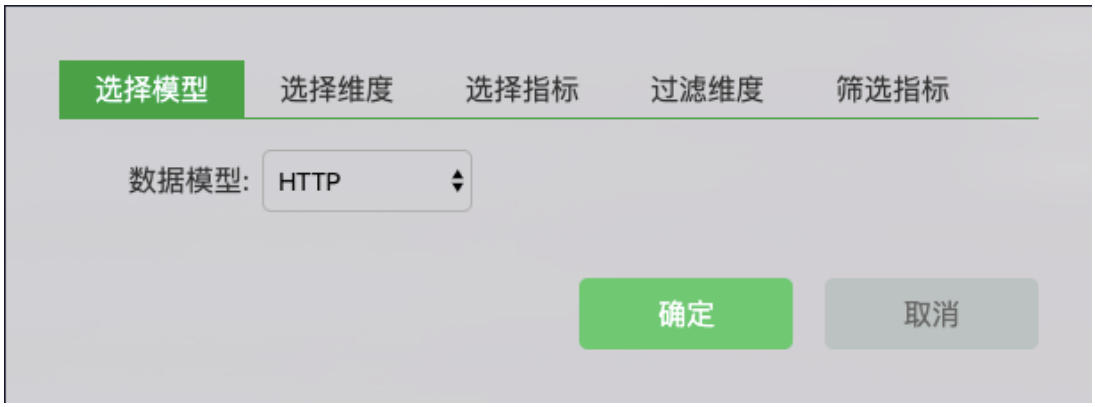
例如我们想搜索在今天上午出现 HTTP 500 错误最高的 URL，那么仅需通过下述几个步骤即可实现：

第一步： 指定数据检索时间，如上午 9：00-10：00

【配置数据检索时间周期】

第二步：设置数据检索条件：

- 选择检索的数据模型： HTTP



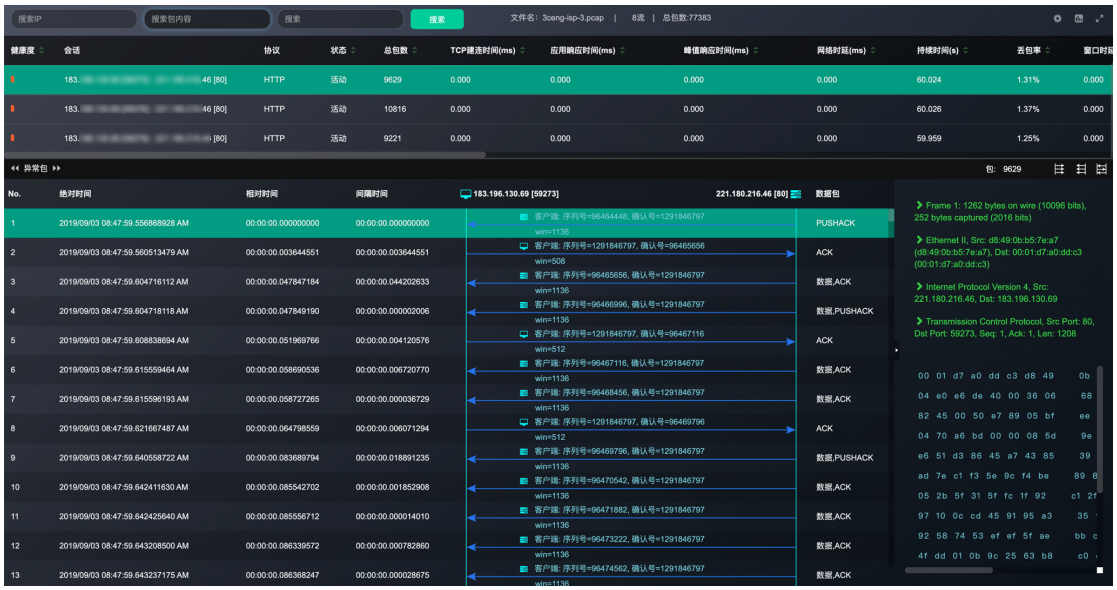
- 选择检索的维度： URL

- 设定过滤条件： http 500 响应码次数 > 0

第三步：设置查看返回的结果数据，nCompass 将会以表格的形式，将所有在上午 09：00-10：00 出现的 HTTP 500 的 URL 页面列出来，如下图

【数据回溯结果呈现】

nCompass 还提供了一套在线网络数据包分析工具 ,用户不仅可以针对统计数据进行数据分析，也可以对原始网络数据包进行解码分析。用户可在该界面中，基于数据包 payload 中的关键词 ,快速找到所需分析的网络会话 ,如基于交易流水号、交易订单号、手机号、用户名等。



【在线网络数据包解码分析界面】

3.10 防火墙策略优化分析

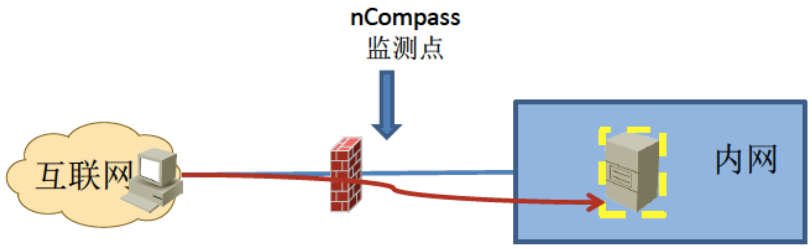
防火墙是通过安全策略来进行安全防护的，所以防火墙的安全策略配置和管理是企业信息安全工作的主要组成部分。目前大多数企业的防火墙策略已经实现安全策略申请-->审批-->配置下发-->策略验证的自动化配置流程。但基本上都缺乏安全策略的退出机制，比如定期的策略风险核查、策略生命周期管理、持续的策略收敛优化等。

由于系统管理人员变更、新增策略记录不完整、防火墙新旧更替等原因，许多防火墙策略建立的原因、用途变得不可追溯。

nCompass对经过防火墙的逐条数据流进行审计，实现从1000亿级别数据流中找出存在安全风险的防火墙安全策略，结合CMDB的IP身份核查，通过周报或者日报的方式提交给用户。用户通过报告可以及时发现存在的安全风险的策略，从而及时对策略进行优化 。

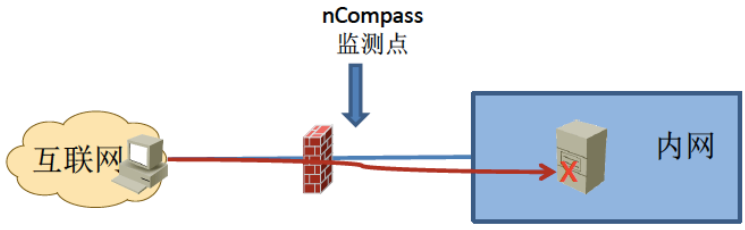
nCompass能发现以下类型的风险策略

1. 策略开通，但内部主机已下线



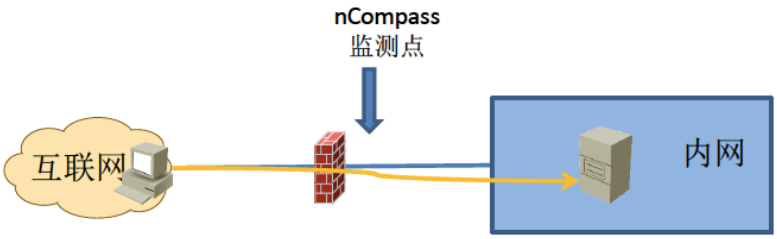
说明：互联网客户端尝试访问内网一台已经下线的服务器，防火墙策略允许通过。
原因：业务已下线，策略未删除

2. 策略开通，但内部主机一不提供相关服务



说明：互联网客户端尝试访问内网一台服务器，防火墙策略允许通过，但该服务器未提供相关服务，拒绝建立连接
原因：服务已下线或防火墙策略过于宽松

3. 策略开通，内部主机也提供相关服务，但客户端与服务器之间没有有效数据交互



说明：互联网客户端成功访问内网一台服务器，防火墙策略允许通过，但整个通讯过程没有传输任何有效数据
原因：服务器误配置配置，防火墙策略过于宽松

防火墙策略开通，但服务器已经下线：

1. 防火墙策略开通，服务器已下线　14　-- 高风险 --

用户的数据包（SYN）已经过了防火墙，说明防火墙策略允许通过

主机没有回复响应包（SYNACK），说明服务器已经下线

建议：联系此策略的创建者，确认知否删除此项策略。

风险策略列表　防火墙 Check Point Software Technologies　防火墙接口MAC 00:1C:7F:81:02:0B

服务端IP	服务端口	SYN包数量	SYNACK包数量	流入包数	流出包数	建连服务端重置
10 55	10080	2,327个	0个	2,327个	0个	0个
10 2	8899	392个	0个	392个	0个	0个
10 0	389	2个	0个	0个	2个	0个
10 9	8088	2个	0个	2个	0个	0个
10 1	443	2个	0个	2个	0个	0个
10 6	443	2个	0个	2个	0个	0个
10 1	389	2个	0个	0个	2个	0个
10 9	9001	1个	0个	1个	0个	0个
1 9	9009	1个	0个	1个	0个	0个
10 4	8088	1个	0个	1个	0个	0个
10 8	8081	1个	0个	1个	0个	0个
10 1	8081	1个	0个	1个	0个	0个
10 7	8081	1个	0个	1个	0个	0个

防火墙策略开通，服务器在线线，但是应用已经下线：

2. 防火墙策略开通，服务器在线，服务已下线 73 -- 高风险 --

用户的数据包（SYN）已经过了防火墙，说明防火墙策略允许通过

服务器拒绝建连连接（RESET），说明服务器在线，但服务已经下线

建议：联系此策略的创建者，确认知否删除此项策略。

风险策略列表 防火墙 Check Point Software Technologies 防火墙接口MAC 00:1C:7F:81:02:0B

服务端IP	服务端口	SYN包数量	SYNACK包数量	流入包数	流出包数	建连服务端重置
10	7300	3,600个	0个	3,600个	3,599个	3,599个
1	7100	1,365个	0个	1,365个	1,365个	1,365个
1	1433	12个	0个	12个	12个	12个
1	1433	11个	0个	11个	11个	11个
1	33989	2个	0个	2个	2个	2个
1	8118	2个	0个	2个	2个	2个
1	5432	2个	0个	2个	2个	2个
1	8088	2个	0个	2个	2个	2个
1	9000	1个	0个	1个	1个	1个
1	9000	1个	0个	1个	1个	1个
1	8008	1个	0个	2个	1个	1个
10	18118	1个	0个	1个	1个	1个
10	15200	1个	0个	1个	1个	1个
1	8083	1个	0个	2个	1个	1个

防火墙策略开通，服务器在线线，应用也在线，但是无有效交互数据：

防火墙策略收敛工作，是一项长期持续的工作。nCompass 可通过定期的巡检方式，检测防火墙策略，并定期输出分析结果。

3.11 网络链路精细化管理

如今很多企业拥有众多职场，每个职场均有链路接入数据中心，供业务人员访问相应的业务系统。而这几百上千条链路如何进行有效的管理，成为许多网络运维人员面临的问题：

- 如何全面的监控运营商的服务质量？
- 业务异常是否是由运营商链路导致？
- 众多运营商链路，哪些需要扩容？哪些需要缩容？如何确保合理投资？

针对上述 3 个问题，nCompass 解决方案则利用数据统计分析，帮助用户解决问题。

功能亮点 1. 主动+被动式的链路质量监控，链路异常时快速判断是运营商问题还是数据中心内部问题

nCompass 解决方案提供“主动+被动式”的链路质量实时监控能力。被动式式监控及基于镜像链路的网络流量或 Netflow 的方式实现，主动式的监控则可通过 nCompass 主动发起拨测，来监控链路质量。两种方式相辅相成，且互相补充，可以全面的监控链路的运行状态，当链路出现拥塞、高延迟、高丢包等问题时，可第一时间发出告警通知。

基于镜像流量的方式，需要镜像互联网出口、广域网出口或外联出口的交换机流量，nCompass 通过实时解析网络流量数据，统计出各链路的实时监控指标数据。

网络用量实时监控：

- 链路利用率： 用于监控链路的流入/l 就出用量，当链路用量过高时，可主动发出告警 ,并智能定位高带宽占用的应用、用户及 IP 通讯对及相关信息。指标精度可达秒级，可视化瞬时的突发流量。
- 丢包率/运营商丢包率/数据中心丢包率：基于 nCompass 独有的丢包节点判断算法，不仅可以实时监控链路的丢包率，还可快速判断丢包是发生在数据中心外部，还是数据中心内部,帮助链路管理人员快速定位故障域。
- 网络时延/运营商网络时延/数据中心网络时延 :基于网络时延切片分析算法，不仅可以实时监控链路的网络时延（RTT），还可快速判断时延是发生在运营商侧还是数据中心内部。

【某政府机构国际网链路监控大屏】

【某证券公司互联网链路监控大屏】

nCompass 同时还支持主动拨测的方式 对所有专线链路进行探测 基于 Ping Loss、Ping 时延等关键指标，进行实时监控告警。

【nCompass 主动拨测监控界面】

主动拨测技术是一个相对轻量级的部署方案，其主要的优势是低成本，且即使在夜间无业务访问的时间段，也能持续测试链路的通断、质量状态。主要用于分支链路的可用性、性能的主动式探测，当某分支机构链路无法 ping 通或者存在较高的 ping

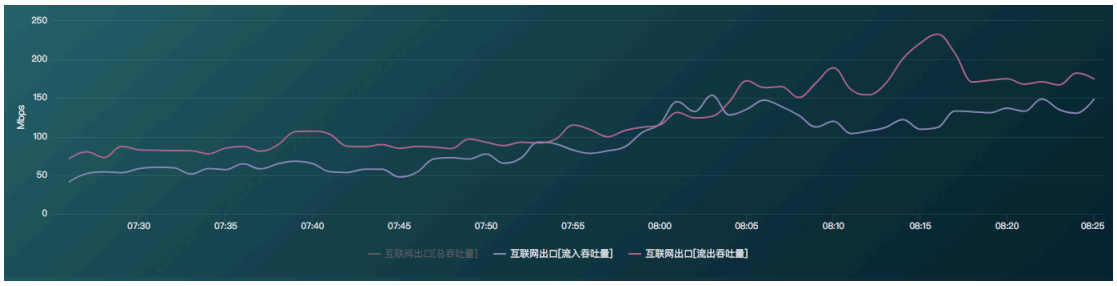
丢包时，nCompass 平台可主动发出告警。

精细化的监控部署后，则需考虑当异常事件出现后，如何快速的定位问题。下面则通过几个真实的案例，来展现 nCompass 的链路分析能力。

某互联网教育行业的 IT 管理人员，总是受到老师和学员的投诉，说经常出现卡顿甚至无端掉出课堂的现象，且毫无规律性，应用部门经过仔细的排查后，并未发现任何异常，则判断是网络问题。网络人员排查了网络设备日志、网管平台上的链路用量及质量数据，也未发现任何异常，设备没有告警、错误日志，网管平台显示，链路用量也不高、丢包、延时都处于正常区间，分析不出任何异常。

之后用户找了 nCompass，并在互联网出口部署了分析设备，仅用了 1 个小时定位就定位故障。

首先我们对互联网带宽用量进行分析，需掌握带宽的真实用量情况：



【网络链路用量 – 1 分钟精度趋势图】

通过一分钟精度的网络用量分析来看，客户的带宽出口是 600Mbps，业务高峰期的流量也才达到 240Mbps，并未出现带宽资源不够的现象。

之后，我们将指标颗粒度切换为秒级，则看出了一些异常：

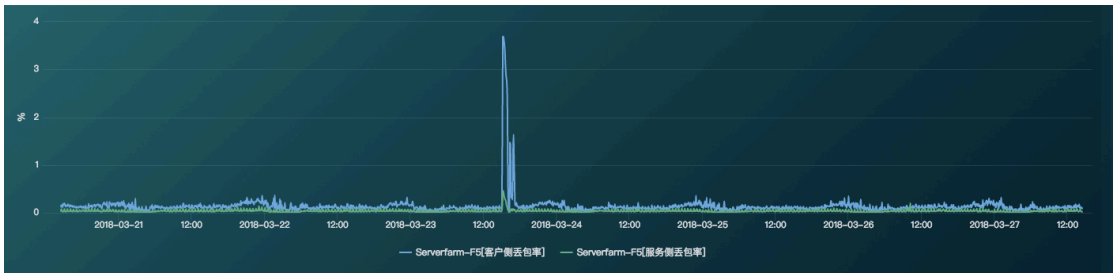
【网络链路用量 – 1 秒钟精度趋势图】

我们发现每 5 分钟的前 10-15 秒，链路中均有秒级的突发流量，并且流量达到的带宽的峰值，如果带宽跑满，那么肯定会对业务产生影响。用户看到这个图之后说，“我们一直怀疑链路中有突发流量，但是我们的网管平台看不到，你能不能帮我看看突发流量是什么业务系统、什么 IP 地址？” 我们则通过用量详情表格，快速的发现原来是用户的大数据平台，通过互联网出口链路跨数据中心采集数据：

网络部门对大数据平台的 IP 进行流量限速后，并主动与一些老师，确认再也没有出现卡顿或者掉线的问题了。

除了对秒级突发流量分析能力外，对运营商链路的质量也可以提供精细分析能力。

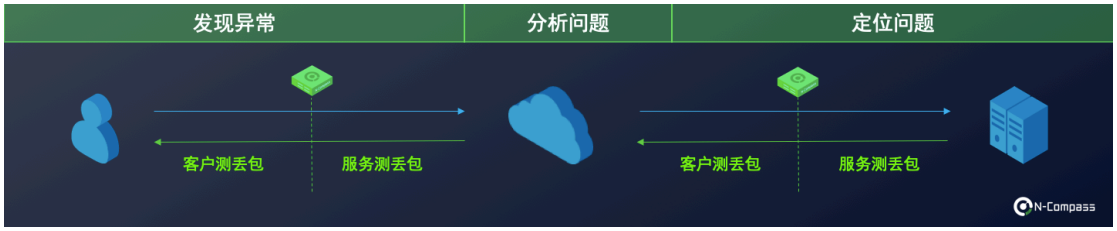
某城商银行近期出现了较高频次的链路丢包现象，联系运营商后，运营商并未发现问题，并将问题返还给了用户，希望用户能检查自己数据中心内部的网络质量。



【链路丢包率出现突发】

通过上图可以看出，该链路出现了突发的丢包，高丢包率对用户的互联网业务产生了一定的影响，用户希望判断丢包的原因及丢包节点。nCompass 独有的丢包几点判断算法，则可帮助用户快速定位丢包节点。

在互联网出口部署镜像并进行分析后，在上图中，我们发现丢包突发曲线，主要是浅蓝色曲线有突发，深蓝色曲线则平稳无波动，在图例中可以看到，浅蓝色曲线代表用户侧丢包，及用户端到数据中心的监控点这段网络路径中发生的丢包，服务侧丢包率角度，且并未出现明显的丢包波动，所以该问题明显是用户端网络质量异常或运营商链路抖动造成。



【nCompass 丢包节点判断算法】

关于丢包节点的算法，可咨询 nCompass 售前工程师了解详情。

功能亮点 2. 基于带宽用量指标的数值区间分布，快速判断哪些链路需要扩容，以及哪些链路的带宽资源严重浪费。

在保险等一些金融行业，企业拥有众多职场链路，链路的数量可能会达到几百条甚至数千条，链路容量合理规划，如何合理做网络链路预算，哪些需要扩容，哪需要降低带宽节省投入，则是不少这类客户的需求。

nCompass 提供业内独有的区间指标，可以统一每条链路的利用率区间分布，如过去一个月中分别统计出：链路利用率<50%的时间占比，链路利用率在 50%-75%的时间占比，链路利用率在<75%的时间占比。通过链路利用率的历史使用率数据，来为链路容量规划提供数据支撑，从而可以更为合理的做出容量规划及预算。

- 高负载链路描述：即带宽占用较高且持续时间较长的链路。计算方式： [TIME (流入/流出利用率 = 100%) / TIME （数据采样 ） * 100%] > 50%
- 低负载链路描述：低负载链路即带宽占用较少且持续时间较长的链路。计算方式：[TIME (流入/流出利用率 <=50%) / TIME （数据采样 ） * 100%] > 50%

用户可通过 nCompass 统计报表 轻松得到基于成百上千条链路的容量规划数据：

【某保险用户职场链路容量规划报表 概览页】

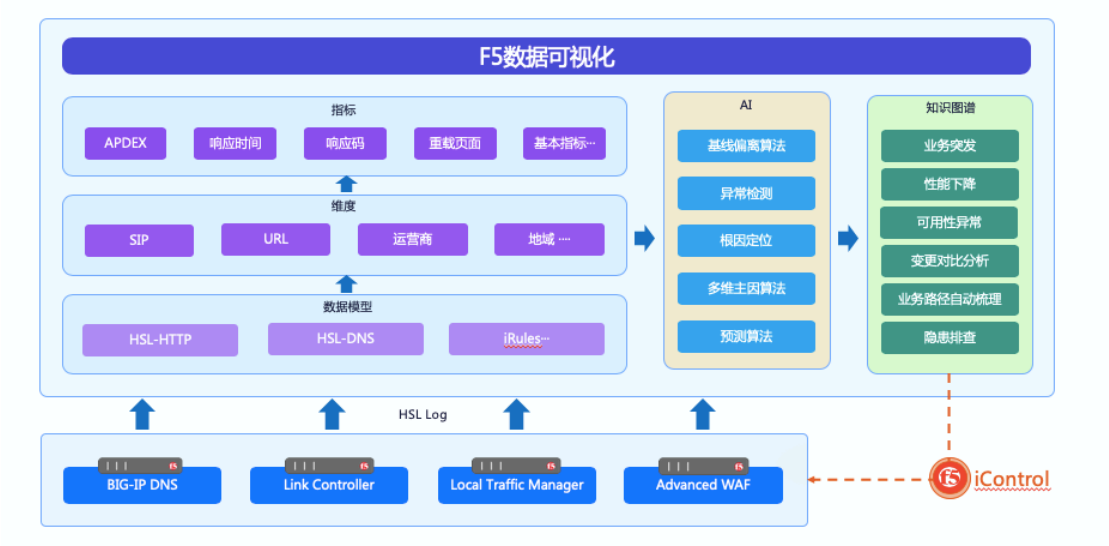
3.12 F5 设备的日志可视化

nCompass 数据可视化平台作为 F5 中国区的数据可视化合作伙伴，经过充分的研究用户对 F5 的使用场景以及 F5 的 API 接口的数据类型 ,与 F5 的 GTM、LTM、AWAF 等产品进行了充分的数据对接及场景化分析。

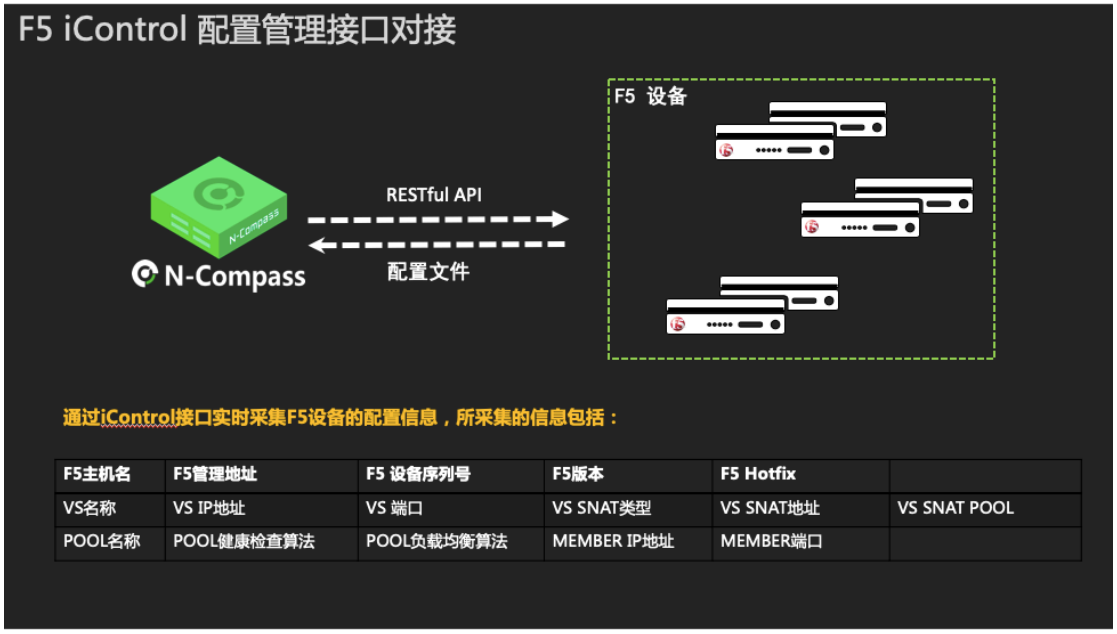
【F5 中国区数据可视化证书】

nCompass 的可以实时采集、对接 F5 设备的 iControl 及 HSL 高速日志，所支持的 F5 产品线包括：

- GTM（Global Traffic Management）
- LTM（Local Traffic Management）
- AWAF（Advanced Web Application Firewal）
- Nginx

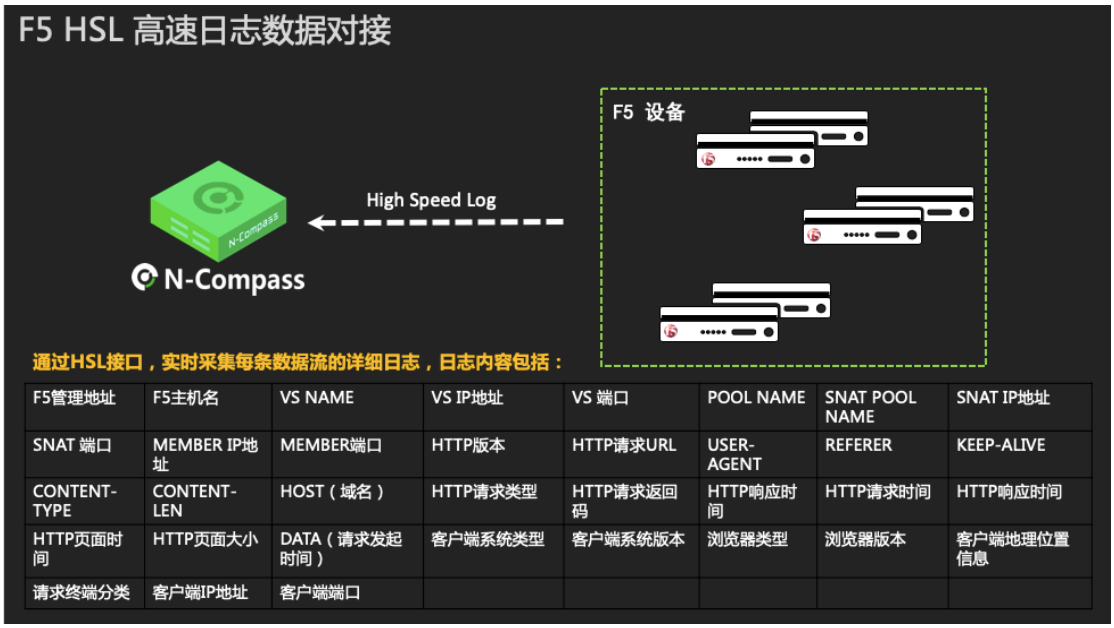


nCompass 与 F5 的数据对接主要是两种方式，通过 iControl 配置管理接口获取每台 F5 设备的配置信息，如 VS 配置、Pool 配置、负载均衡策略配置、设备信息、版本信息等。



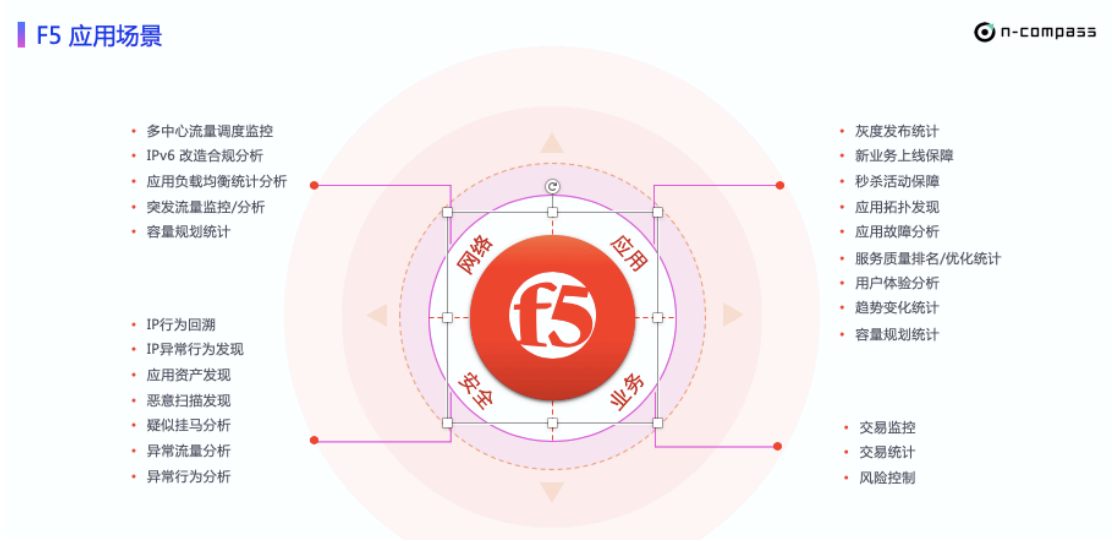
【F5 iControl 配置管理接口对接】

nCompass 还支持实时采集分析 F5 的 HSL(High Speed Logging)高速日志，F5 作为应用交付的关键节点，其承载的网络会话日志蕴含丰富的数据分析价值。



【F5 iControl 配置管理接口对接】

通过对 F5 数据与其他 nCompass 数据的整合，我们可以帮助用户在许多场景下解决其面临的困难。



【已支持的 F5 数据可视化使用场景】

3.13 SDN 环境下的网络路径可视化追踪分析

众所周知，云计算及虚拟化技术为用户的业务弹性扩展带来了极大的便利，但是业务上云后，其数据可视化的能力往往受到了较大的影响。用户在 SDN 下进行网络故障排查时，受限于 Overlay、Underlay 地址无法关联，而难以快速定位问题的困扰。

nCompass 平台可支持 SDN 环境中的基于指定两台虚拟机的网络通讯路径自动发现功能。实现 Overlay 地址与 Underlay 地址以及设备 ID 的串联分析，为 SDN 环境下的故障排查，提供可视化功能。

【SDN 环境中的网络通讯路径可视化】

3.14 每个用户都是场景设计师

在 nCompass 数据可视化分析平台中，每个用户都是场景设计师。用户由于其行业不同、部门不同、分工部门所处的 IT 架构环境也不同。所以每个用户都会存在自己个性化的数据分析、数据可视化需求。nCompass 平台则为用户提供一套灵活的场景定制功能，让每个用户都能基于 nCompass 平台的数据采集能力、分析能力及数据可视化能力，设计出可以解决自己问题的数据消费场景。

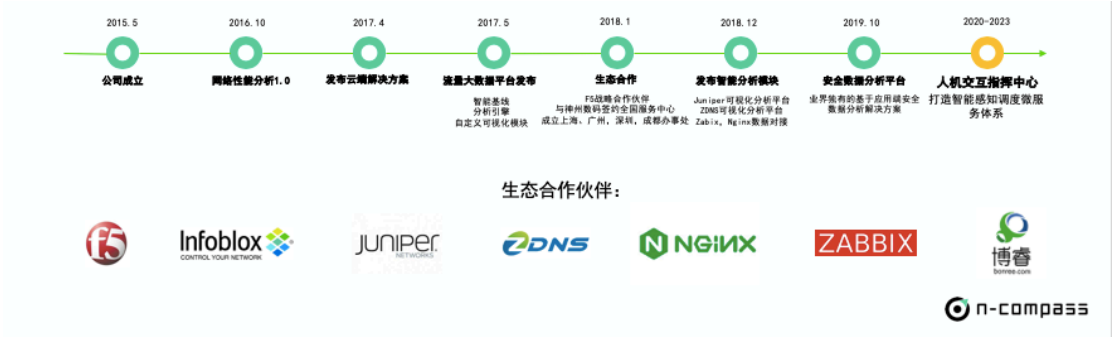
第四章 方案收益

nCompass 的愿景，是希望能通过多源数据的采集、对接，实现运维管理数据的整合。依托于内置的智能算法、专家知识库以及多平台联动能力，成为用户的业务保障指挥平台，帮助用户实现从设备级运维，到基于用户体验、基于业务交易的场景化运维。

nCompass 平台可以在整个运维体系中，无论是在网络运维、安全运维、应用运维还是业务运维部门中，发挥其数据整合、智能分析的能力，为各个部门的运营工作，提供数据支撑，实现数字化运营转变。

第五章 公司介绍

公司成立于 2015 年，是目前业内唯一一家专注于通过流量大数据+智能算法解决网络应用故障及安全的公司（Traffic Data Analysis）。公司独创的智能流量大数据分析平台，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。 nCompass 产品线，除了拥有传统的抓包分析，数据回溯，定位故障和报警的基本功能之外，其独有的智能基线与智能分析规则引擎结合可自定义的 Dashboad 可以帮助用户清晰的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，极大的提升了用户的运维效率和人工盲点，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，服务于运营商，金融、政企，互联网等多领域和行业中，得到客户的一致认可。



n-compass
www.ncmps.com
tel: 400-666-8216
北京市朝阳区八里庄西里99号住邦2000 2号楼807

我们的客户：

第六章 附录

6.1 支持的数据源清单

数据类型	数据源	采集方式	说明
网络流量	物理交换机	端口镜像，镜像端口与探针接口直连	用于采集数据中心南北向的流量数据； 数据用于全网流量的异常流量监控及溯源取证分析
	虚拟交换机	虚拟环镜端口镜像，通过 GRE 或 Vxlan 转发	用于采集数据中心东西向的流量； 数据用于私有云环境下的异常流量监控及溯源取证分析
	公有云 VM	基于 OS 数据采集探针，虚拟机的流量通过网络转发至管理端	用于采集公有云 VM 的流量数据； 数据用于公有云环境下的异常流量监控及溯源取证分析
Netflow	路由器/交换机	Netflow 数据指向 nCompass 管理地址	用于采集流量镜像覆盖不到的区域的数据，如分支机构的

			数据可以通过 Netflow 的方式采集
主动拨测	nCompass 管理机	可针对拨测的目的，进行主动探测，并记录探测结果	可弥补夜间无流量时的监控缺失，以及可拨测链路远端的主机，监控链路通断及延时状态
日志	VS HSL 日志	F5 的 HSL 日志可通过 Syslog 发送实时日志到 nCompass 管理地址，由 nCompass 进行数据统计分析呈现	F5 HSL 是一种低 TCO 的数据可视化方案，优点是目前客户关键业务均由 F5 进行应用交付，只需采集 HSL 日志即可看到所有的用户访问及 F5 与后端应用服务的交互日志。需确定是不是全量数据，数据完整性上有所缺失。
	Nginx	Nginx 具备丰富的日志统计能力。可通过 Syslog 发送实时日志到 nCompass 管理地址，由 nCompass 进	与 F5 HSL 日志一样，Nginx 日志同样也是一种低 TCO 的数据可视化方案，优缺点与 HSL 数据一致，但是 Nginx 可配置的日志类型相对丰富

		行数据统计分析呈现	
	HAProxy	HAProxy 具备丰富的日志统计能力。可通过 Syslog 发送实时日志到 nCompass 管理地址，由 nCompass 进行数据统计分析呈现	与 Nginx 类似，HAProxy 可将 4 层的用户访问、转发至 nCompass 平台 ,可用于实时监控及故障分析
	ZDNS	ZDNS 可通过 Syslog 发送实时 DNS 相关日志到 nCompass 管理地址，由 nCompass 进行数据统计分析呈现	数据可用于实时监控 DNS 的运行状态以及可以通过告警规则，发现异常 DNS 解析行为
	Imperva	Imperva 可以将告警事件以 syslog 日志的方式发给 nCompass 管理端地址，由 nCompass 进行数据统计分析呈现	可以将 Imperva 告警事件与原始网络流量结合分析，数据可提升安全分析人员定性告警事件的分析效率

	山石网康	山石防火墙可以将用户访问 VPN 的登陆记录以 syslog 日志对方式发给 nCompass 管理地址 ,由 nCompass 进行数据统计呈现 ,对用户访问记录进行可视化合规管理	用于采集山石防火墙的 VPN 日志访问日志。可通过 nCompass 系统统计分析用户访问 VPN 的行为数据
	Juniper	Juniper 可通过 syslog 发送实时 telemetry 数据到 nCompass 管理端地址	数据可呈现 Juniper 设备上的 qos 队列包数、带宽、buffer、接口丢包率、时延和抖动等信息，可通过 nCompass 平台集中化监控所有 Juniper 接口的实时状态
	Zabbix	Zabbix 可以将告警事件以 syslog 日志的方式发给 nCompass 管理地址 ,由 nCompass 进行数据统计分析呈	可以将 Zabbix 告警事件与原始网络流量结合分析，为运维人员提供更详细的数据，提升排障分析效率

		现	
API	iControl 配置管理 API	iControl 是 F5 的配置管理接口，可通过 F5 的 restful 接口，获取 F5 设备的配置信息以及针对 F5 下发策略配置命名	数据可用于获取 F5 的设备信息、配置信息以及当出现异常事件后的一键控制 F5 修改策略，如网络攻击后一键禁封、限速攻击源 IP 或目的 URL、主机等。
	博睿 SDK	博睿 SDK 可以通过 Kafka 组件将原始数据发送至 nCompass 管理端地址，包含终端的 App 崩溃率，卡顿率，请求类等数据，由 nCompass 将终端手机用户访问 App 的质量进行分析呈现，统一监控	用于采集博睿 SDK_kafka 数据。数据可实现用户 APP 手机端的数据数据与其他数据的无缝整合，更精细化的可视化业务交互过程中的每一步状态
	博睿 Server	nCompass 管理端通过主动获取博睿	用于采集博睿 Server_api 数据。数据可实现应用程序内部的代码执行数据与其他数

		Server 的 API，数据包含应用程序的代码耗时，精细至代码的类和方法耗时，并且可以和原始网络流量结合分析，提升分析问题根因的效率	据的无缝整合，更精细化的可视化业务交互过程中的每一步状态
	CMDB	可获取任意的 CMDB 库中的相关信息	用于对数据进行身份标识及关联，提升网络可视化的效率及数据管理成本
	微步威胁情报	可通过 API 主动查询微步的威胁情报数据并得到返回结果	数据用于情报数据的获取，通过情报数据提升告警准确率以及提升安全分析人员分析告警事件的效率

6.2 TCP/IP 数据模型的维度及指标介绍

统计维度：

维度分类	维度名称	用途说明
IP&端口统计	客户端 IP	统计流量中的客户端 IP 信息 ,可基于客户端 IP 进行数据检索、回溯、监控告警及报表统计
	客户端端口	统计流量中的客户端端口信息，可基于客户端端口进行数据检索、回溯、监控告警及报表统计
	服务端 IP	统计流量中的服务端 IP 信息 ,可基于服务端 IP 进行数据检索、回溯、监控告警及报表统计
	服务端端口	统计流量中的服务端端口信息，可基于服务端端口进行数据检索、回溯、监控告警及报表统计
	服务端 IP:端口	统计流量中的服务端 IP:端口信息，可基于服务端 IP:端口进行数据检索、回溯、监控告警及报表统计
	IP 通讯对	统计流量中的 IP 通讯对信息，可基于 IP 通讯对进行数据检索、回溯、监控告警及报表统计

	IP 版本	可自动识别网络流量的 IPv4 及 IPv6 流量，进行分别的统计分析
	X-Forword-For	可通过数据包头中的 X-Forword-For 地址，并针对 X-Forword-For 地址进行数据检索、回溯、监控告警及报表统计
采集点	采集探针	可基于某台探针所采集的所有数据进行聚合分析
	采集接口	可基于某台探针的指定接口所采集的所有数据进行聚合分析，如某个探针采集接口的是互联网出口的流量，那么可通过该接口体现互联网出口的整体运行状态，并可针对探针接口进行数据检索、回溯、监控告警及报表统计，采集接口维度也可用于故障分析，如多节点的数据比对，防火墙前后端的指标状态比对等场景
	Vlan	可统计分析网络数据包中的 Vlan 信息，并基于各个 Vlan ID 进行统计，呈现各个 Vlan 的数据，并可针对 Vlan ID 地址进行数据检索、回溯、监控告警及报表统计。Vlan 维度也可用于故障分析，如多节点的数据比对，防火墙前后端的指标状态

		比对等场景
	Vxlan	可统计分析 SDN 网络数据包中的 Vxlan 的 VNI ID 信息，并基于各个 Vxlan ID 进行统计，呈现各个 Vxlan 的数据，并可针对 Vxlan ID 地址进行数据检索、回溯、监控告警及报表统计
	租户/租户组	可多个 VxlanID 定义为组合，定义完成后，即可按照租户相关的流量进行聚类统计。以租户为视角，进行数据检索、回溯、监控告警及报表统计
	数据中心	可通过将指定的一台或多台数据采集探针定义为数据中心，完成定以后，即可按照整个数据中心相关的流量进行统计。以数据中心为视角，进行数据检索、回溯、监控告警及报表统计
应用	应用/应用组	可将多个 IP、端口定义为某应用，如服务端 IP 地址：192.168.1、服务端口：8080，定义完成后，即可按照指定应用定义信息进行统计。以应用为视角，进行数据检索、回溯、监控告警及报表统计。应用定义解决的数据身份可视化的问题及数据使用便捷性的问题，使用人员不用记住每个应用的 IP 及端口、域名等信息即可快捷的找到相应的数

		据
站点	站点/站点组	可指定的 IP 地址段或 IP 地址定义为某应用，如服务端 IP 地址：192.168.0/24、192.168.1.100-192.168.1.200 等，站点应用多用于标识某条链路。定义完成后，即可按照指定站点信息进行统计。以站点(链路)为视角，进行数据检索、回溯、监控告警及报表统计。
其他	MPLS	可统计网络流量中的 MPLS 标签，以 MPLS 标签为视角，进行数据检索、回溯、监控告警及报表统计
	QOS	可统计网络流量中的 QOS 信息，以 QOS ID 为视角，进行数据检索、回溯、监控告警及报表统计
	网络位置	可基于用户我的网络的定义，进行快速的数据过滤，如客户端服务端都在我的网络内、客户端服务端都不在我的网络内、服务端在我的网络内，客户端在我的网络内，该维度主要用户数据快速过滤，识别客户端服务端在不在数据中心内。
	MAC 地址	可统计网络流量中的源、目的 MAC 地址信息，以

		MAC 地址为视角，进行数据检索、回溯、监控告警及报表统计
	MAC 地址厂商	nCompass 数据可视化平台内置 MAC 地址厂商库，可自动识别 MAC 地址所属的厂商，如 Dell、F5、H3C、华为等。该维度多用于 MAC 身份标识以及过滤统计
	IP 来源信息	nCompass 数据可视化平台内置全球 IP 地址库，可自动识别 IP 的来源信息，如国家、省份、城市、运营商等。该维度多用于 IP 身份标识以及用户分布统计
	VTEP IP	可统计 SDN 网络中 Vxlan 隧道的端点设备 IP，可用于 SDN 网络路劲的追踪分析

监控指标：

指标分类	指标名称	用途说明
网络流量指标	总吞吐量	该指标用于监控传输过程中，主机之间实际传输平均速率，单位为 bps（bit per second）。
	流入吞吐量	该指标用于监控传输过程中，以我的网络为参考点，外部 IP 流向我的网络内部 IP 平均传输速率，单位为 bps（bit per second）。
	流出吞吐量	该指标用于监控传输过程中，以我的网络为参考点，我的网络中内部 IP 流向外部 IP 平均传输速率，单位为 bps（bit per second）。
	总包数	该指标用于统计交互过程中，主机之间交互的数据包总数。总包数=流入包数+流出包数。
	流入包数	该指标用于统计交互过程中，以我的网络作为参考点，流入我的网络的数据包数量。
	流出包数	该指标用于统计交互过程中，以我的网络作为参考点，流出我的网络的数据包数量。

	总流量	该指标用于统计单位时间内主机之间传输的数据量大小，单位为 Byte。总流量=流入流量+流出流量+网络外流量+网络内流量。
	流入流量	该指标用于统计以我的网络为参考点，单位时间内外部 IP 流入我的网络内部 IP 的数据量大小，单位为 Byte。
	流出流量	该指标用于统计以我的网络为参考点，单位时间内内部 IP 流向外部 IP 的数据量大小，单位为 Byte。
	总 PPS	
	流入 PPS	该指标用于统计交互过程中，以我的网络作为参考点，流入我的网络的数据包传输速率，单位为 pps（packet per second）。
	流出 PPS	该指标用于统计数据交互过程中，以我的网络作为参考点，流出我的网络的数据包传输速率，单位为 pps（packet per second）。
	小包个数	该指标用于统计交互过程中，数据包长度 <

		128Byte 的数据包数量。
	中包个数	该指标用于统计交互过程中，数据包长度≥128Byte 且＜512Byte 的数据包数量。
	大包个数	该指标用于统计交互过程中，数据包长度≥512Byte 的数据包数量。
	站点流入利用率	该指标用于评估流入带宽使用量，默认情况下按 1G 带宽计算带宽占用比。
	站点流出利用率	该指标用于评估流出带宽使用量，默认情况下按 1G 带宽计算带宽占用比。
	客户端数量	该指标用于统计单位时间内访问应用的总客户端数量。
	应用数量	该指标用于统计单位时间内客户端访问的的总应用数量。
网络性能指标	丢包率	该指标用于计算数据传输过程中，两端出现丢包的概率。丢包率=客户侧丢包率+服务侧丢包率。
	客户侧丢包率	该指标用于计算数据传输过程中，客户侧出现丢包的概率。客户侧丢包率=客户侧丢包数/客户侧

		总包数。
	服务侧丢包率	该指标用于计算数据传输过程中，服务侧出现丢包的概率。服务侧丢包率=服务侧丢包数/服务侧总包数。
	网络时延	该指标用于计算交互过程中，两端网络传输时延+响应的平均时延。网络时延=客户端网络时延+服务端网络时延。
	客户端网络时延	该指标用于计算交互过程中，客户端至监控节点网络传输时延+客户端响应的平均时延。
	服务端网络时延	该指标用于计算交互过程中，服务端至监控节点网络传输时延+应用响应的平均时延。
	重传时延	该指标用于计算数据传输过程中，因两端丢包造成重传的平均间隔时间。重传时延=客户端重传时延+服务端重传时延。
	客户端重传时延	该指标用于计算数据传输过程中，因服务端丢包造成客户端重传的平均间隔时间。
	服务端重传时延	该指标用于计算数据传输过程中，因客户端丢包

		造成服务端重传的平均间隔时间。
网络连接指标	SYN 包数量	该指标用于统计 TCP 建立连接三次握手过程中，客户端发起的建连请求 SYN 次数。若建连过程中请求包发生丢包重传 SYN 包数量会累加。例如丢包重传一次，SYN 包数量则计数为 2 个。区别于“建连请求数”。
	SYNACK 包数量	该指标用于统计 TCP 建立连接三次握手过程中，服务端回复的建连响应 ACK+SYN 次数。若建连过程中回复包发生丢包重传 ACK+SYN 包数量会累加。例如丢包重传一次，ACK+SYN 包数量则计数为 2 个。
	建连请求数	该指标用于统计 TCP 建立连接三次握手过程中，客户端发起的请求次数 ,每个会话仅计数一次。区别于“SYN 包数量”
	新建会话数	该指标用于统计 TCP 建立连接三次握手时，TCP 交互隧道是否建立成功。若成功则新建会话数计数 1 个，失败则不计数。
	活动会话数	该指标用于统计当前一分钟第 58 秒仍存在的会

		话数量。
	建连成功率	统计 TCP 建连成功率
	建连失败数	该指标用于统计 TCP 建立连接时，TCP 交互隧道是否建立成功。若失败则建连失败数计数 1 个，成功则不计数。
	建连失败率	该指标用于统计 TCP 建立连接时，TCP 交互隧道建立成功率。建连失败率=建连失败数/建连请求数。
	建连服务端失败	该指标用于统计 TCP 建立连接三次握手时，所有因服务端异常导致失败的总次数。服务端建连失败=建连服务端重置+建连服务端无响应。
	建连服务端重置	该指标用于分析 TCP 建立连接三次握手时失败的原因，服务端拒接对外提供服务。
	建连服务端无响应	该指标用于分析 TCP 建立连接三次握手时失败的原因，服务端没有响应客户端的建连请求。
	建连客户端失败	该指标用于统计 TCP 建立连接三次握手时，所有因客户端异常导致失败的总次数。客户端建连失

		败=建连客户端重置+建连客户端无响应。
	端口复用	统计 TCP 交互过程中端口复用的次数
	建连客户端无响应	该指标用于分析 TCP 建立连接三次握手时失败的原因，当客户端出现异常不再响应后续建连动作。
	客户端 Reset	两端数据交互过程中，服务端正常发送了数据内容给客户端，但客户端因异常拒收服务端返回的带数据内容，并拆除连接。
	服务端 Reset	两端数据交互过程中，客户端正常发送了数据内容给服务端，但服务端因异常拒收客户端发送的带数据内容，并拆除连接。
	建连客户端重传	该指标用于统计 TCP 建立连接三次握手时，因服务端网络质量较差出现了丢包重传事件。建连客户端重传数值计数会累加。例如客户端重传一次，计数为 1 个，客户端重传二次，计数为 2 个。
	建连服务端重传	该指标用于统计 TCP 建立连接三次握手时，因客户端网络质量较差出现了丢包重传事件。建连服务端重传数值计数会累加。例如服务端重传一次，

		计数为 1 个，服务端重传二次，计数为 2 个。
	拆连个数	统计 TCP 连接的拆链个数
	客户端拆连请求数	该指标用于统计 TCP 建立拆连过程中，客户端先发起了拆连请求，每个会话仅计数一次。
	服务端拆连请求数	该指标用于统计 TCP 建立拆连过程中，服务端先发起了拆连请求，每个会话仅计数一次。
	中间人攻击次数	该指标用于统计中间人攻击的次数
应用性能指标	TCP 建连时间	该指标用于计算 TCP 建立连接三次握手总耗时。
	应用响应时间	该指标用于计算数据交互过程中，客户端发送带数据的请求与服务器回复带数据的响应平均间隔时间。
	用户体验时间	该指标用于评估用户访问业务实际体验平均时间，记录当客户端发起一次数据请求到服务端回复完所有数据的时间差值。
	峰值响应时间	该指标用于统计数据交互过程中，最大一次应用响应时间。

	首包时延	
	客户端网络时延	该指标用于计算交互过程中，客户端至监控节点网络传输时延+客户端响应的平均时延。
	服务端网络时延	该指标用于计算交互过程中，服务端至监控节点网络传输时延+应用响应的平均时延。
	客户端重传时延	该指标用于计算数据传输过程中，因服务端丢包造成客户端重传的平均间隔时间。
	服务端重传时延	该指标用于计算数据传输过程中，因客户端丢包造成服务端重传的平均间隔时间。
	响应快	该指标用于评估数据交互过程中，服务器响应快慢分布，分为两种场景。 1. 已定义为应用按应用定义内响应时延配置栏数值计算，默认场景下应用响应时间＜200ms 则响应快指标计数+1。 未定义为应用的 IP 默认按＜100ms 则响应快指标计数+1。
	响应慢	该指标用于评估数据交互过程中，服务器响应快慢分布，分为两种场景。

		1. 已定义为应用按应用定义内响应时延配置栏数值计算，默认场景下应用响应时间≥500ms 且＜1000ms 则响应快指标计数+1。 未定义为应用的 IP 默认按≥300ms 且＜500ms 则响应快指标计数+1。
	响应超时	该指标用于统计数据交互过程中，服务端响应时间≥1000ms 的次数。
主机性能指标	TCP 窗口时延	该指标用于记录数据交互过程中，因主机性能下降为 0 窗口所产生的交互停顿平均时间。TCP 窗口时延=客户端小窗口时延+服务端小窗口时延。
	客户端小窗口	该指标用于评估客户端综合处理性能，每个数据包 TCP 头部包含 Windows size 字段，若该字段数值≤512 客户端小窗口产生计数。每个数据包均统计。
	客户端小窗口时延	该指标用于记录数据交互过程中，因客户端性能下降为 0 窗口所产生的交互停顿平均时间。
	服务端小窗口	该指标用于评估服务器综合处理性能，每个数据包 TCP 头部包含 Windows size 字段，若该字段

		数值≤512 服务端小窗口产生计数。每个数据包均统计。
	服务端小窗口时延	该指标用于记录数据交互过程中，因服务器性能下降为零窗口所产生的交互停顿平均时间。
	客户端净荷	该指标用于统计数据交互过程中，客户端传输的数据总量。
	服务端净荷	该指标用于统计数据交互过程中，服务端传输的数据总量。