恒景科技
Netscout产品介绍

主题

- 公司简介
- 整体解决方案简介
- 服务保障解决方案
- 安全保障解决方案
- 流量安全调度解决方案
- 优势总结

NETSCOUT

NETSCOUT公司简介

可视性无边界

可视性无边界

NETSCOUT

愿景：充分利用IP智能的潜力，实现无与伦比的业务洞察力
和决策能力

使命：交付世界领先的、与时俱进的数据信息平台，通过自动化
和无处不在的实时监控，保障安全、管理风险、驱动业务性能

VISIBILITY WITHOUT BORDERS™

目标：互联世界的守护者（Guardians of Connected World）

价值：帮助客户加快数字化转型

服务保障分析

网络安全分析

大数据分析

Gartner NPMD魔力象限

•Gartner魔力象限反映了NETSCOUT的真实市场地位

•在第一象限里面，NETSCOUT的执行能力是最强的（纵轴），这反映了NETSCOUT在把技术产品化的能力以及对于收购后的产品整合能力是最强的

•Gartner对第一象限厂商收入的估计：
- NETSCOUT： $500~750 million
- Riverbed： $100~250 million
- Viavi：$100~250 million

数据来源: Gartner, 2017年2月

Gartner NPMD魔力象限

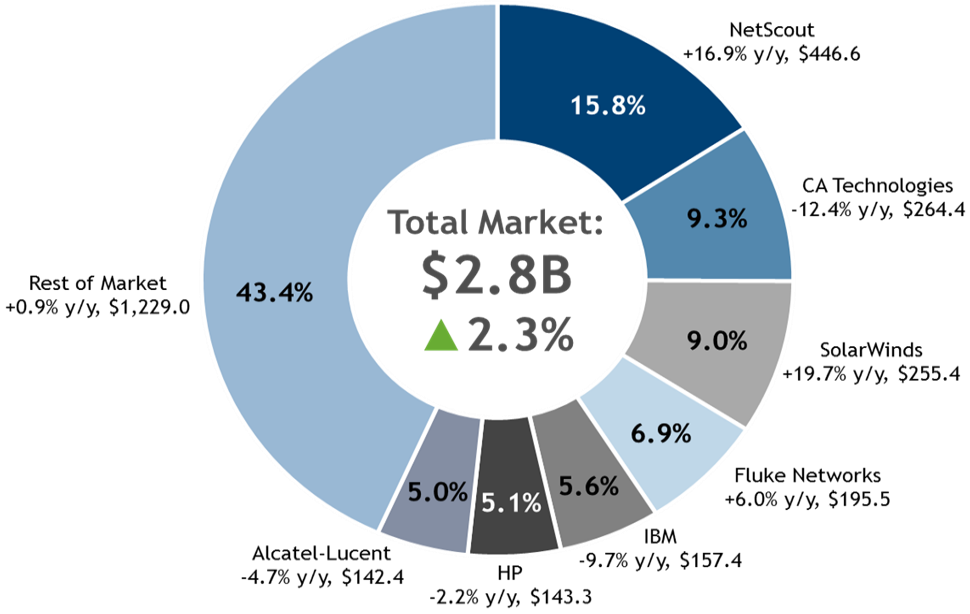
2018年和2019年数据

资料来源：Gartner（2018年2月）

资料来源：Gartner（2019年2月）

NETSCOUT市场占有率第一（IDC报告）

全球网络管理软件和设备



Worldwide Network Management Software and Appliance Revenue by Vendor, 2013, 2014, and 1H15

	2013		2014		1H15	
Vendor	Revenue ($M)	Share (%)	Revenue ($M)	Share (%)	Revenue ($M)	Share (%)
NetScout	382	13.8	446.6	15.8	220.1	15.9
CA Technologies	301.9	10.9	264.4	9.3	111.4	8.1
SolarWinds	213.4	7.7	255.4	9	127.9	9.2
Fluke Networks	184.5	6.7	195.5	6.9	93	6.7
IBM	174.3	6.3	157.4	5.6	67	4.8
HP	146.5	5.3	143.3	5.1	56.1	4.1
Alcatel-Lucent	149.4	5.4	142.4	5	58.8	4.3
Riverbed	77.4	2.8	112.1	4	59.5	4.3
EMC	158.9	5.7	102.3	3.6	45.1	3.3
Other	981.9	35.4	1,014.50	35.8	544.2	39.3
Total	2,770.30	100	2,834.00	100	1,383.00	100

Source: IDC, 2016

数据来源: IDC, 2016

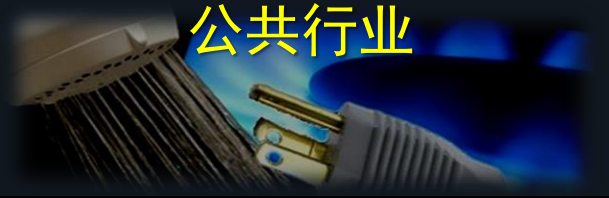
注：NETSCOUT已经收购并整合了Fluke Networks

NETSCOUT得到全球顶级公司信任

— 保障业务交付和业务质量

排名前10的10个公司
金融服务

排名前20的19个公司
公共行业



排名前10的10个公司
航天国防

美军的所有5个分支
军队

财富榜排名前100的公司有
97 个使用NETSCOUT产品

排名前20的20个公司
服务提供商

排名前20中的19个公司
商业及银行业

排名前10的10个公司
航空公司

排名前10的10个公司
生物制药行业

国内主要金融用户名单

序号	行业	客户名称
1	**五大银行**	**中国农业银行**
2	**五大银行**	**中国银行**
3	**五大银行**	**中国建设银行**
4	**五大银行**	**中国工商银行**
5	**五大银行**	**中国交通银行**
6	**央行**	**中国人民银行**
7	银行	招商银行
8	银行	国家开发银行
9	银行	中国进出口银行
10	银行	中国光大银行
11	银行	民生银行
12	银行	中信银行
13	银行	华夏银行
14	银行	平安银行
15	银行	上海浦东发展银行
16	银行	上海银行
17	银行	上海农商行
18	银行	广发银行
19	银行	包商银行
20	银行	昆仑银行
21	银行	宁波银行
22	银行	成都银行

序号	行业	客户名称
23	银行	东亚银行
24	银行	浙江农信
25	银行	广东农信
26	银行	海南农商行
27	银行	天津农商行
28	银行	深圳农商行
29	银行	顺德农商行
30	银行	渣打中国
31	银行	美林中国
32	银行	汇丰中国
33	交易所	中国金融期货交易所
34	交易所	中国外汇交易所
35	交易所	上海证券交易所
36	交易所	深圳证券交易所
37	交易所	上海期货交易所
38	交易所	上海金融期货交易所
39	交易所	上海黄金交易所
40	交易所	上海期货交易所
41	交易所	大连期货交易所
42	交易所	郑州商品交易所
43	银联	中国银联
44	清算	上海清算所

序号	行业	客户名称
46	保险	中国人寿
47	保险	平安保险
48	保险	太平洋保险
49	保险	大地保险
50	保险	太平保险
51	保险	天安保险
52	保险	泰康人寿
53	证券	海通证券
54	证券	招商证券
55	证券	国泰君安
56	证券	华泰证券
57	证券	中信证券
58	证券	光大证券
59	证券	巴克莱资本证券
60	其他	中国期货交易保险金监控中心
61	其他	中国证券金融股份有限公司
62	其他	中小企业股份转让
63	其他	中国证券登记结算
64	其他	中央国债登记结算
65	其他	中国中央存托股份
66	其他	中国烟草商业贸易
67	其他	上海印钞有限公司

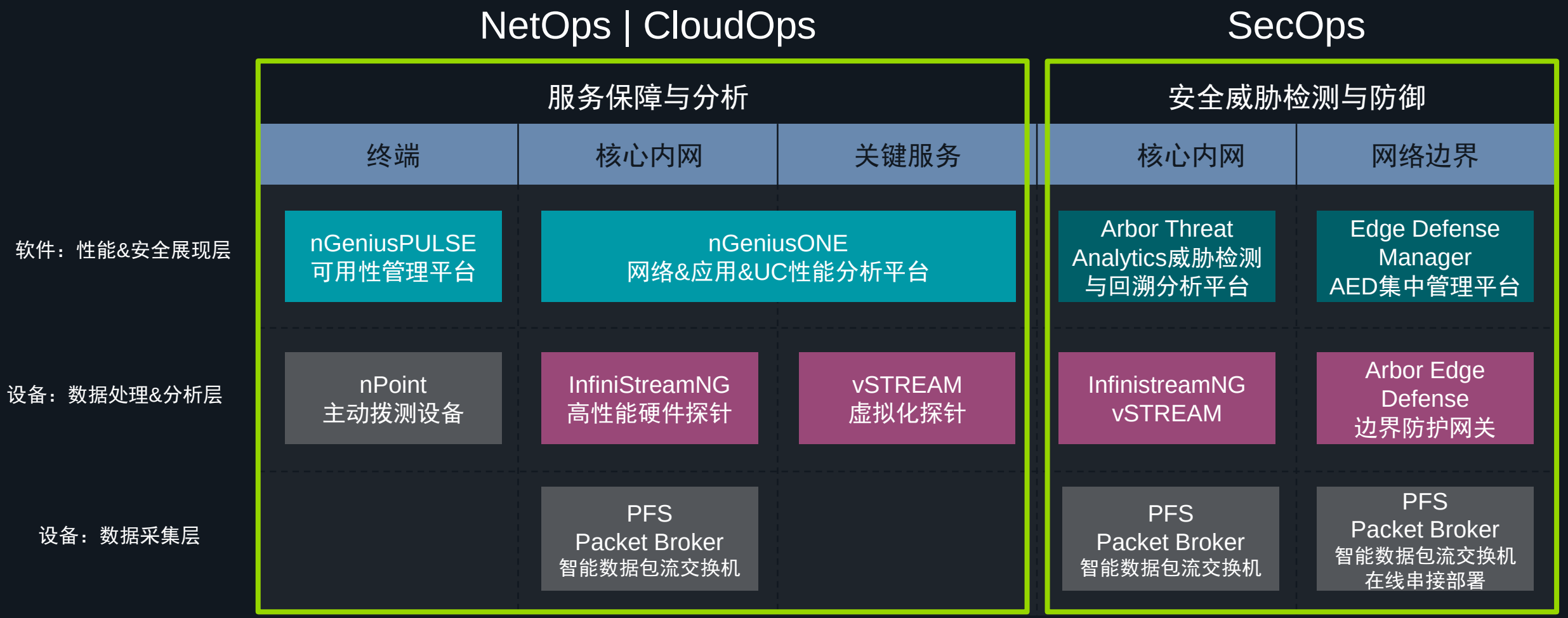
NETSCOUT

NETSCOUT 整体解决方案简介

可视性无边界

NETSCOUT企业产品概览

致力于将Wire Data转化为Smart Data，实现服务保障和安全保障



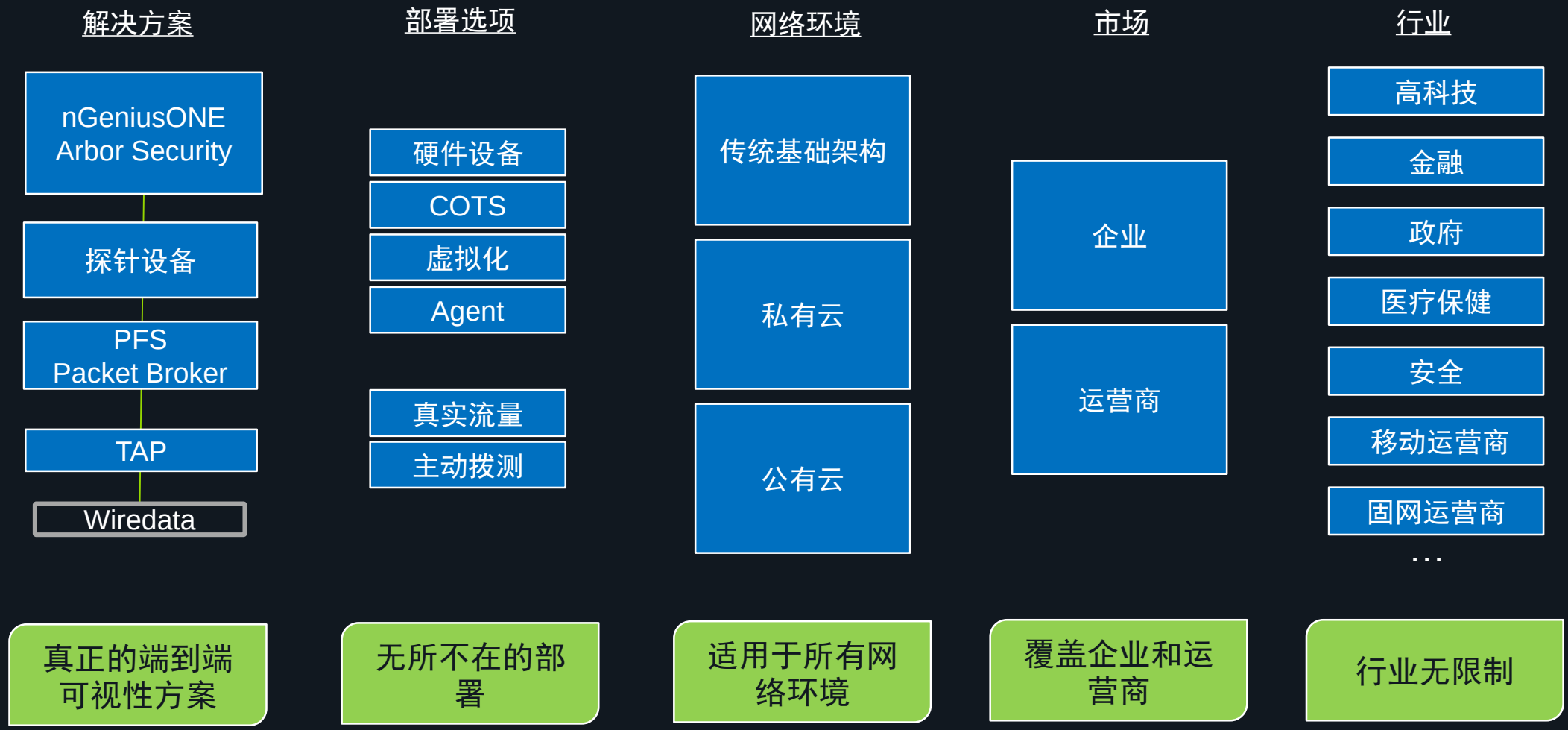
NETSCOUT 主要产品套件

为网络、云、安全运维提供全面的、统一的可视性解决方案

服务保障 nGeniusONE	智能数据包流交换机 nGenius Packet Flow Switch	可用性监测 nGeniusPULSE	边界安全防护 Arbor Edge Defense	威胁分析 Arbor Threat Analytics
				
服务保障 NPM/APM	**数据包流交换机 NPB**	**基础架构性能 IPM**	**边界DDoS和威胁防护**	**内部威胁检测和调查**
被动式 数据包捕获存储 ASI智能分析 端到端的网络和 应用性能可视化	统一的数据包中转 和调度平台: 复制、汇聚、过滤、 标记、去重、协议 封装剥除、切片	健康性监测：服务 器、网络设备 主动性拨测：网络 和应用服务、业务 交易、VoIP SLA监测	DDoS防护 IoC安全威胁防护 防御出站数据泄露 AIF威胁情报库	基于数据包的风险识 别和威胁分析 高效的威胁调查分析 AIF威胁情报库

可视性无边界

端到端的NETSCOUT解决方案，适应所有环境的部署



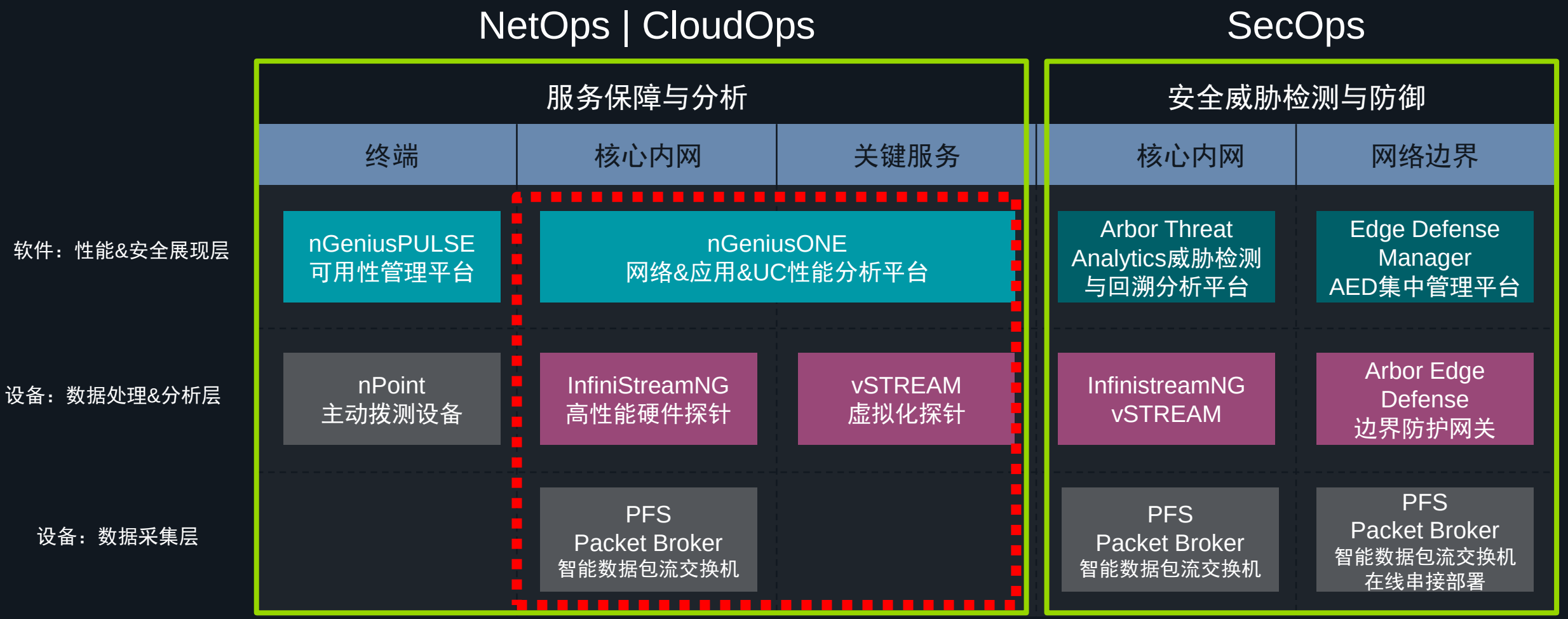
NETSCOUT

服务保障解决方案

nGeniusONE和nGeniusPULSE

nGeniusONE服务保障解决方案

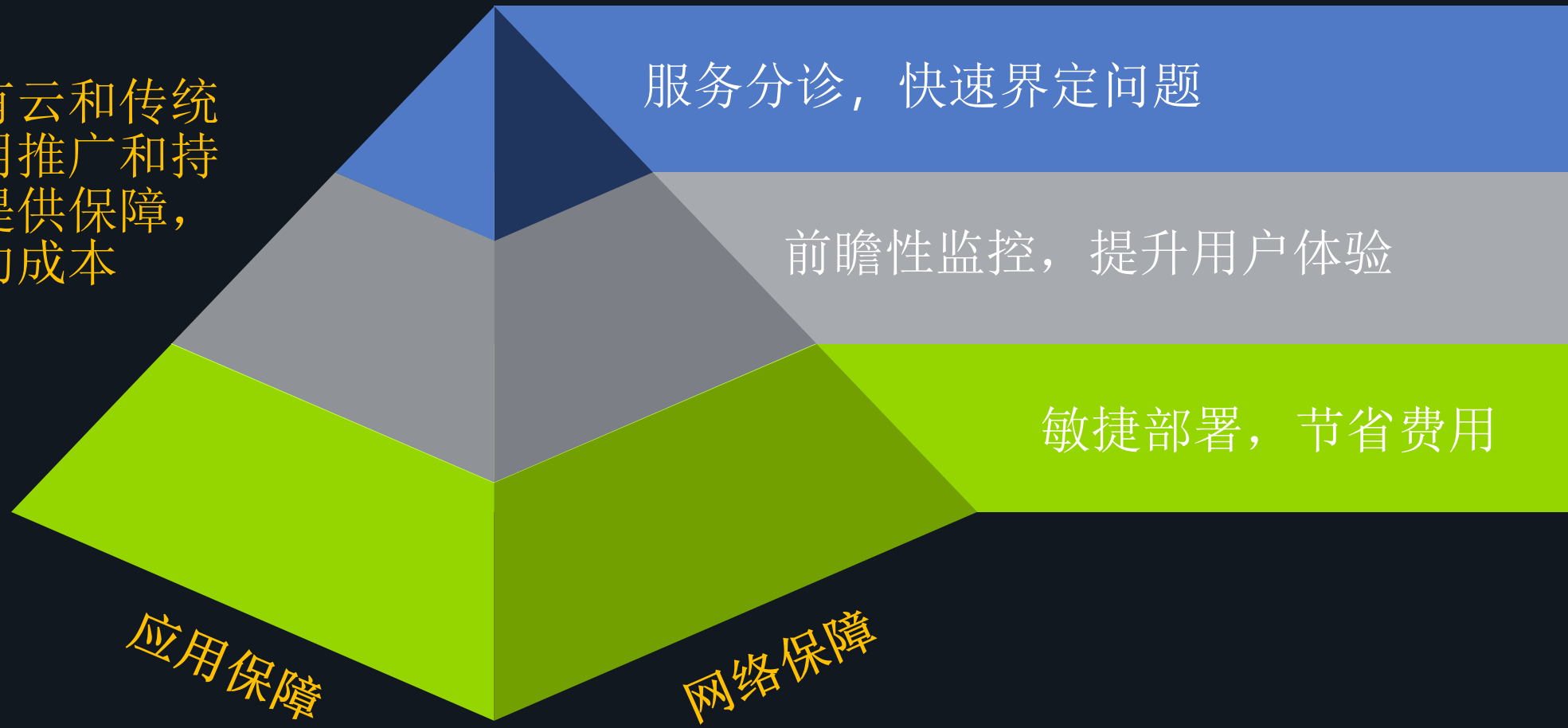
为传统网络、云运维提供全面的、统一的可视性解决方案



nGeniusONE服务保障解决方案

端到端的网络和应用性能可视化

为公有云、私有云和传统基础设施的应用推广和持续的服务性能提供保障，确保成功和节约成本



nGeniusONE统一性能管理平台

融合网络、应用、服务器和UC的统一可视性

可视化和主动预警 | 性能分析 | 优化和规划 | 趋势和报告 | 取证分析

软件：Linux或Windows平台

nGeniusONE 性能管理平台

- 集中管理和配置分布式监控设备
- 对探针解析好的数据入库，统一展现统计和分析结果
- 跨技术领域（NPM+APM）的统一视图
- HTML5.0风格，随时随地访问
- 中文语言支持

Packet-Flow Intelligence

- 所有服务
- 所有节点
- 所有用户
- 所有设备

设备：物理或虚拟探针

nGenius 智能数据源

Packets ASI

交换机配置端口镜像或TAP，将流量发送至监控探针

对所有服务流进行深度包分析，实现普遍的端到端可见性

用户群组

IT 基础架构

AD DNS DHCP Frontend Middlewar SQL

端到端的IP服务流量

服务器群组

nGeniusONE 产品架构

传统数据中心网络部署示意

统一性能管理平台—nGeniusONE

集中管理探针和关联分析数据

当网络和应用性能问题分生时，从数据包流的角度去分析问题的根源

ASI智能数据源

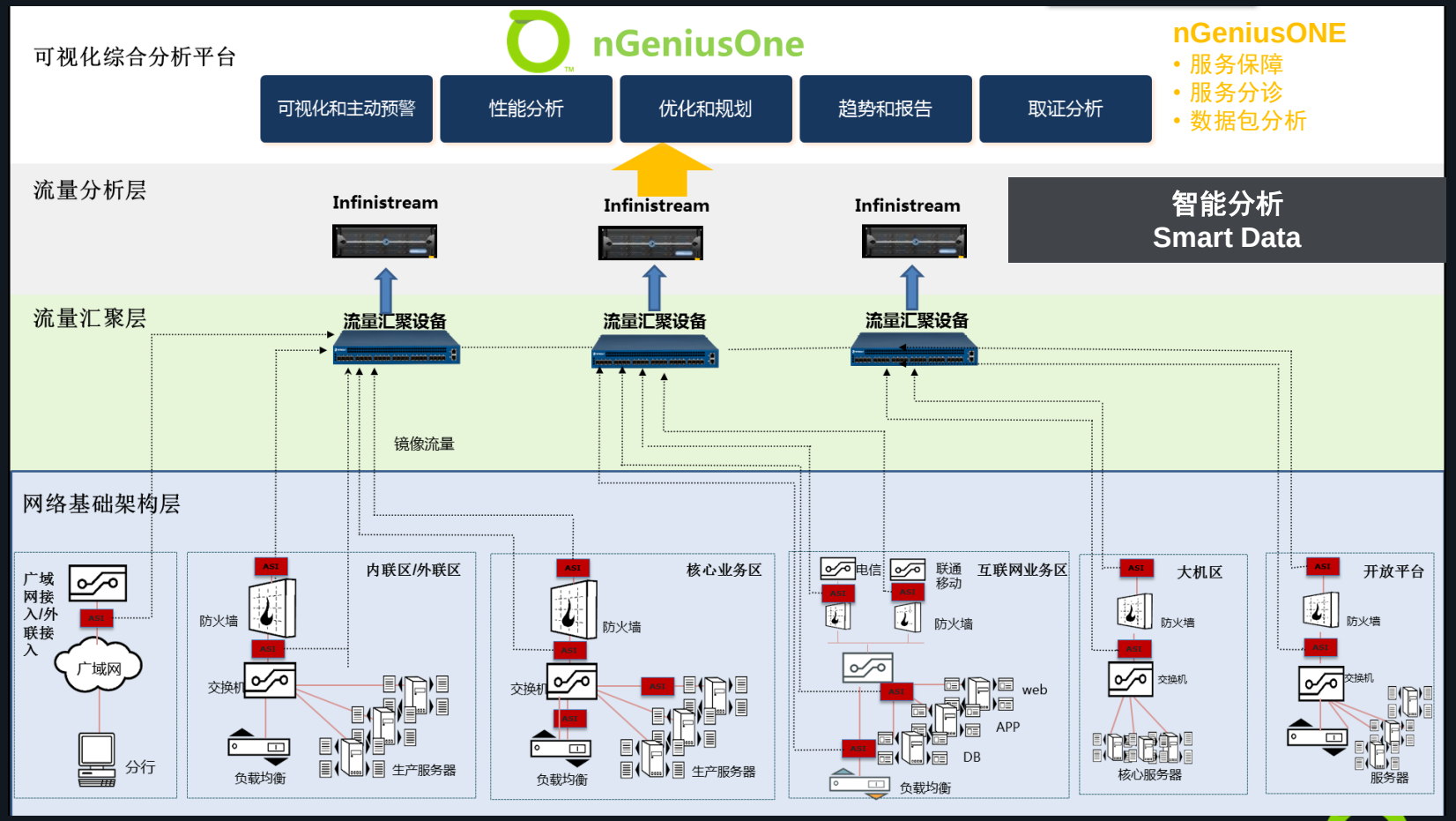
实时流量分析处理和存储

- InfiniStream硬件探针
- vSTREAM云探针
- Flow Collector流采集

数据包中转调度—PFS

收集流量并且高效调度流量

网络镜像数据作为资源，为监测工具集中管理、统一调度数据包



智能数据源 – InfiniStreamNG

新一代多功能探针

InfiniStreamNG

On-premise

私有云

公有云/混合云

厂商自有硬件探针

业界性能优化最好的设备

1G/10G/40G/100G

COTS系列 – 客户自己提供硬件平台

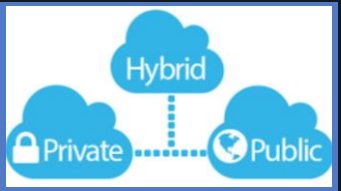
NETSCOUT提供 InfiniStreamNG ASI软件

NETSCOUT提供 ASI 加速网卡

vSTREAM虚拟化探针

具备**InfiniStreamNG**同样的功能

灵活的部署选项（公有云、私有云、虚拟化环境）



NETSCOUT具有全面的适用于传统物理网络、公有云、私有云和虚拟化环境的探针设备

对智能数据价值的创新—软件定义分析

新一代多功能智能探针

弹性部署、易扩展、持续更新功能

IP INTELLIGENCE ASI POWERED BY NETSCOUT

“+”

核心专利技术

大数据 & AI

高级威胁分析

UC统一通信监控

网络流量分析

Cyber Optimizer 数据优化

PFX 高级数据包处理（NPB plugin）

InfinistreamNG 平台

多功能，一机多用

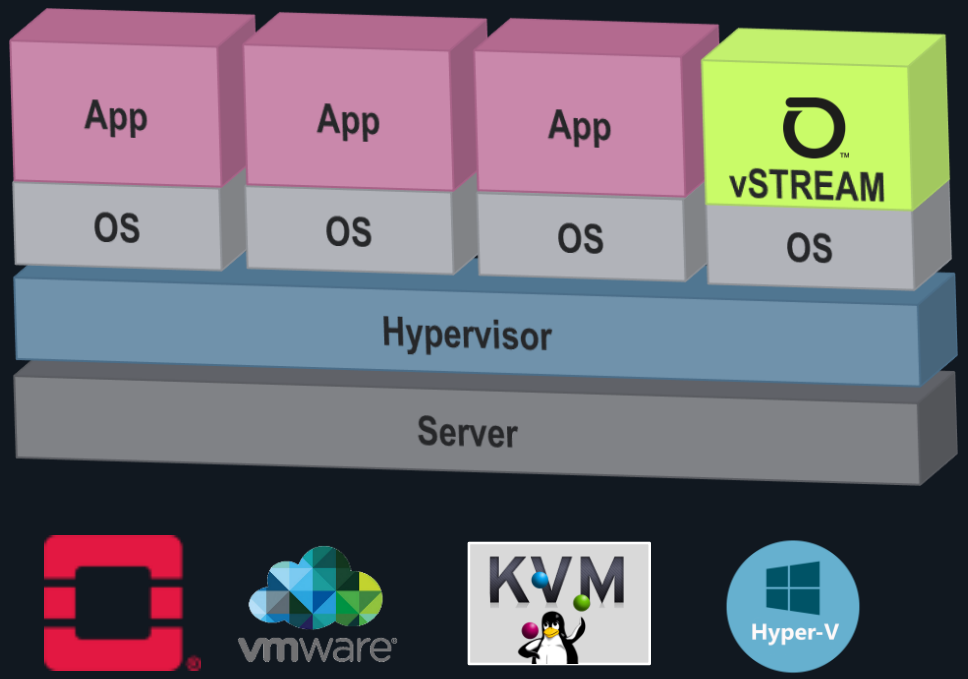
丰富的应用场景

NPM、APM、安全、大数据

更低的 TCO & 更高的 ROI

vSTREAM虚拟探针

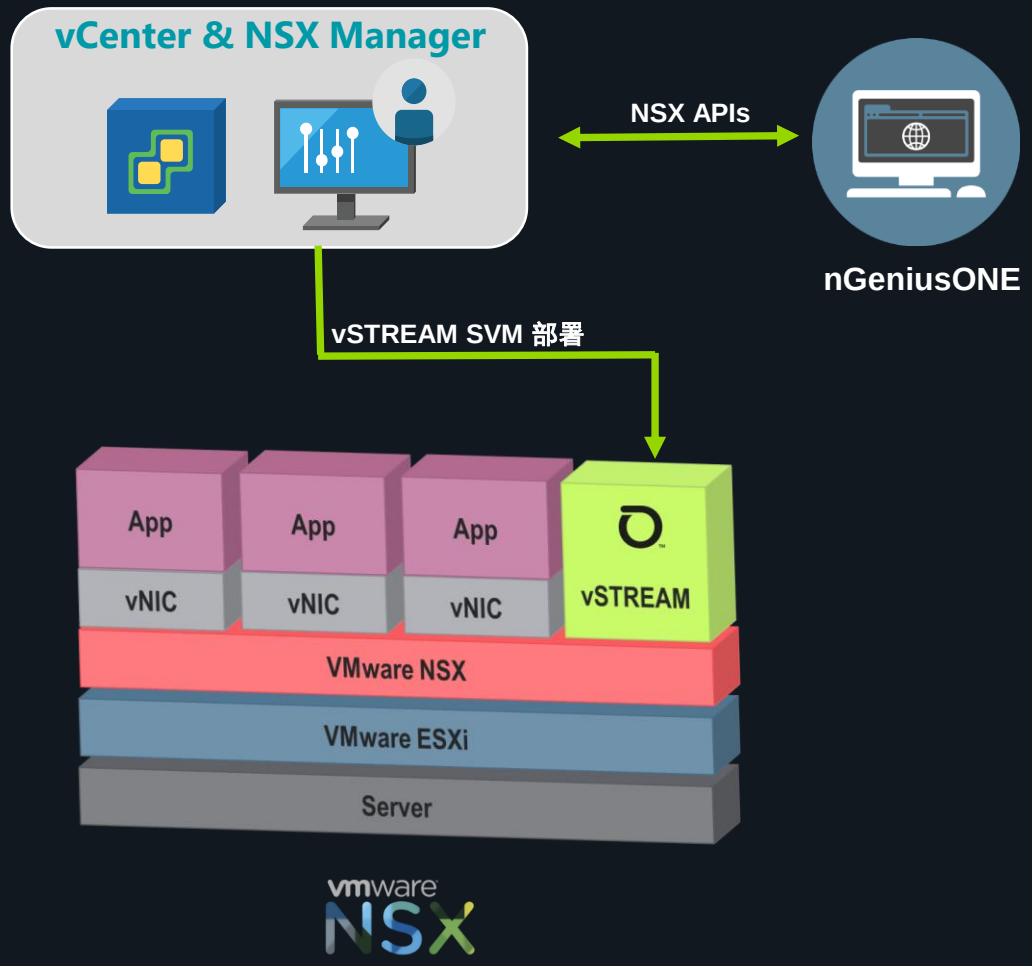
独立虚机模式 (VNF)



- **安装于独立的虚机**
  - ✓ 通过vSwitch镜像获取流量
- **支持公有/私有云**
  - ✓ AWS, Azure, Google, 腾讯云
  - ✓ OpenStack, VMware , Hyper-V
- **24x7**
  - ✓ 实时监控
  - ✓ 数据包捕获和存储
  - ✓ 支持数据包转发
- ***性能加速***
  - ✓ DPDK
  - ✓ SR-IOV & PCI Pass through

vSTREAM 虚拟化探针

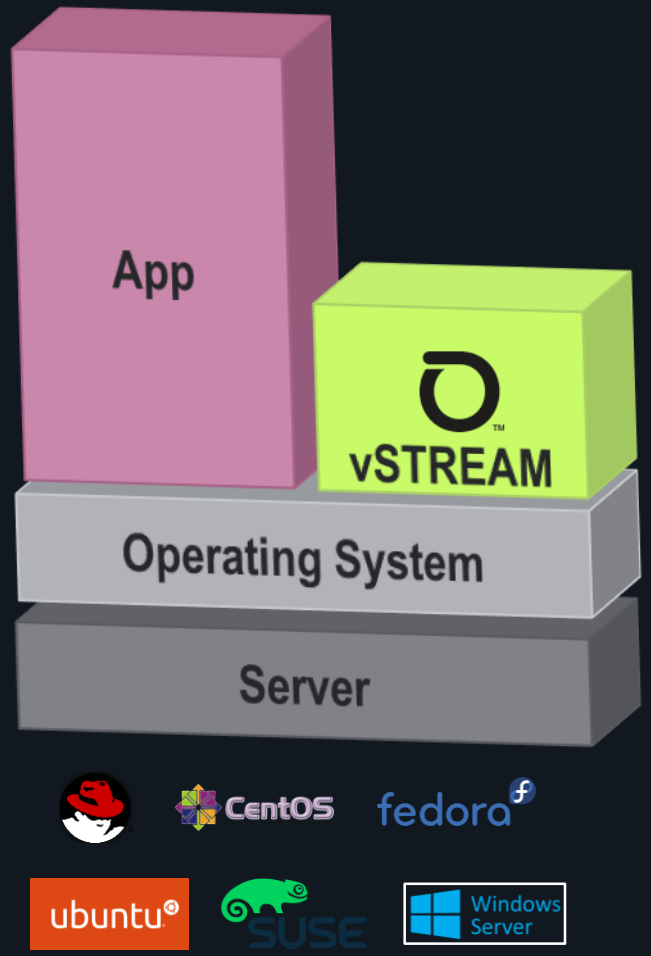
VMware NSX集成模式（SVM）



- **VMware NSX Certified**
  - ✓ 轻量级的 VMware NSX 服务虚机 (SVM)
  - ✓ 跨多个NSX集群自动安装
  - ✓ 下一代软件定义数据中心（SDCC）的服务监控
- **24x7**
  - ✓ 实时监控
  - ✓ 数据包捕获和存储
  - ✓ 支持数据包转发
- **最小化资源占用**
  - ✓ 最小 2个 vCPU
  - ✓ 最小化数据包在虚拟环境中的移动

vSTREAM虚拟化探针

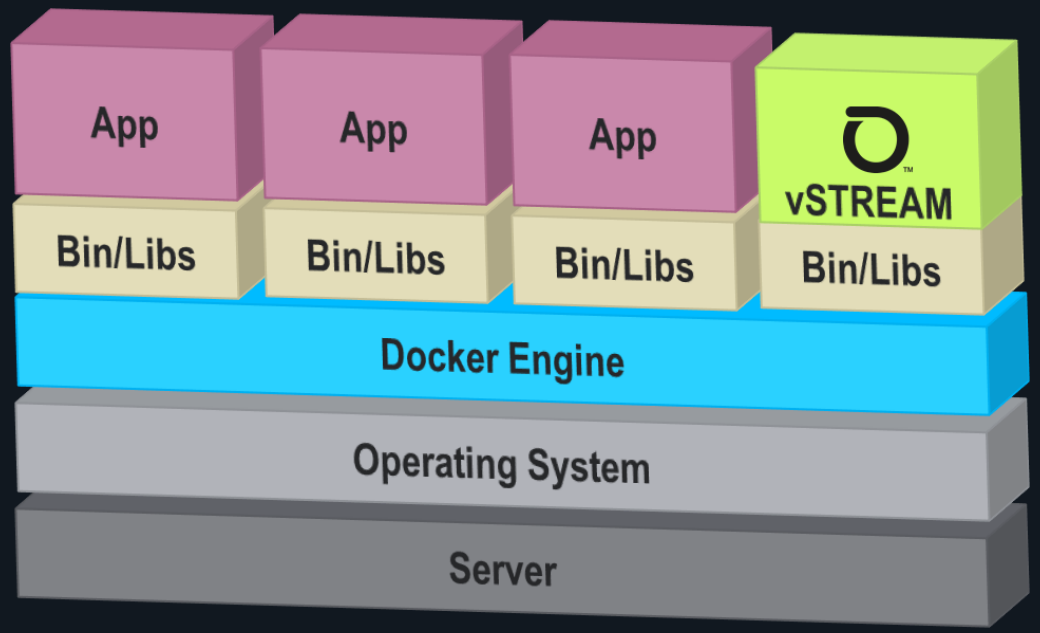
Embedded嵌入式模式（Agent）



- **智能可视性**
  - ✓ 实时ASI指标
  - ✓ 流量转发&过滤
- **最小化资源占用**
  - ✓ 可限制为1个 vCPU
- **支持公有/私有云**
  - ✓ AWS, Azure, Google, 腾讯云
  - ✓ OpenStack, VMware, Hyper-V
- **支持的操作系统**
  - ✓ Linux – Ubuntu, Red Hat/CentOS, SUSE
  - ✓ Windows Server

vSTREAM虚拟化探针

容器化的Smart Data



docker

- **作为独立的容器部署**
  - ✓ 通过Docker Engine获取流量
- **智能可视性**
  - ✓ 实时ASI指标
  - ✓ 流量转发&过滤
- **最小化资源占用**
  - ✓ 可限制为1个 vCPU
- **Containers支持**
  - ✓ Docker
  - ✓ Kubernetes

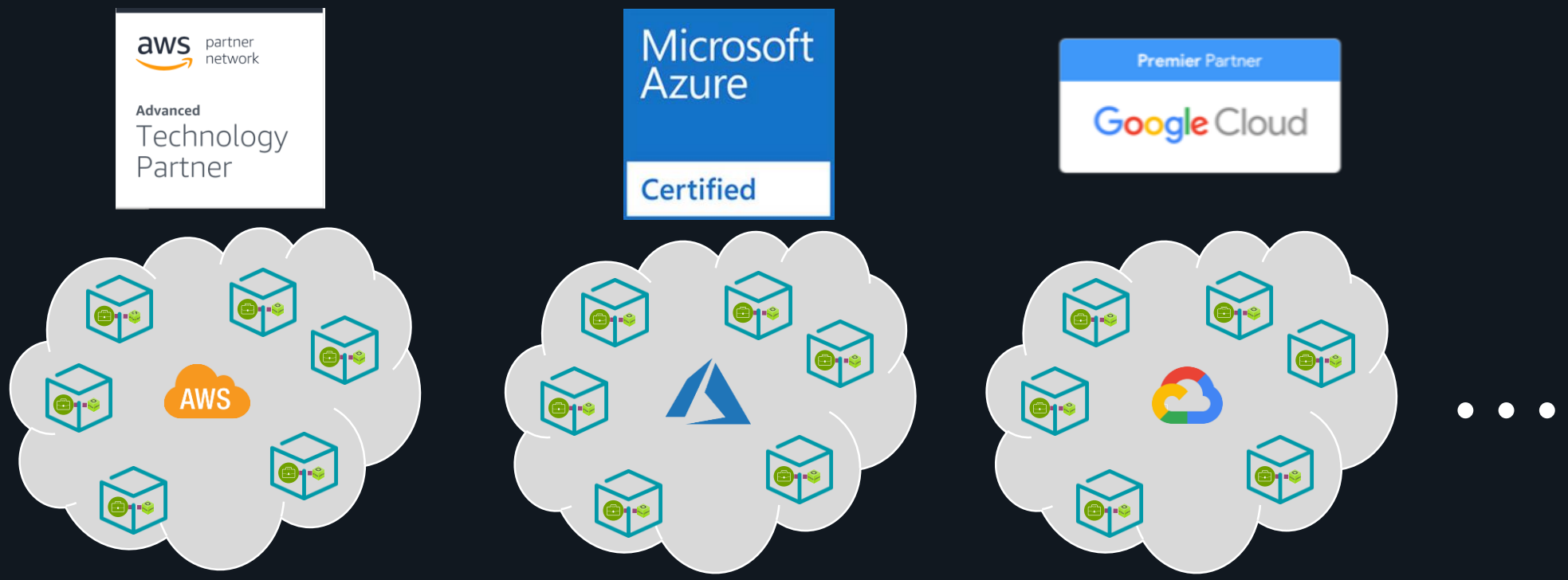
vSTREAM 对混合和多云环境

统一的 vSTREAM 实施，一致的数据源

- 适用于多种环境
  - 嵌入式或标准模式部署
  - 私有云、公有云，容器，裸金属(Bare Metal)
- ASI 智能数据
  - 全面的 ASI 指标
  - 完整的数据包功能
  - 服务保障和安全保障
- 高可扩展性
  - 最小1个 vCPU
  - 增加资源，增长性能
  - 流量转发和过滤

vSTREAM虚拟化探针对公有云的支持

Smart Data for Public Cloud



AWS Web Services

Azure web Services

Google Cloud*

NETSCOUT提供云的全面可视性

提升业务向云环境迁移的信心

网络和应用保障

KPI
延迟，错误
交易
服务分诊

服务依赖性

清晰服务节点依赖
关系和业务流程
验证应用通信和安
全策略

数据包分析

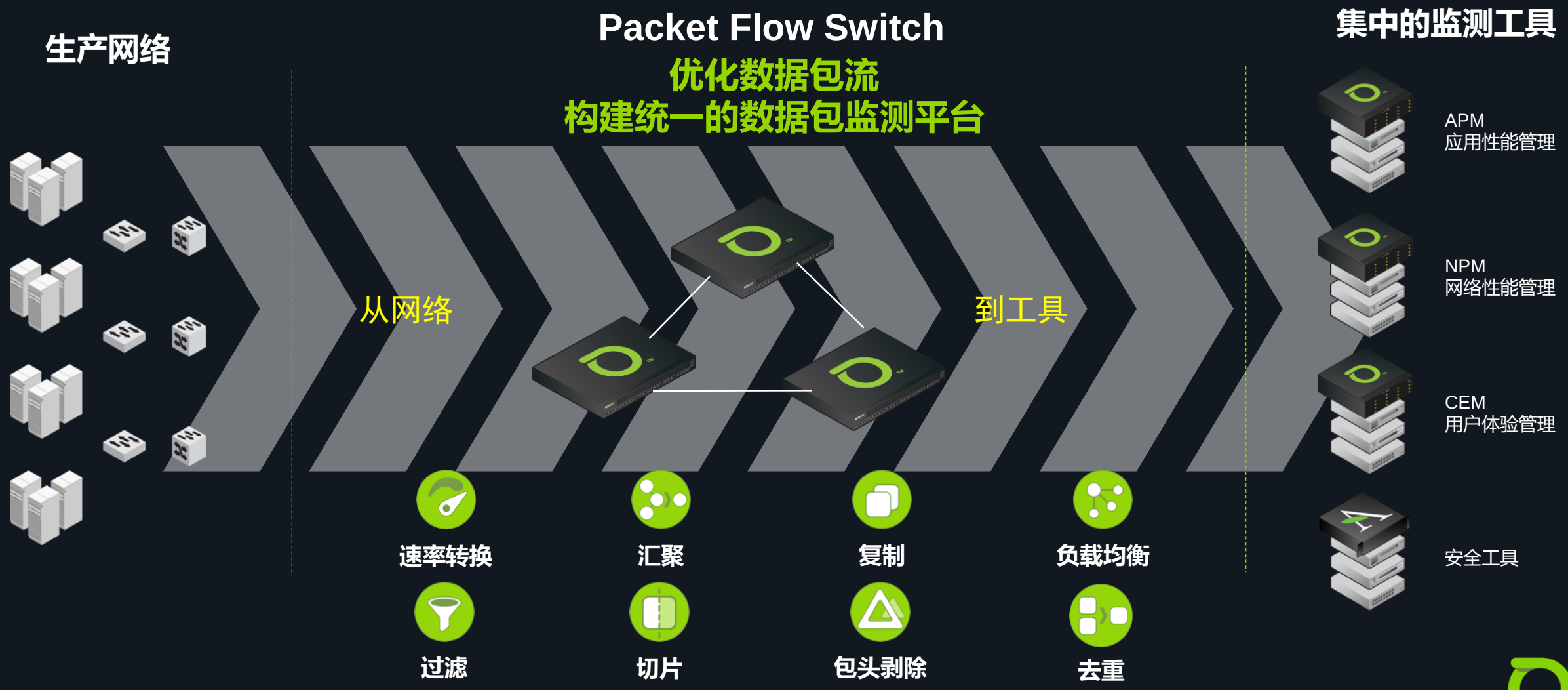
虚拟化环境的数据
包存储
数据溯源
根源分析

数据包转发

为安全工具或第三
方工具提供原始数
据包
按需转发，过滤，
切片

智能数据包流交换机 (PFS)

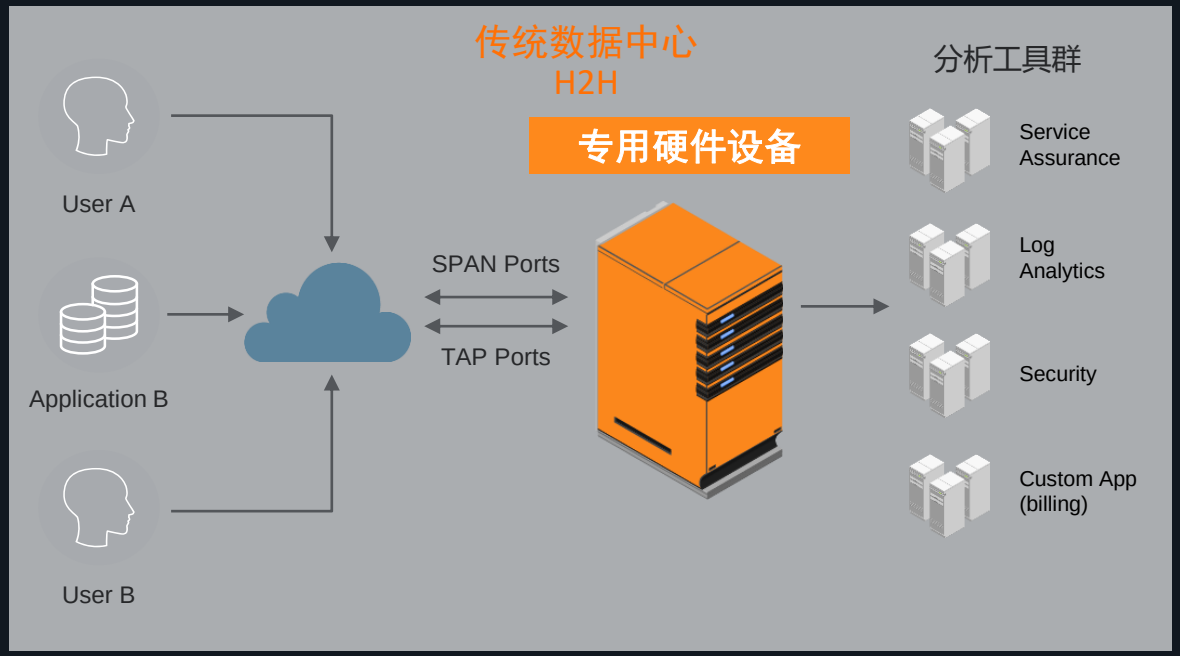
连接网络与监测工具的数据包中转设备（NPB）

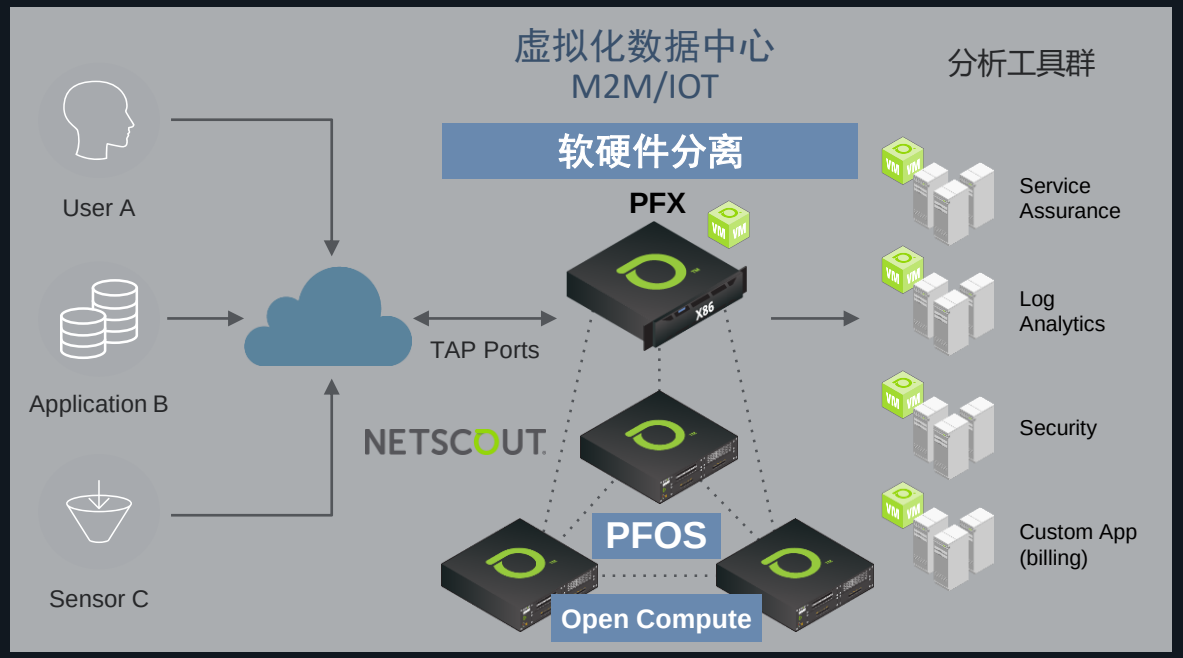


新一代NPB设备：Packet Broker2.0

软硬件解耦

Packet Broker 1.0 → Packet Broker 2.0





使用厂家专用的硬件平台

价格昂贵的固化平台

缺乏扩容升级的弹性

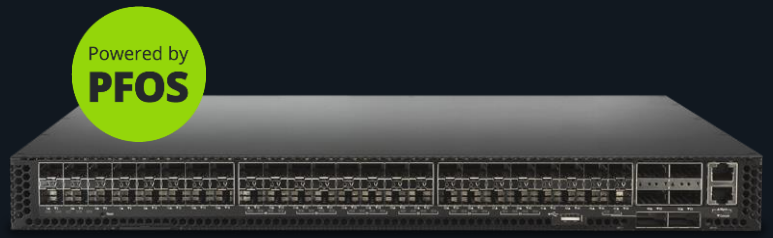
软硬件分离，快速功能迭代

基于X86架构的OCP通用设备，降低成本

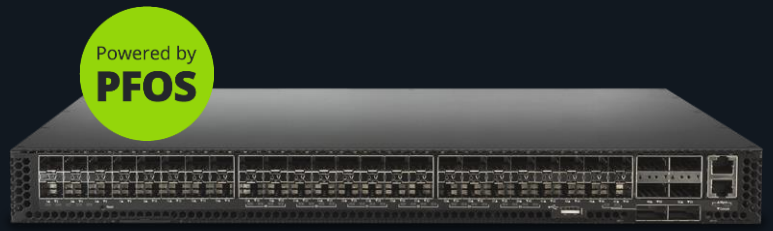
按需升级，敏捷部署，灵活扩展

PFS产品

软硬件解耦—基于开放计算联盟（OCP）的白盒化



PFS-5010：48 x 10GE/1GE + 6 x 40GE
720Gbps线速处理能力



PFS-5110： 48 x 25GE/10GE/1GE + 6 x /100GE/40GE
1.8Tbps线速处理能力

PFS5100：32 x 100GE/40GE
3.2Tbps线速处理能力

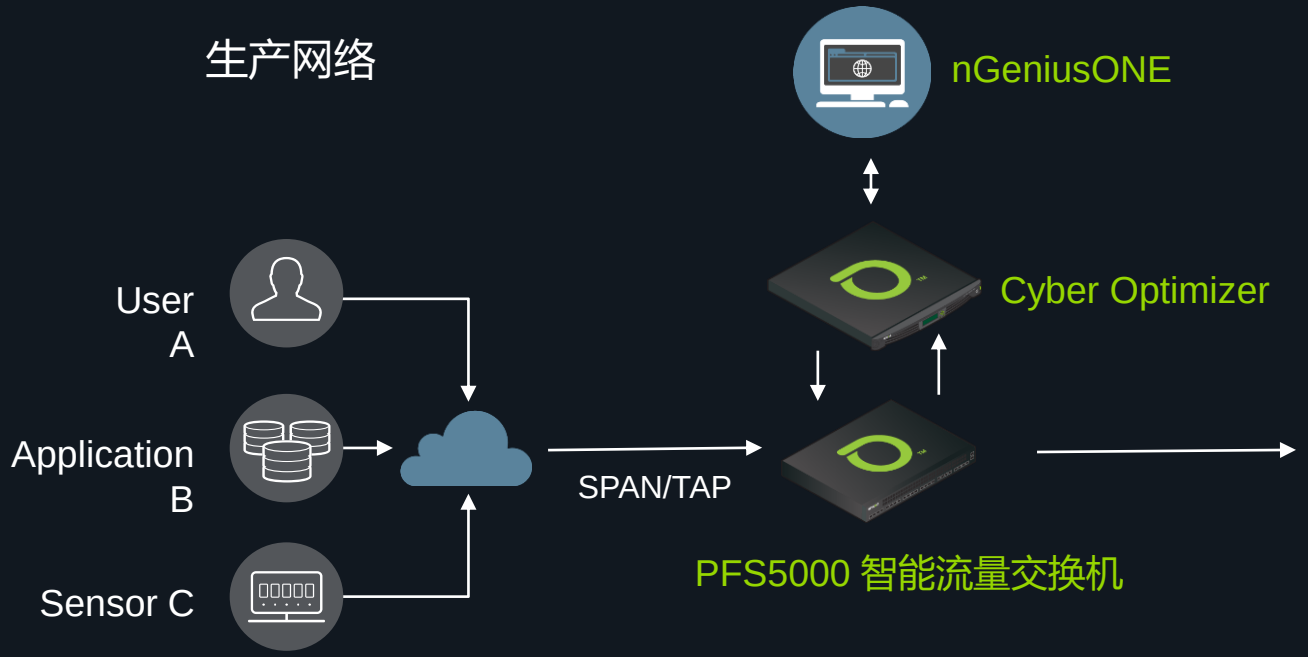
- 100GE可分为2x50GE、4x25GE或4x10GE
- 40GE可分为4x10GE
- 可选择性汇聚
- 1-N、N-1或N-N的复制
- L2 – L4 层过滤
- L7层内容匹配过滤
- 保持会话完整性的负载均衡分流
  - L2-L4 N元组可选
  - 多种XOR和CRC的哈希算法可选
- VLAN Tagging & Stripping
- VN-Tag & VXLAN Stripping
- GRE/IP 隧道终结
- vMesh 动态Full Mesh互联
- CLI、 NETCONF、WebUI 管理
- 基于策略的触发器
- 安全Tool Chaining

提供业界最高端口密度，合理的端口速率匹配，组网架构更合理
如PFS5010可选6个40G口作为上连，确保汇聚不丢包

NETSCOUT对数据采集层的改变—数据整形和优化

软件化的高级数据包梳理

弹性部署、易扩展、持续更新功能



功能和作用

- DPI智能应用过滤
- 数据包存储、检索、输出
- 加密流量清洗
- 头部剥除 （MPLS、GRE、VxLAN等）
- 数据包去重
- 切片& 掩码
- 生成NetFlow

。。。。。。

降低监测和安全工具的投入成本

提升工具的性能

核心专利技术Adaptive Service Intelligence

统一数据格式，Wire Data转化为Smart Data

1

软件为中心
为物理、虚拟化、云环境设计
业界领先
灵活扩展

2

智能数据
多维的元数据
KPI, Flow, Session, Packet
用户，设备，应用，服务，OTT，端到端

3

开放API
Kafka – Streaming
按需 REST
自由输出给第三方

4

绿色部署
处理再存储的模型
使用最少数量的硬件，更小的足迹，
更少的能耗

NETSCOUT服务保障解决方案特点

更完整的覆盖度

- 传统物理网络和云化网络统一的监测
- 面向服务的应用依赖关系视角

更高效的运维

- 自上而下的服务监控工作流
- 动态基线的异常监测告警

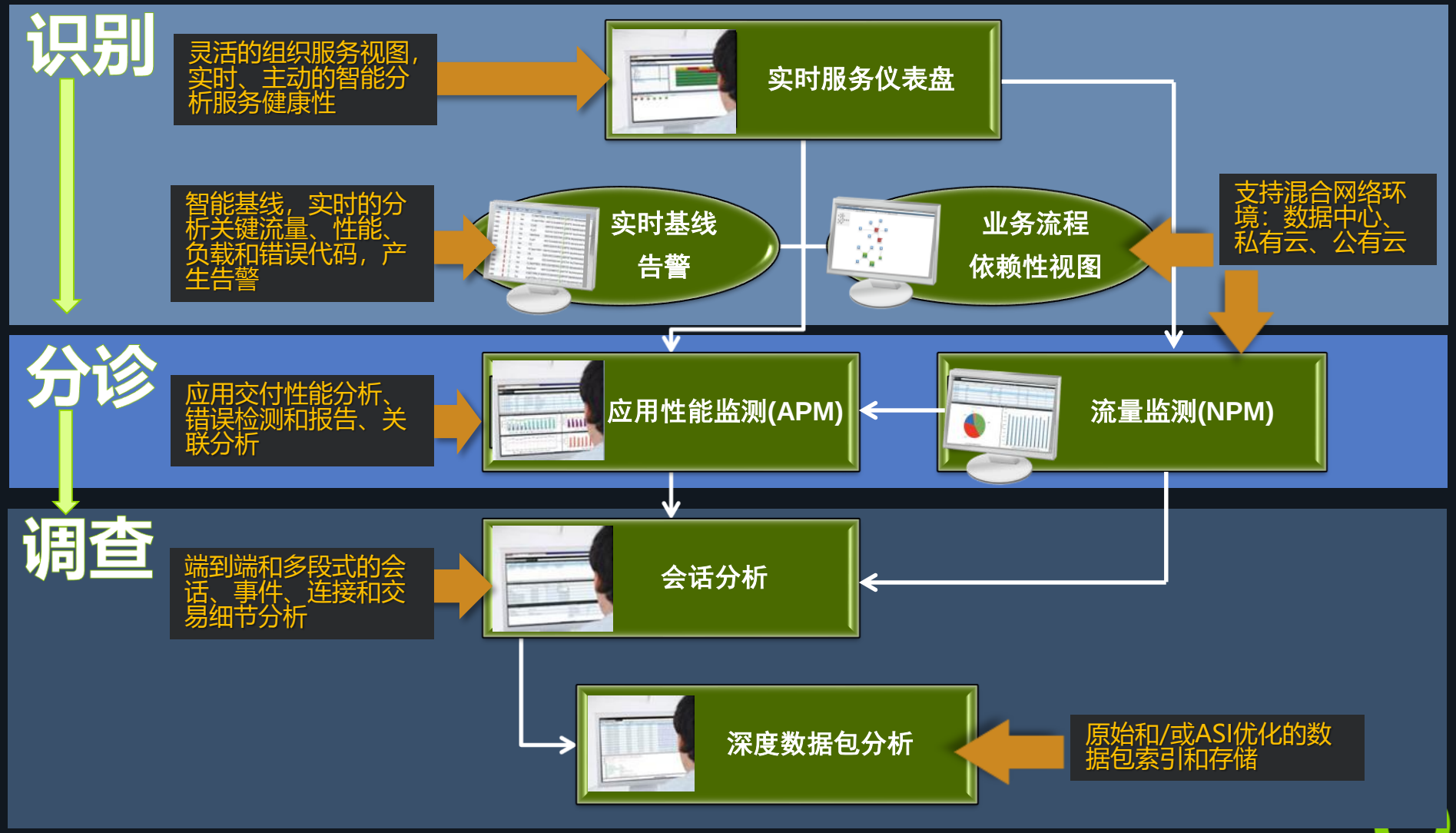
更前瞻的引领

- 软件定义分析
- 主、被动监控融合
- Smart Data元数据的多样化使用

致力于将Wire Data转化为Smart Data，打造通用智能数据平台

以服务为导向的分析工作流

自上而下的工作流



全面的网络应用监控能力

情境分析 Situation Analysis

无需配置
自动分析各种影响延时、失败和可用性的场景

客制化应用监控

ASI Extender提供自开发应用的深度定制监控能力

开箱即用的服务监控

自动识别和深度监控常见企业服务：数据库, MQ, 银联、基础服务 ....

精细化的多维视图

分钟级监控指标
毫秒级突发流量
物理接口、IP站点、MPLS、VLAN、VXLAN、QoS等维度

服务依赖性

基于每个服务，自动映射服务器访问关系
可视化每个节点的KPI

多段关联

自动测量和关联多段会话的延迟

语音 / 视频

集成语音、视频分析模块，监控信令流程和媒体质量

强大的搜索和发现

全局搜索
主机、通信对、应用、应用消息、站点/VLAN/QoS、用户

35

深度包DPI检测

基于Web的应用 (HTTP, HTTPS)	企业应用 (Oracle数据库、MySQL数据库)	信用卡 (银联、Visa, MasterCard ...)	Citrix (Multi-Tier)	Call Manager (SIP, H.323,SCCP)
中间件 IBM MQ	基础服务 (DNS, Radius, LDAP)	微软应用 (SharePoint, Exchange, SQL)	交易应用 (FIX, OUCH)	网管应用（SNMP、NetFlow)

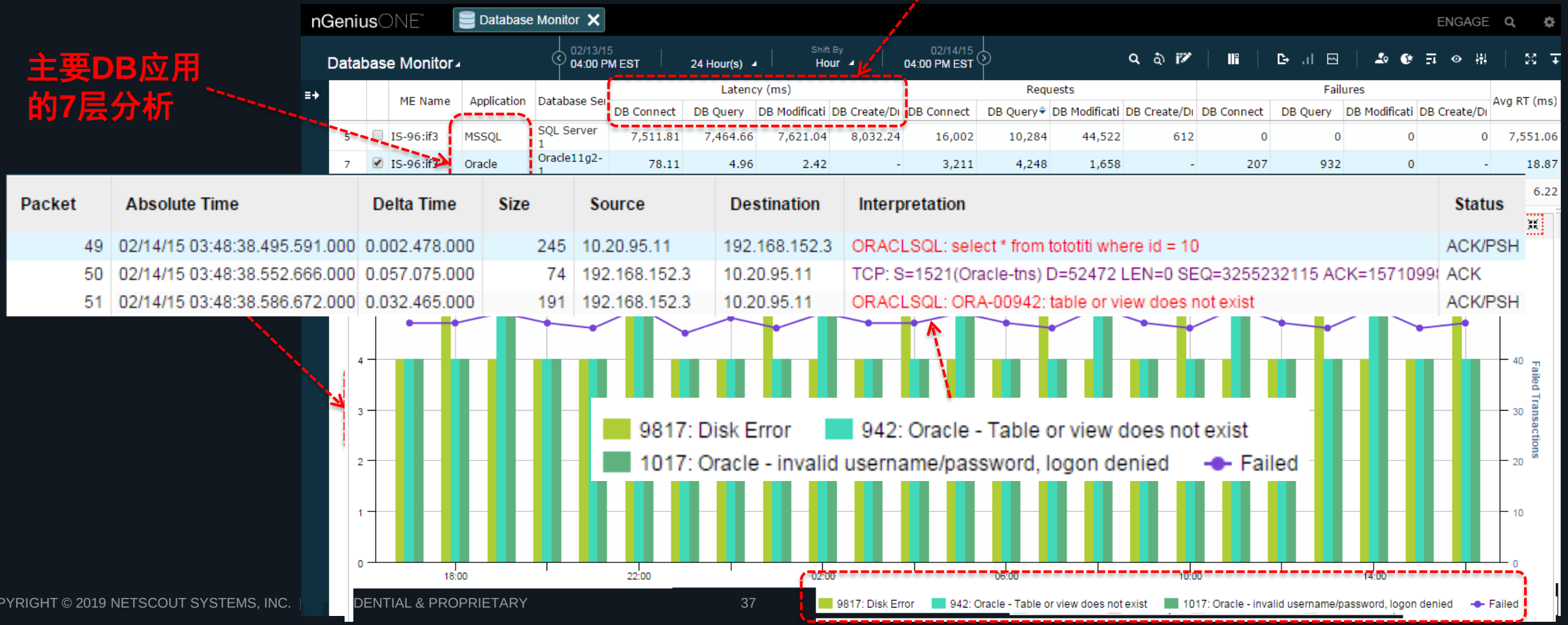
从网络视角透视应用错误：从高层协议维度分析，确定请求失败率（通过应用返回代码进行判断，例如HTTP的400和500的错误代码等）、交易量的变化、交易的超时次数、应用的平均响应时延变化等

DPI举例—数据库监控与分析

实时监控数据库应用，展示数据库性能和错误

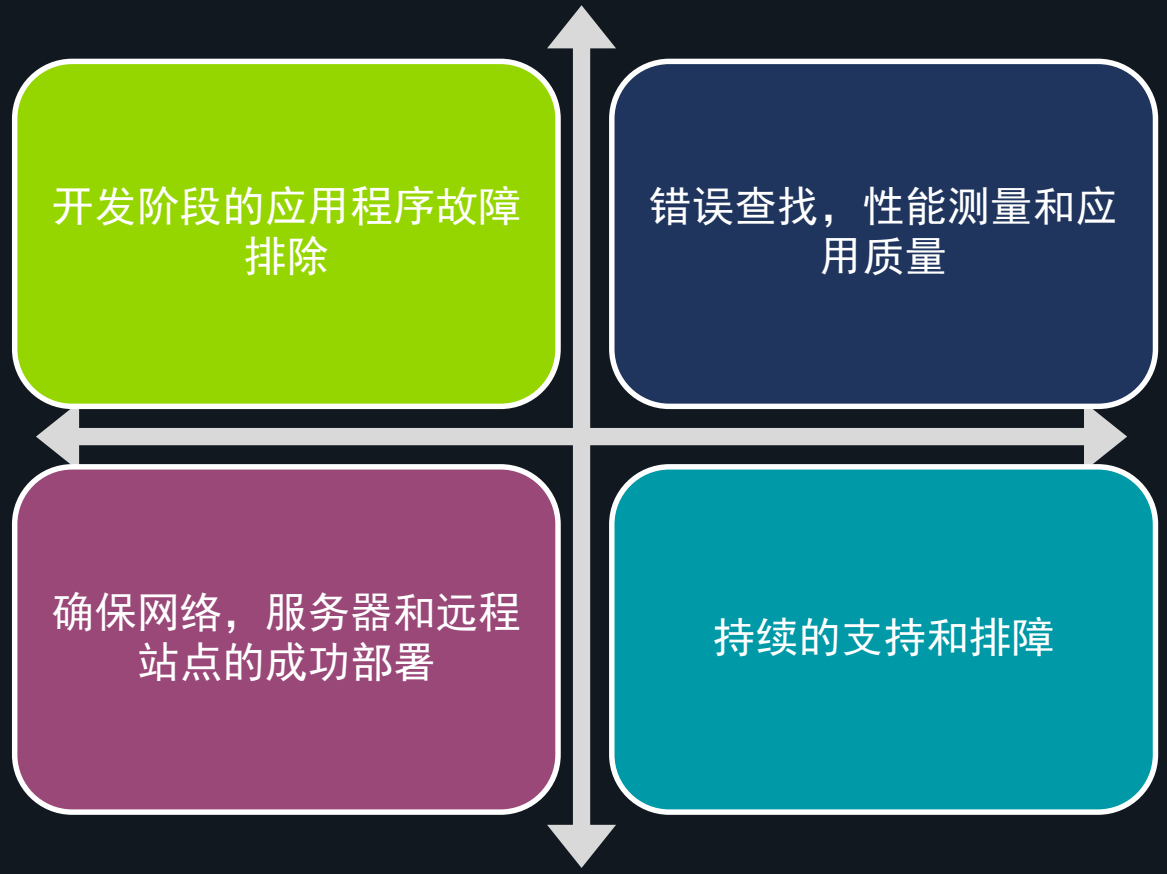
关键交易类型的性能状况

主要DB应用的7层分析



自开发应用的DPI检测—ASI Extender

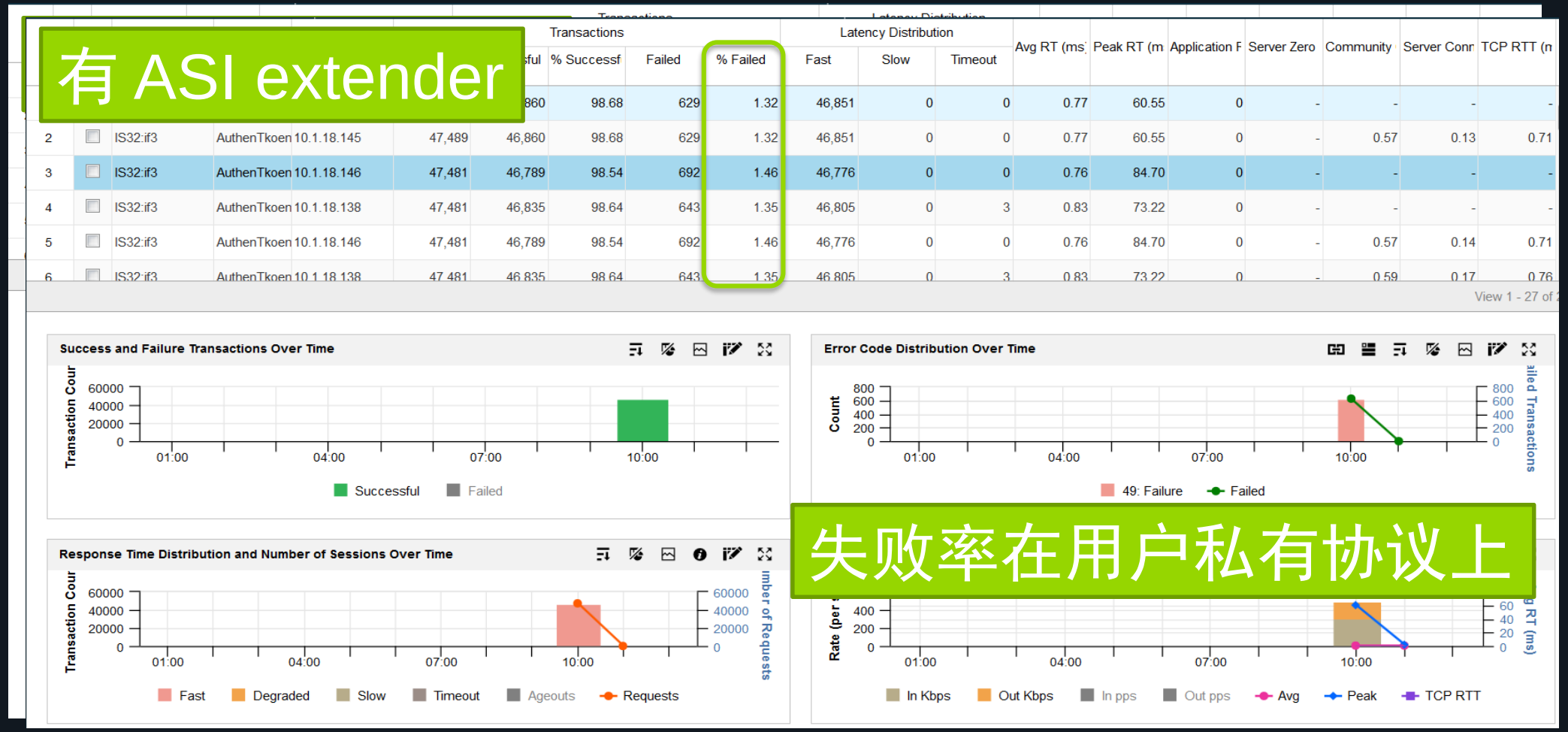
- 针对自开发应用的DPI解码引擎
- 同时支持TCP 和 UDP 应用的业务分析
- 无需额外的设备或License
- 安全 / 竞争优势
- 加快应用上市时间
  - 应用程序开发
  - QA 测试
  - 应用程序推广
- 确保DevOps / NOC的关键服务的可视性



简单、快速、完全可控、全局可视

DPI—应用交易分析

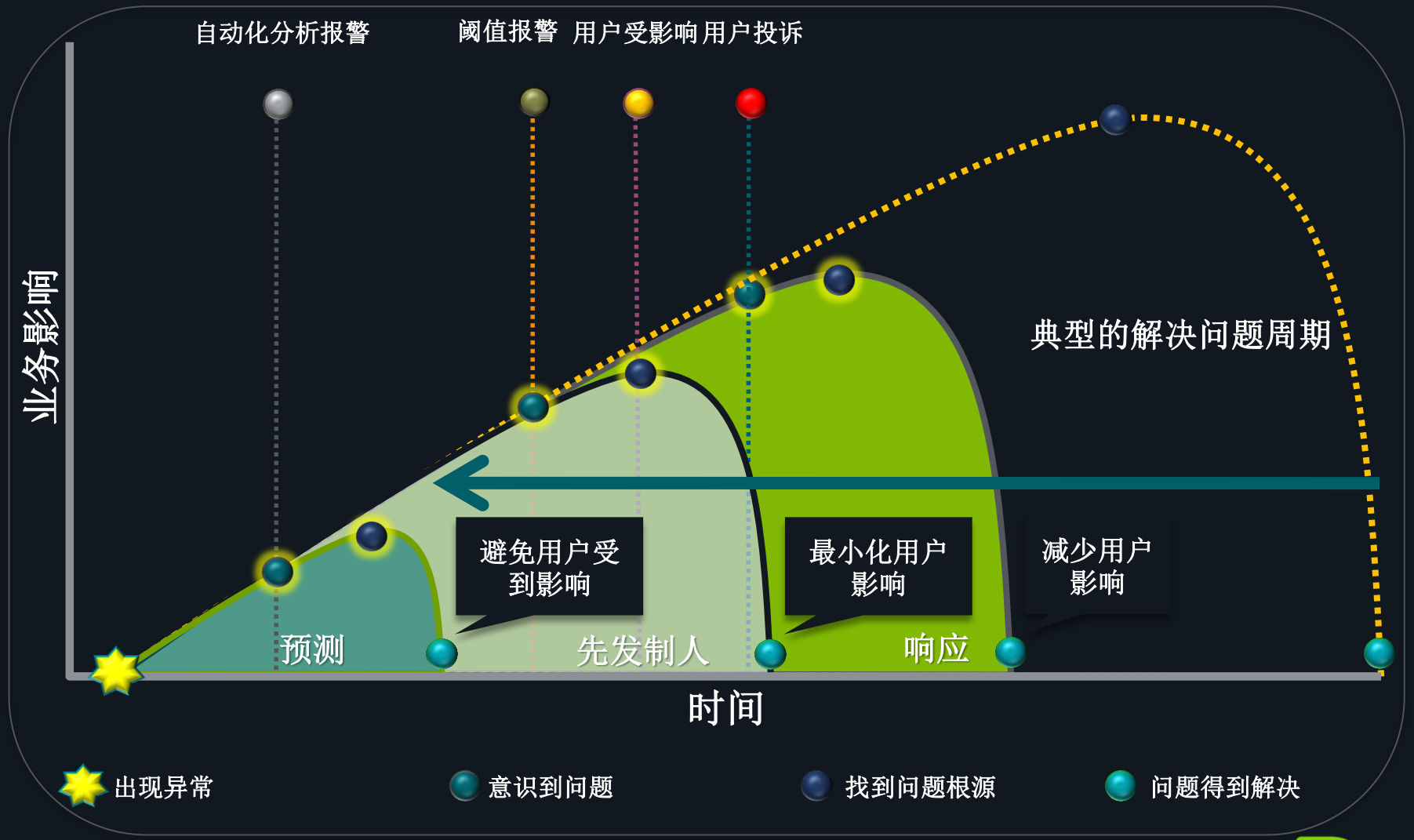
自定义应用深度监控 ASI-Extender



机器学习和智能基线告警

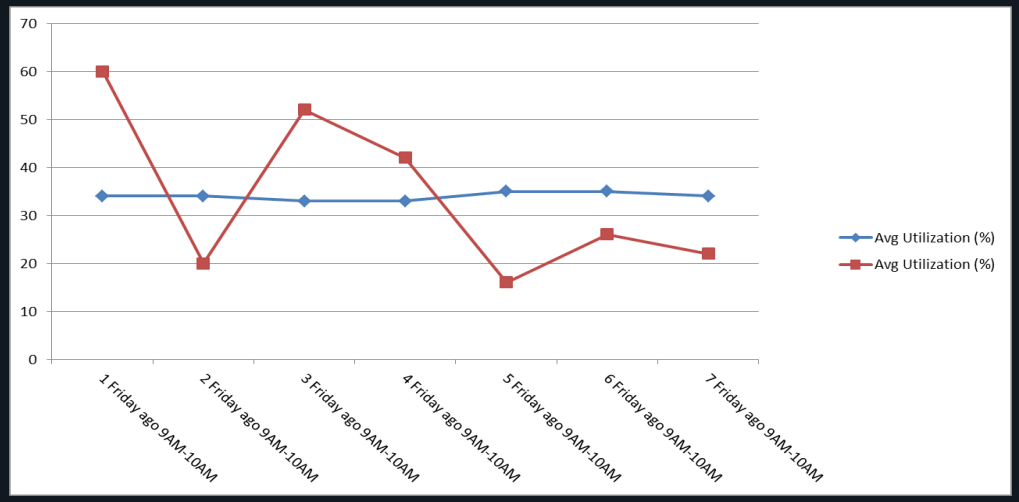
快速发现问题，降低MTTR

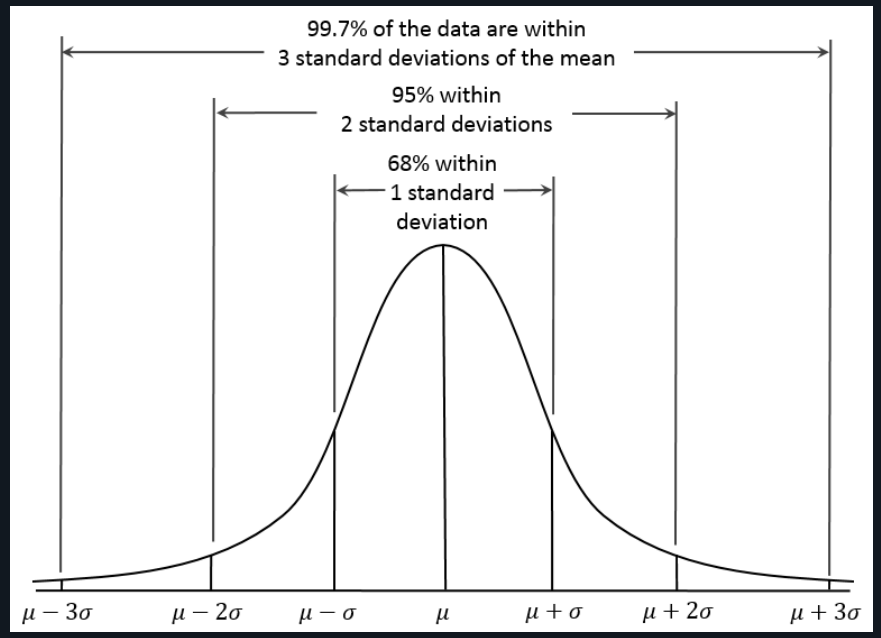
- 提前发现问题，快速定位、提高分析效率
  - ✓ 降低应用的平均修复时间 (MTTR)
- nG1内置Baseline机器学习能力，可以基于历史数据经验匹配当前数据值，对违背基线的行为进行预警，无需传统的故障阀值定义
- 引入标准偏差（Standard Deviation）算法，降低误报和漏报



标准偏差对基线告警的作用示意

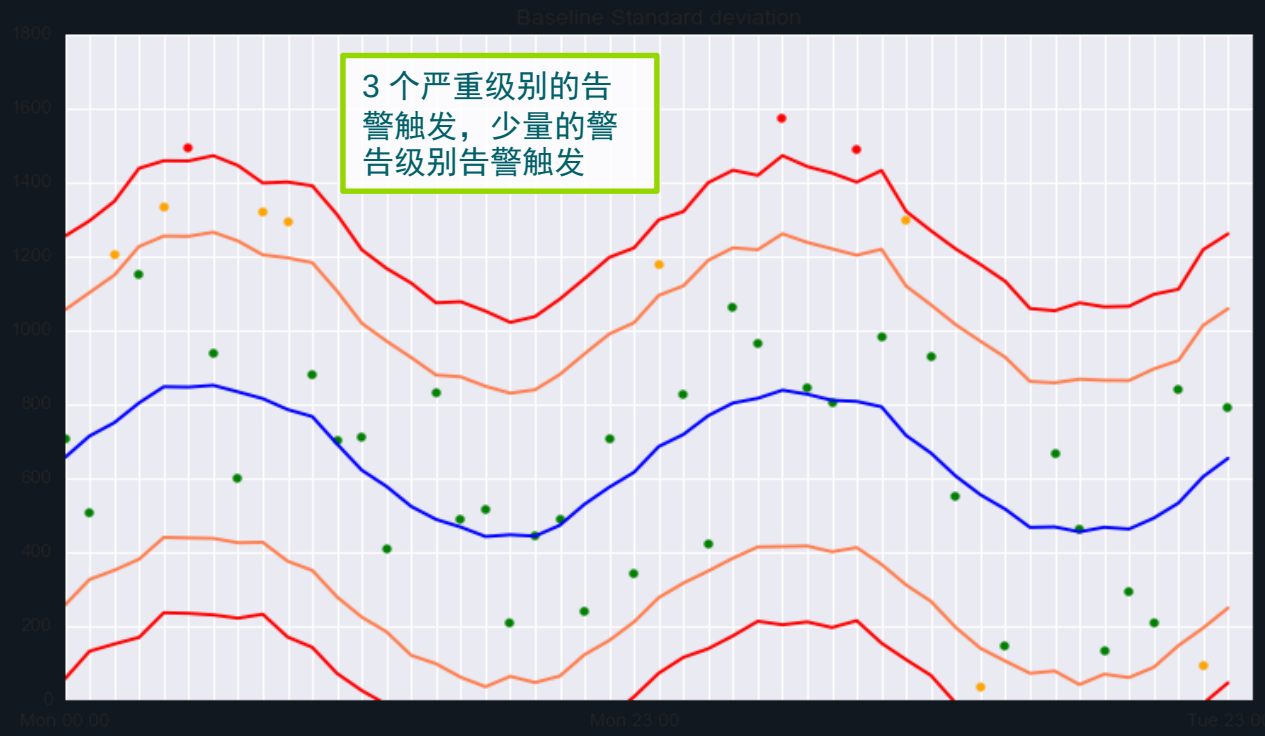
Example		Scenario A	Scenario B
Date	Time	Avg Utilization (%)	Avg Utilization (%)
1 Friday ago	9AM-10AM	34	60
2 Friday ago	9AM-10AM	34	20
3 Friday ago	9AM-10AM	33	52
4 Friday ago	9AM-10AM	33	42
5 Friday ago	9AM-10AM	35	16
6 Friday ago	9AM-10AM	35	26
7 Friday ago	9AM-10AM	34	22
Mean/Average		**34**	**34**
Standard Deviation		**0.8**	**17.3**
Absolute Threshold		**25%**	**25%**
Resulting Trigger Point		**34*1.25 = 42.5%**	**34*1.25 = 42.5%**
1 SD – 68.3%		**34 + 0.8 = 34.8%**	**34 + 17.3 = 51.3%**
2 SD – 95.4%		**34 + 1.6 = 35.6%**	**34 + 34.6 = 68.6%**
3 SD – 99.7%		**34 + 2.4 = 36.4%**	**34 + 51.9 = 85.9%**

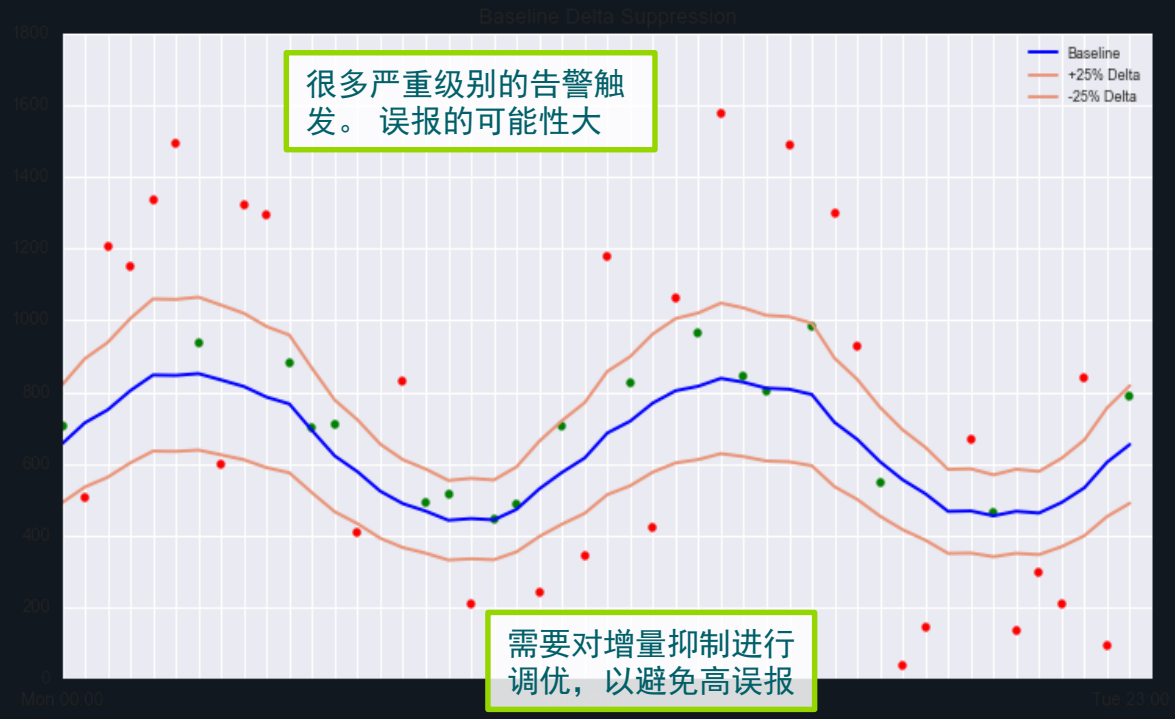




标准偏差 vs 增量抑制

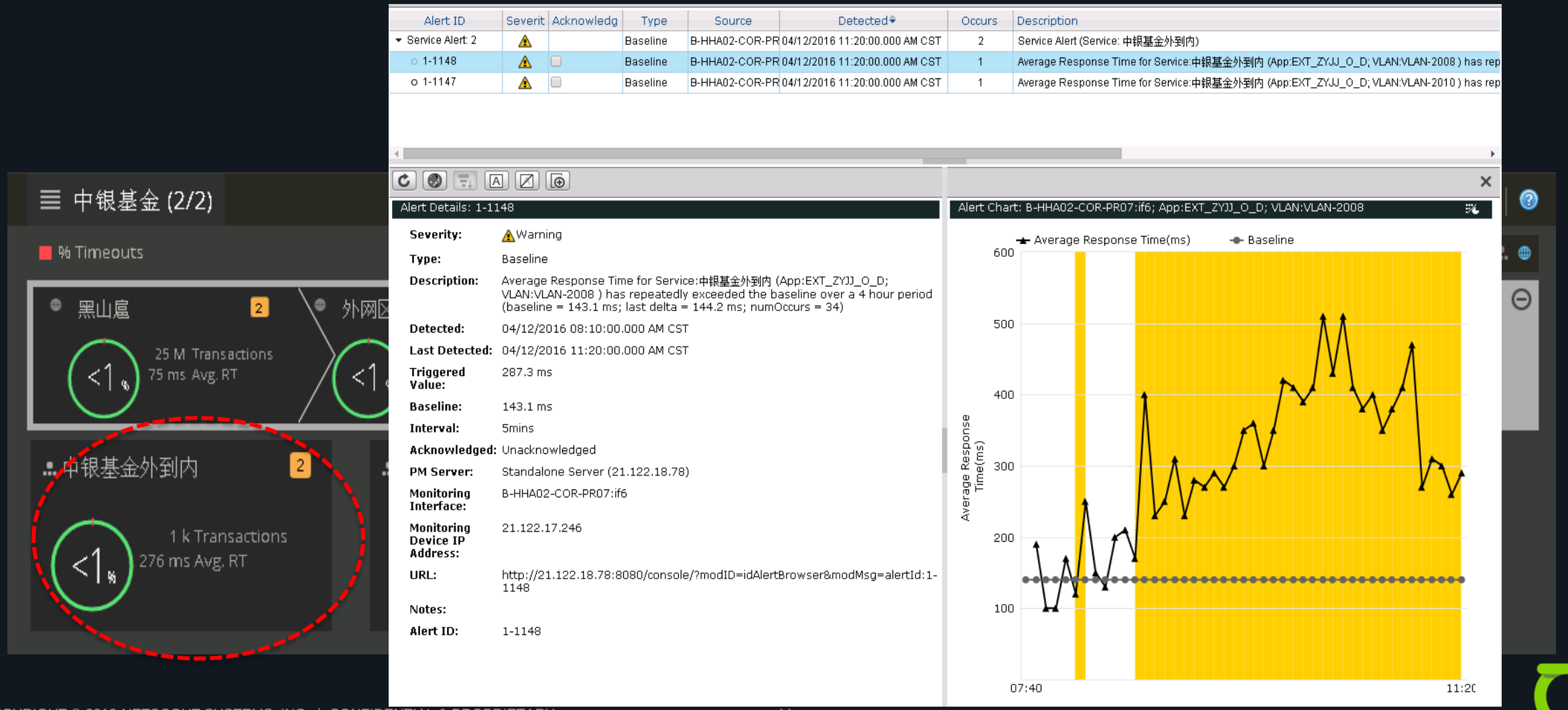
- 相同数据场景下，设置2倍和3倍标准偏差 对比 25%增量抑制的结果





前瞻性监控—智能告警

通过告警信息快速发现问题、圈定问题范围。



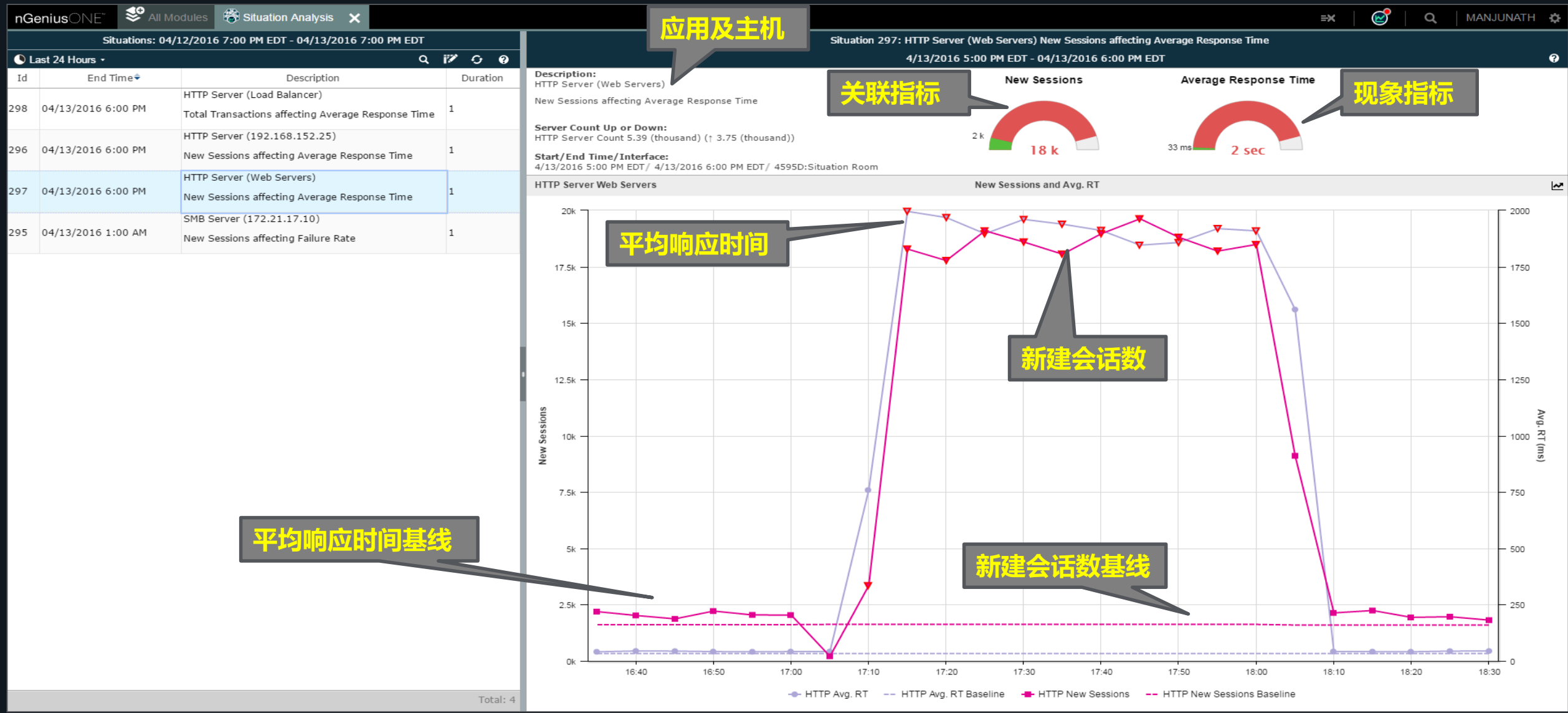
智能情境分析Situation Analysis

机器学习和问题关联分析

45

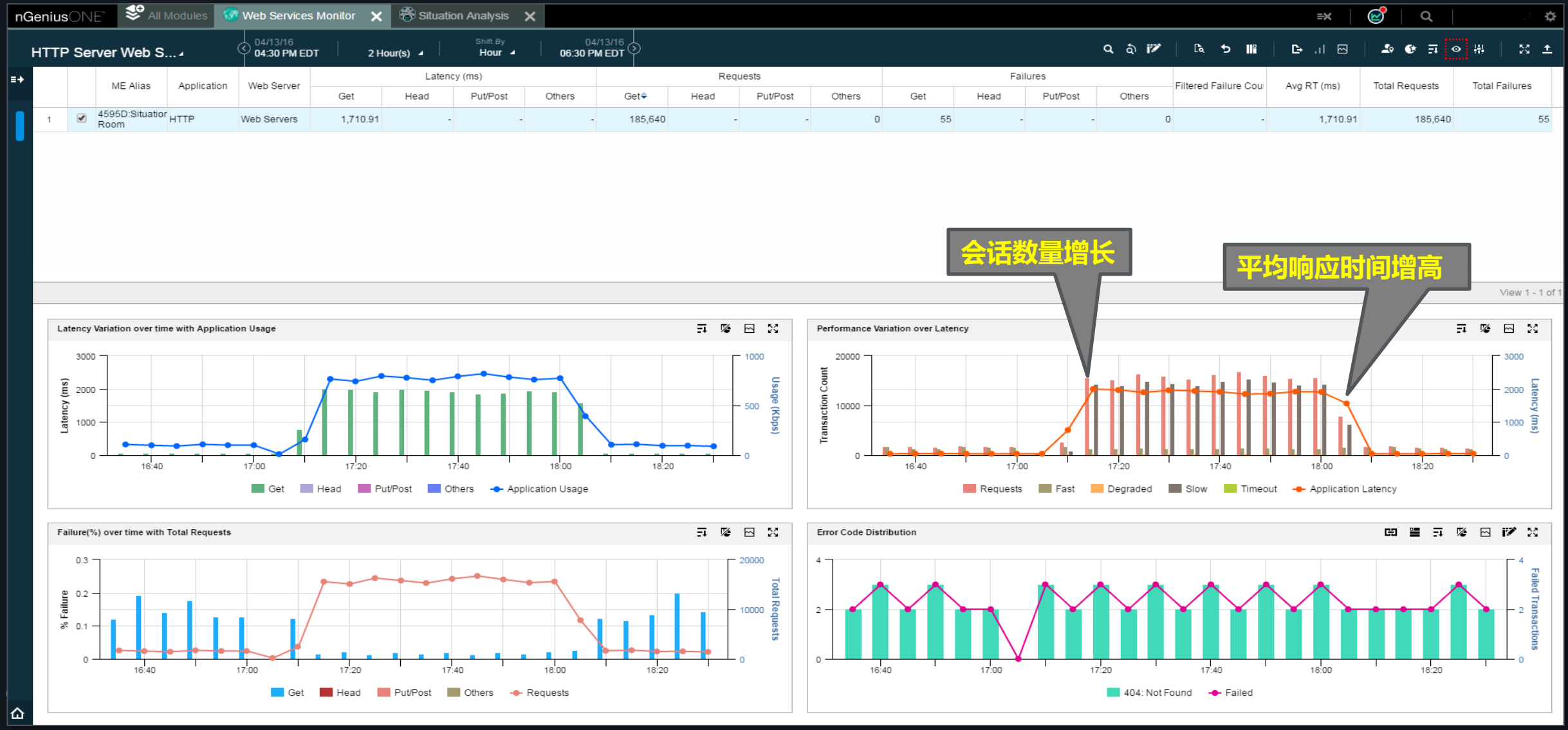
智能情境分析示例

大量的新建会话数→导致延迟增高



智能情境分析示例

分析证据

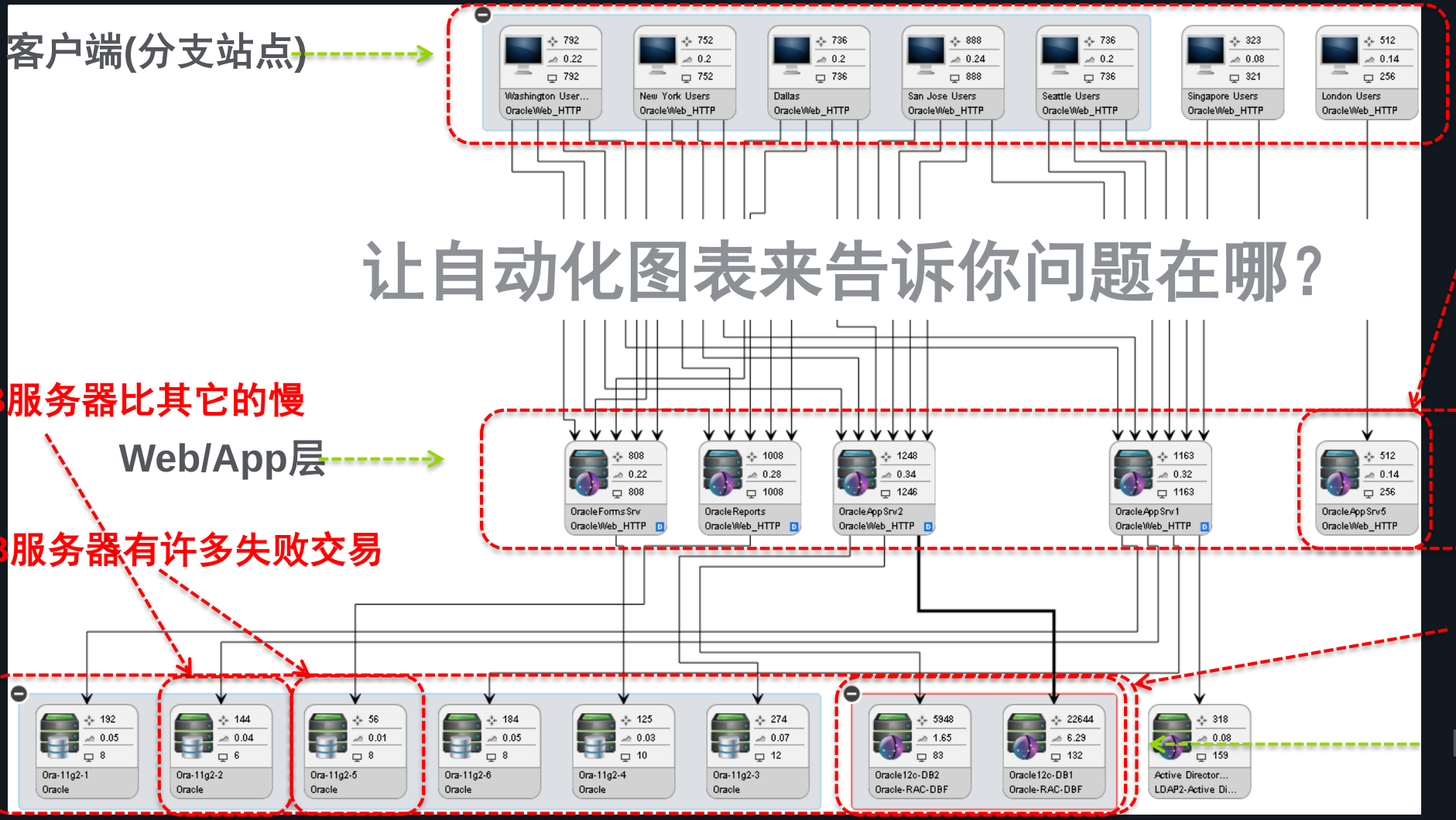


智能情境分析流程

48

自动服务依赖性分析

应用路径自动发现和分析

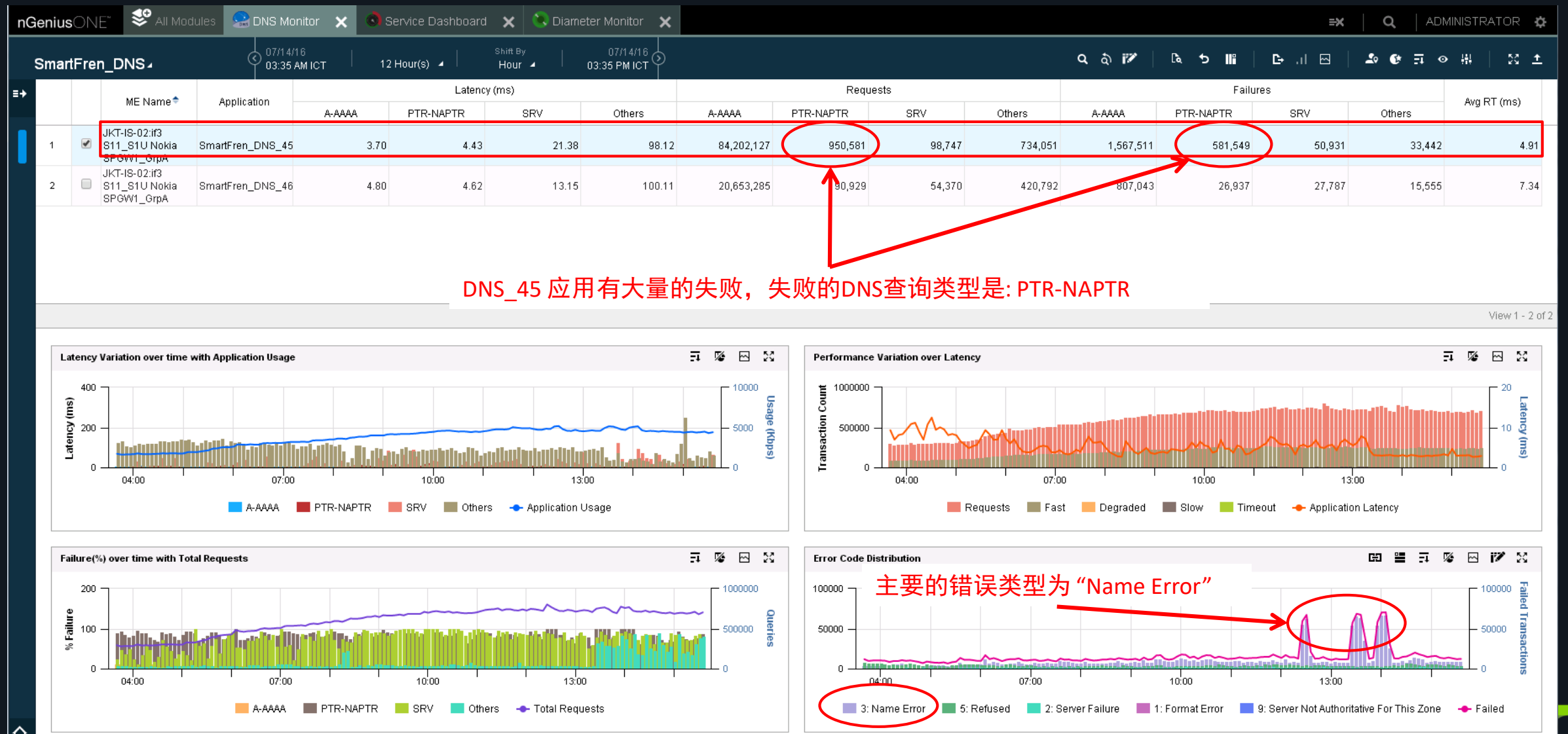


突发流量分析

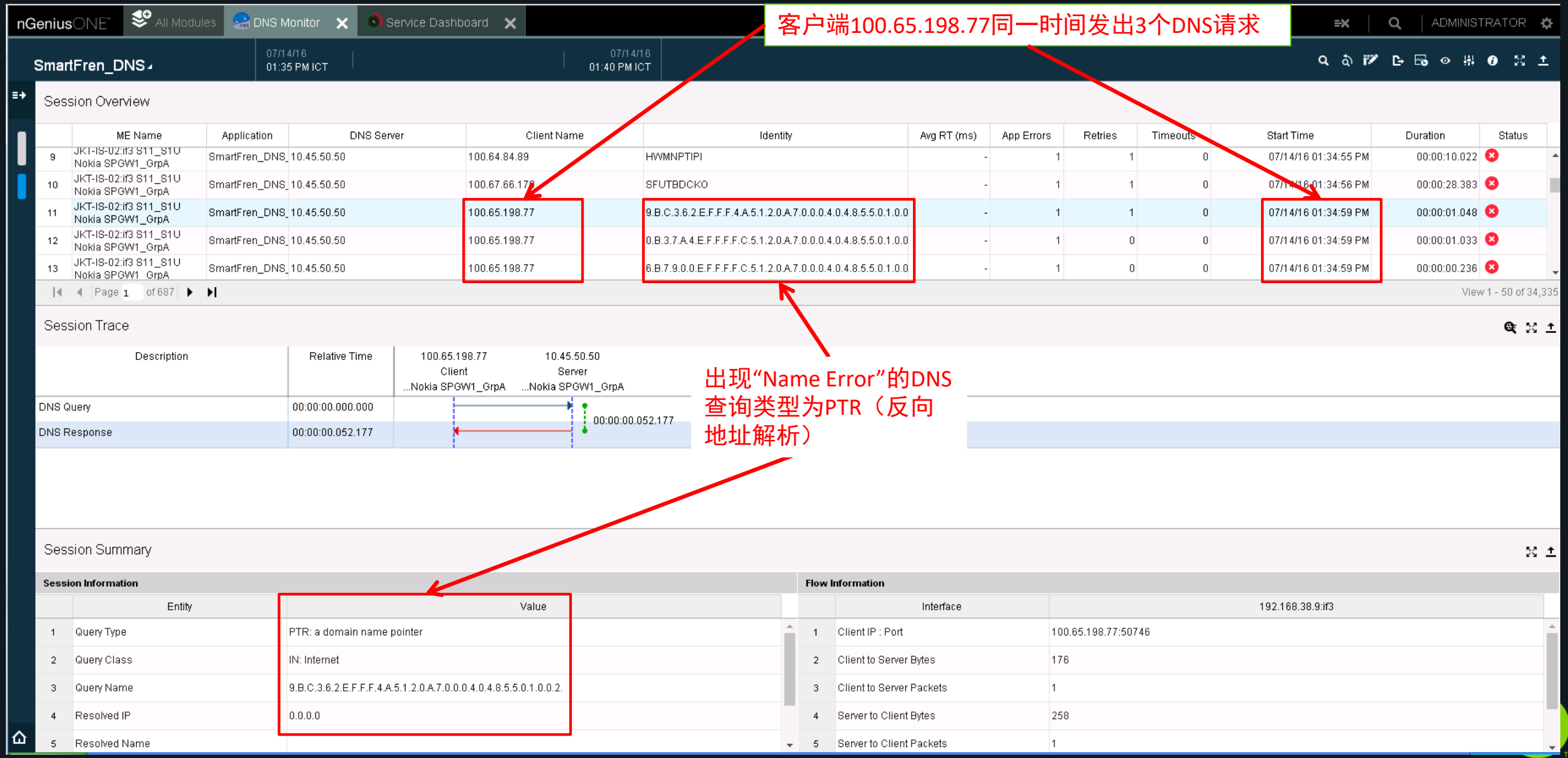
微秒级的精度，揭示突发流量的成因

服务仪表盘—快速发现问题

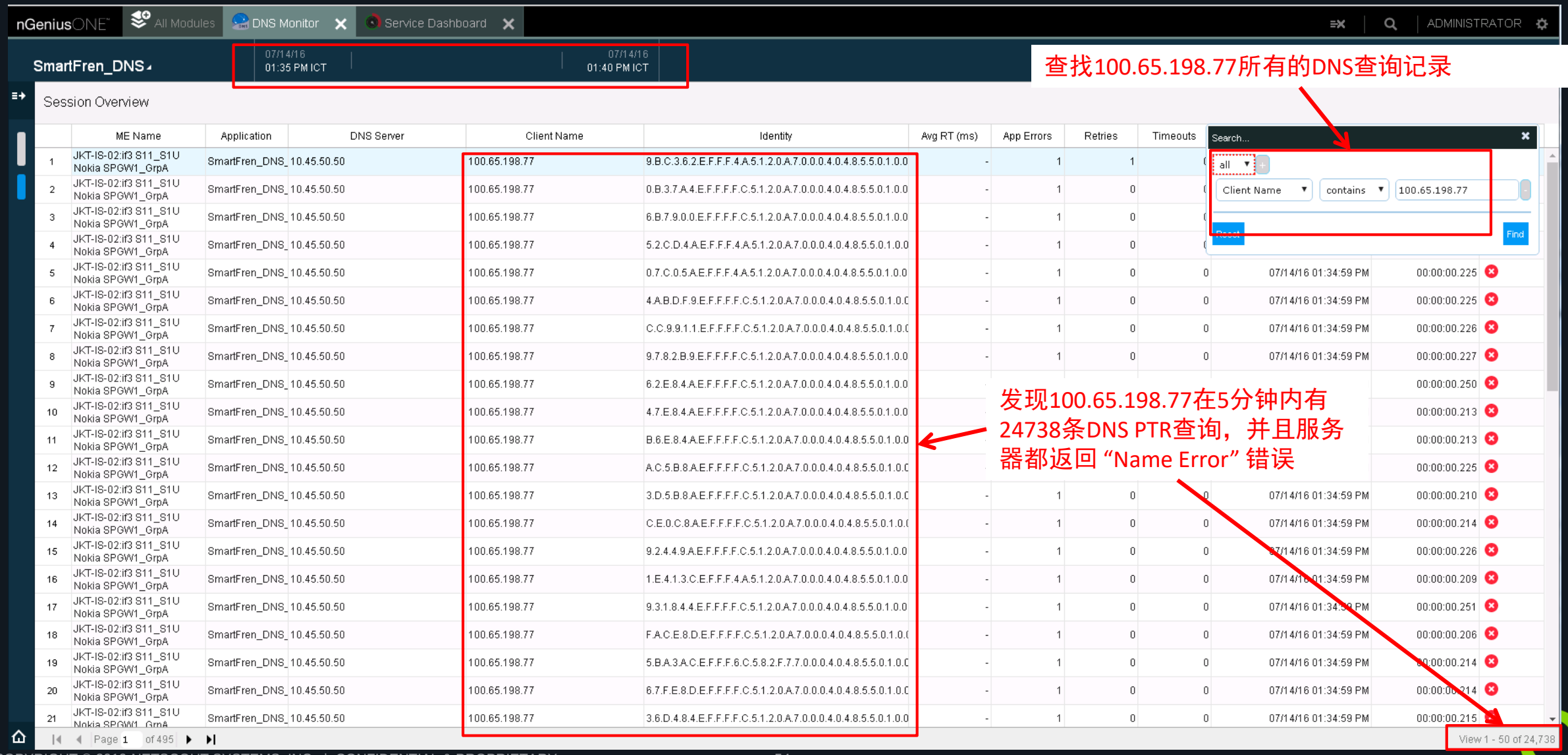
服务监测器—深度分析DNS应用问题



会话分析—查找问题根源


nGeniusONE
All Modules
DNS Monitor
Service Dashboard
ADMINISTRATOR
SmartFren_DNS
07/14/16 01:35 PM ICT
07/14/16 01:40 PM ICT
客户端100.65.198.77同一时间发出3个DNS请求
Session Overview
ME Name | Application | DNS Server | Client Name | Identity | Avg RT (ms) | App Errors | Retries | Timeouts | Start Time | Duration | Status
9 JKT-IS-02:if3 S11_S1U Nokia SPGW1_GrpA SmartFren_DNS 10.45.50.50 100.64.84.89 HWMNPTIPI - 1 1 0 07/14/16 01:34:55 PM 00:00:10.022
10 JKT-IS-02:if3 S11_S1U Nokia SPGW1_GrpA SmartFren_DNS 10.45.50.50 100.67.66.178 SFUTBDCKO - 1 1 0 07/14/16 01:34:56 PM 00:00:28.383
11 JKT-IS-02:if3 S11_S1U Nokia SPGW1_GrpA SmartFren_DNS 10.45.50.50 100.65.198.77 9.B.C.3.6.2.E.F.F.F.4.A.5.1.2.0.A.7.0.0.0.4.0.4.8.5.5.0.1.0.0 - 1 1 0 07/14/16 01:34:59 PM 00:00:01.048
12 JKT-IS-02:if3 S11_S1U Nokia SPGW1_GrpA SmartFren_DNS 10.45.50.50 100.65.198.77 0.B.3.7.A.4.E.F.F.F.F.C.5.1.2.0.A.7.0.0.0.4.0.4.8.5.5.0.1.0.0 - 1 0 0 07/14/16 01:34:59 PM 00:00:01.033
13 JKT-IS-02:if3 S11_S1U Nokia SPGW1_GrpA SmartFren_DNS 10.45.50.50 100.65.198.77 6.B.7.9.0.0.E.F.F.F.F.C.5.1.2.0.A.7.0.0.0.4.0.4.8.5.5.0.1.0.0 - 1 0 0 07/14/16 01:34:59 PM 00:00:00.236
Page 1 of 687
View 1 - 50 of 34,335
Session Trace
Description | Relative Time | 100.65.198.77 Client ...Nokia SPGW1_GrpA | 10.45.50.50 Server ...Nokia SPGW1_GrpA
DNS Query 00:00:00.000.000
DNS Response 00:00:00.052.177
00:00:00.052.177
出现“Name Error”的DNS查询类型为PTR（反向地址解析）
Session Summary
Session Information
Entity | Value
1 Query Type PTR: a domain name pointer
2 Query Class IN: Internet
3 Query Name 9.B.C.3.6.2.E.F.F.F.4.A.5.1.2.0.A.7.0.0.0.4.0.4.8.5.5.0.1.0.0.2.
4 Resolved IP 0.0.0.0
5 Resolved Name
Flow Information
Interface | 192.168.38.9:if3
1 Client IP : Port 100.65.198.77:50746
2 Client to Server Bytes 176
3 Client to Server Packets 1
4 Server to Client Bytes 258
5 Server to Client Packets 1

会话查找—查找问题根源

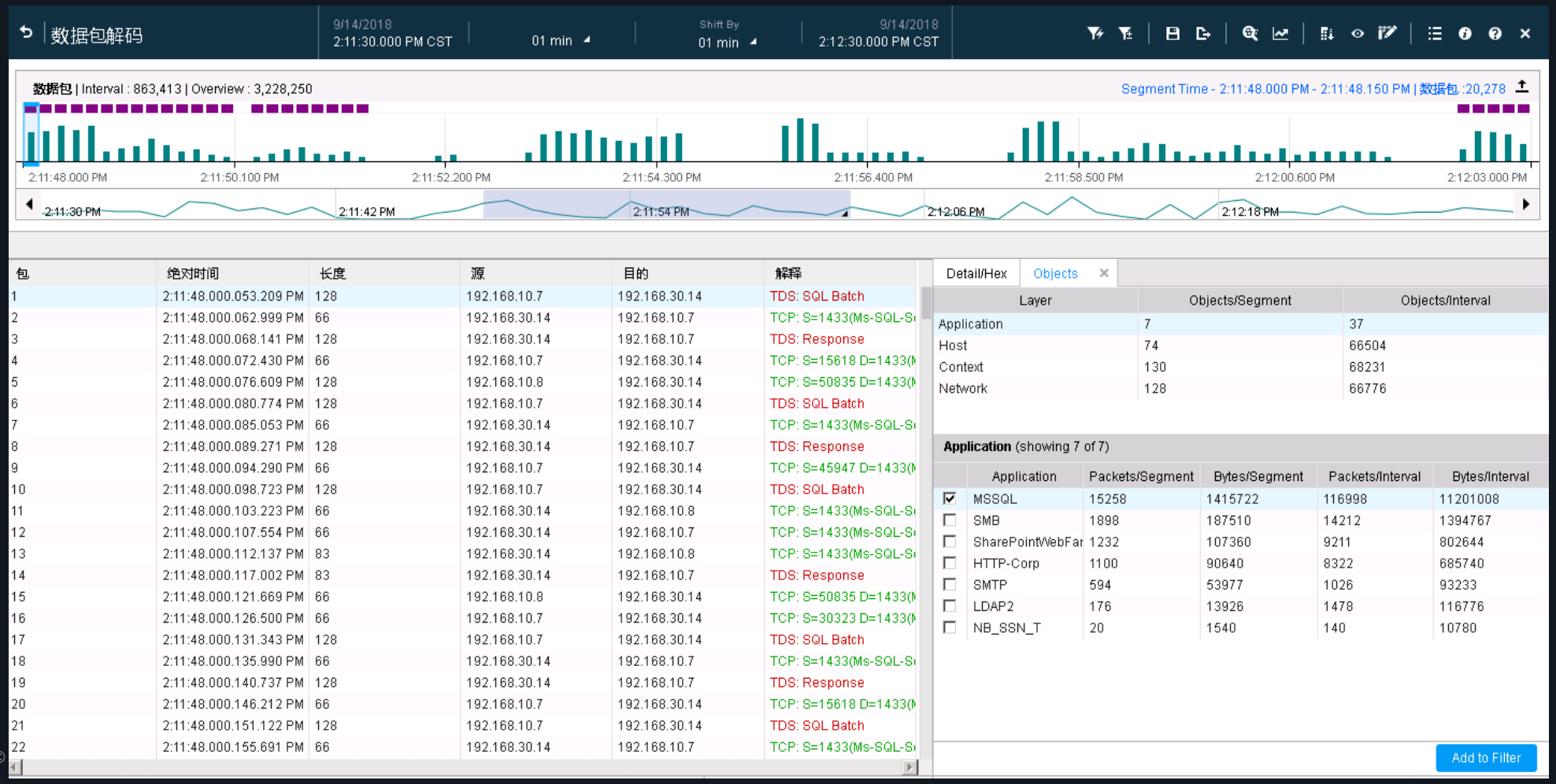


	ME Name	Application	DNS Server	Client Name	Identity	Avg RT (ms)	App Errors	Retries	Timeouts		
1	JKT-IS-02:if3 S11_S1U Nokia SPGW1_GrpA	SmartFren_DNS_	10.45.50.50	100.65.198.77	9.B.C.3.6.2.E.F.F.F.4.A.5.1.2.0.A.7.0.0.0.4.0.4.8.5.5.0.1.0.0	-	1	1			
2	JKT-IS-02:if3 S11_S1U Nokia SPGW1_GrpA	SmartFren_DNS_	10.45.50.50	100.65.198.77	0.B.3.7.A.4.E.F.F.F.F.C.5.1.2.0.A.7.0.0.0.4.0.4.8.5.5.0.1.0.0	-	1	0			
3	JKT-IS-02:if3 S11_S1U Nokia SPGW1_GrpA	SmartFren_DNS_	10.45.50.50	100.65.198.77	6.B.7.9.0.0.E.F.F.F.F.C.5.1.2.0.A.7.0.0.0.4.0.4.8.5.5.0.1.0.0	-	1	0			
4	JKT-IS-02:if3 S11_S1U Nokia SPGW1_GrpA	SmartFren_DNS_	10.45.50.50	100.65.198.77	5.2.C.D.4.A.E.F.F.F.4.A.5.1.2.0.A.7.0.0.0.4.0.4.8.5.5.0.1.0.0	-	1	0			
5	JKT-IS-02:if3 S11_S1U Nokia SPGW1_GrpA	SmartFren_DNS_	10.45.50.50	100.65.198.77	0.7.C.0.5.A.E.F.F.F.4.A.5.1.2.0.A.7.0.0.0.4.0.4.8.5.5.0.1.0.0	-	1	0	0	07/14/16 01:34:59 PM	00:00:00.225
6	JKT-IS-02:if3 S11_S1U Nokia SPGW1_GrpA	SmartFren_DNS_	10.45.50.50	100.65.198.77	4.A.B.D.F.9.E.F.F.F.F.C.5.1.2.0.A.7.0.0.0.4.0.4.8.5.5.0.1.0.0	-	1	0	0	07/14/16 01:34:59 PM	00:00:00.225
7	JKT-IS-02:if3 S11_S1U Nokia SPGW1_GrpA	SmartFren_DNS_	10.45.50.50	100.65.198.77	C.C.9.9.1.1.E.F.F.F.F.C.5.1.2.0.A.7.0.0.0.4.0.4.8.5.5.0.1.0.0	-	1	0	0	07/14/16 01:34:59 PM	00:00:00.226
8	JKT-IS-02:if3 S11_S1U Nokia SPGW1_GrpA	SmartFren_DNS_	10.45.50.50	100.65.198.77	9.7.8.2.B.9.E.F.F.F.F.C.5.1.2.0.A.7.0.0.0.4.0.4.8.5.5.0.1.0.0	-	1	0	0	07/14/16 01:34:59 PM	00:00:00.227
9	JKT-IS-02:if3 S11_S1U Nokia SPGW1_GrpA	SmartFren_DNS_	10.45.50.50	100.65.198.77	6.2.E.8.4.A.E.F.F.F.F.C.5.1.2.0.A.7.0.0.0.4.0.4.8.5.5.0.1.0.0						00:00:00.250
10	JKT-IS-02:if3 S11_S1U Nokia SPGW1_GrpA	SmartFren_DNS_	10.45.50.50	100.65.198.77	4.7.E.8.4.A.E.F.F.F.F.C.5.1.2.0.A.7.0.0.0.4.0.4.8.5.5.0.1.0.0						00:00:00.213
11	JKT-IS-02:if3 S11_S1U Nokia SPGW1_GrpA	SmartFren_DNS_	10.45.50.50	100.65.198.77	B.6.E.8.4.A.E.F.F.F.F.C.5.1.2.0.A.7.0.0.0.4.0.4.8.5.5.0.1.0.0						00:00:00.213
12	JKT-IS-02:if3 S11_S1U Nokia SPGW1_GrpA	SmartFren_DNS_	10.45.50.50	100.65.198.77	A.C.5.B.8.A.E.F.F.F.F.C.5.1.2.0.A.7.0.0.0.4.0.4.8.5.5.0.1.0.0						00:00:00.225
13	JKT-IS-02:if3 S11_S1U Nokia SPGW1_GrpA	SmartFren_DNS_	10.45.50.50	100.65.198.77	3.D.5.B.8.A.E.F.F.F.F.C.5.1.2.0.A.7.0.0.0.4.0.4.8.5.5.0.1.0.0	-	1	0	0	07/14/16 01:34:59 PM	00:00:00.210
14	JKT-IS-02:if3 S11_S1U Nokia SPGW1_GrpA	SmartFren_DNS_	10.45.50.50	100.65.198.77	C.E.0.C.8.A.E.F.F.F.F.C.5.1.2.0.A.7.0.0.0.4.0.4.8.5.5.0.1.0.0	-	1	0	0	07/14/16 01:34:59 PM	00:00:00.214
15	JKT-IS-02:if3 S11_S1U Nokia SPGW1_GrpA	SmartFren_DNS_	10.45.50.50	100.65.198.77	9.2.4.4.9.A.E.F.F.F.F.C.5.1.2.0.A.7.0.0.0.4.0.4.8.5.5.0.1.0.0	-	1	0	0	07/14/16 01:34:59 PM	00:00:00.226
16	JKT-IS-02:if3 S11_S1U Nokia SPGW1_GrpA	SmartFren_DNS_	10.45.50.50	100.65.198.77	1.E.4.1.3.C.E.F.F.F.4.A.5.1.2.0.A.7.0.0.0.4.0.4.8.5.5.0.1.0.0	-	1	0	0	07/14/16 01:34:59 PM	00:00:00.209
17	JKT-IS-02:if3 S11_S1U Nokia SPGW1_GrpA	SmartFren_DNS_	10.45.50.50	100.65.198.77	9.3.1.8.4.4.E.F.F.F.F.C.5.1.2.0.A.7.0.0.0.4.0.4.8.5.5.0.1.0.0	-	1	0	0	07/14/16 01:34:59 PM	00:00:00.251
18	JKT-IS-02:if3 S11_S1U Nokia SPGW1_GrpA	SmartFren_DNS_	10.45.50.50	100.65.198.77	F.A.C.E.8.D.E.F.F.F.F.C.5.1.2.0.A.7.0.0.0.4.0.4.8.5.5.0.1.0.0	-	1	0	0	07/14/16 01:34:59 PM	00:00:00.206
19	JKT-IS-02:if3 S11_S1U Nokia SPGW1_GrpA	SmartFren_DNS_	10.45.50.50	100.65.198.77	5.B.A.3.A.C.E.F.F.F.6.C.5.8.2.F.7.7.0.0.0.4.0.4.8.5.5.0.1.0.0	-	1	0	0	07/14/16 01:34:59 PM	00:00:00.214
20	JKT-IS-02:if3 S11_S1U Nokia SPGW1_GrpA	SmartFren_DNS_	10.45.50.50	100.65.198.77	6.7.F.E.8.D.E.F.F.F.F.C.5.1.2.0.A.7.0.0.0.4.0.4.8.5.5.0.1.0.0	-	1	0	0	07/14/16 01:34:59 PM	00:00:00.214
21	JKT-IS-02:if3 S11_S1U Nokia SPGW1_GrpA	SmartFren_DNS_	10.45.50.50	100.65.198.77	3.6.D.4.8.4.E.F.F.F.F.C.5.1.2.0.A.7.0.0.0.4.0.4.8.5.5.0.1.0.0	-	1	0	0	07/14/16 01:34:59 PM	00:00:00.215

在线图形化解码视图

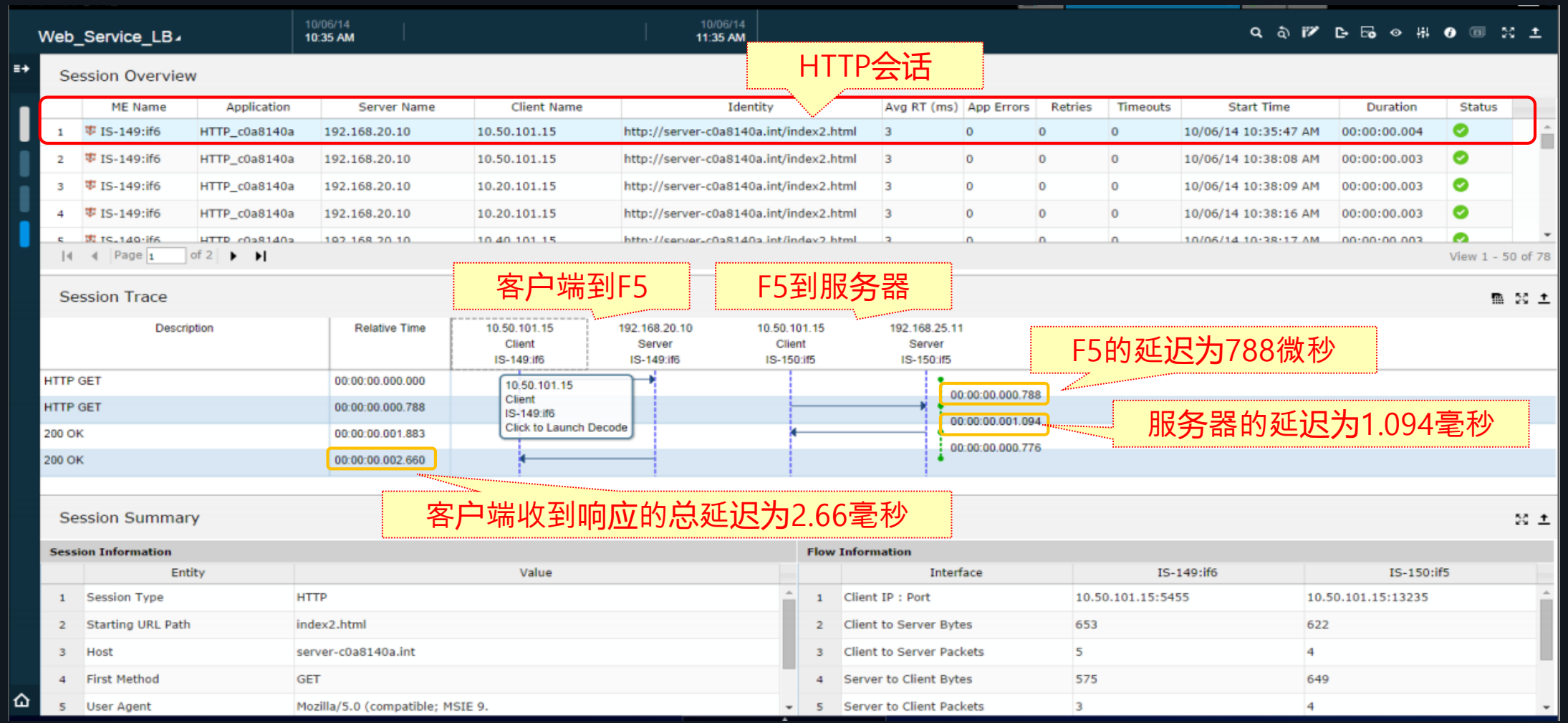
无需下载数据包，快速解码，图形化呈现

- 提供Sniffer专家分析视图，使用基于时间的选择器、包分类描绘器或过滤器来查找感兴趣的数据包



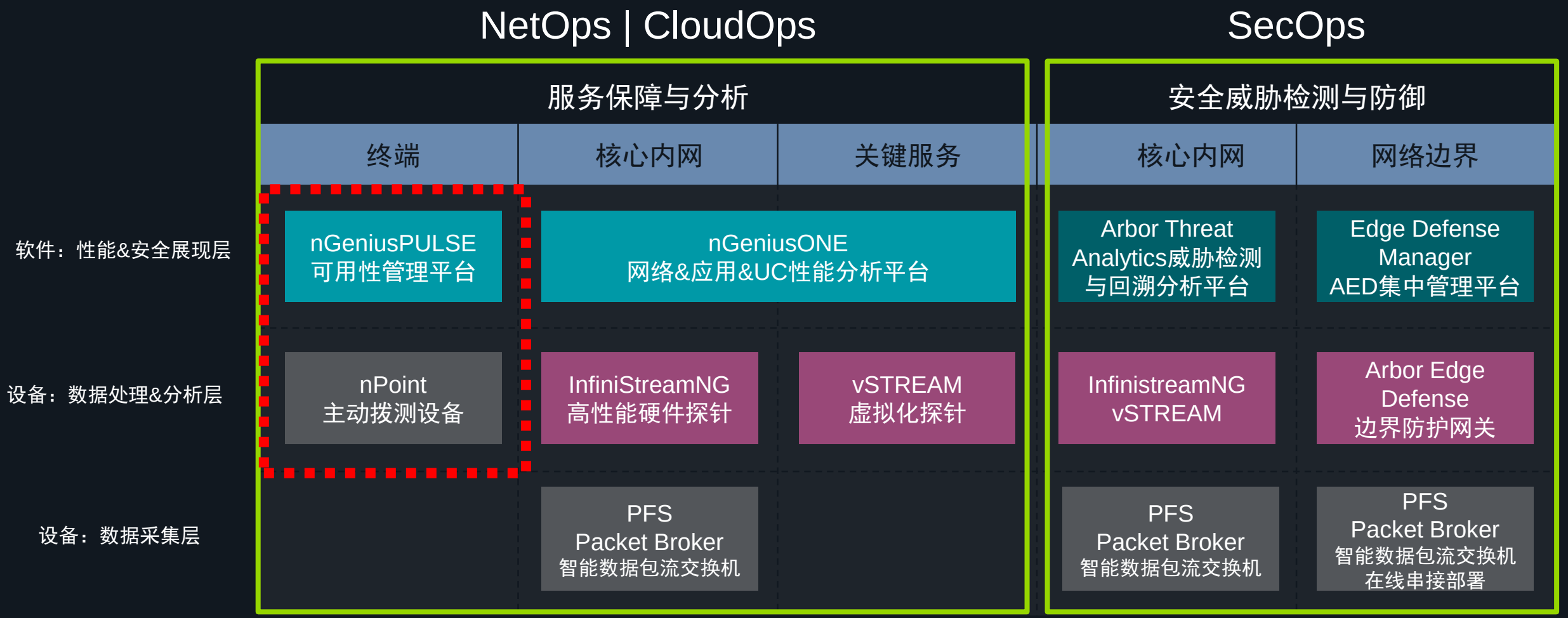
多网段智能关联分析

自动关联分析多段数据



nGeniusPULSE可用性监测解决方案

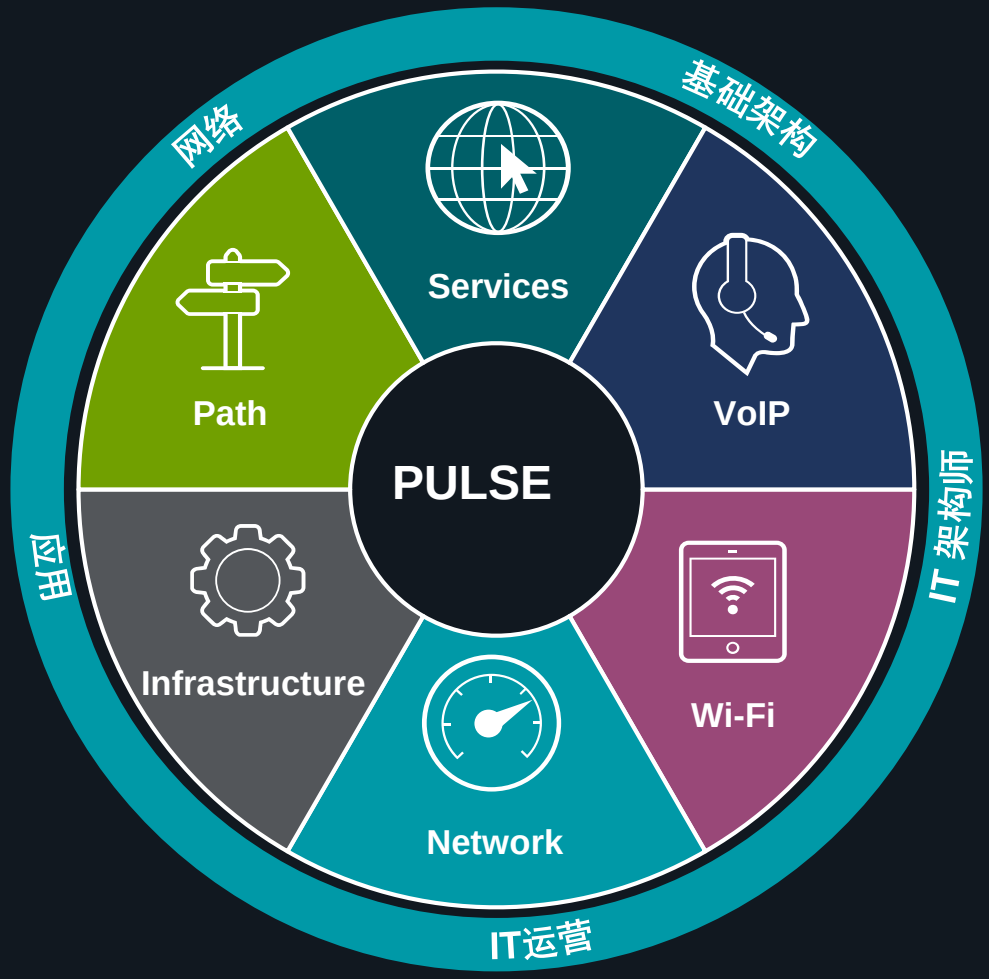
云、数据中心网络、VoIP服务可用性和健康性



可用性监测—nGeniusPULSE

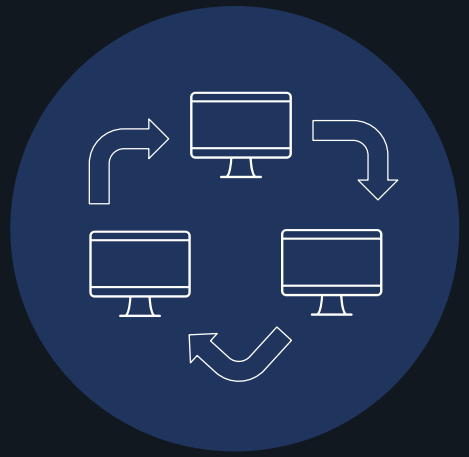
从远程可视化当今复杂的业务生态系统

- **商业收益**
  - 管理云/ SaaS应用程序的用户体验
  - 界定自有的资产和多个服务提供者之间的问题
  - 将服务交付与关键基础设施关联起来
- **特点**
  - 积极主动，始终在线和自动化
  - 适用于云、混合和虚拟环境



可用性监测—nGeniusPULSE

SaaS
服务主动监测



云、网络、VoIP服务可用性

网络
基础架构监测

网络设备可用性和健康性

服务器
基础架构监测

服务器可用性和健康性

主动拨测

基础架构性能数据采集（SNMP、Syslog、WinRM）

nPULSE功能和组件

服务器健康性	• Windows和 Linux服务器的可用性和健康性监测 • 系统运行时间，CPU，内存，磁盘利用率，磁盘I/O，网络 I/O
网络设备健康性	• 路由器和交换机的可用性和健康性监测 • 运行时间，CPU，内存，接口状态和利用率 • 无线和网络通路分析
综合性测试	• SaaS应用可用性（从外部或分支机构角度） • 主动性测试：HTTP, VoIP, Ping, TCP端口连接, Traceroute, 自定义脚本
Syslog故障排查	• 从服务器和设备收集Syslog数据 • 利用轮询到的指标和主动性测试的数据，进行事件和错误关联

nGeniusPULSE 服务器

集中的收集和报告

- SNMP
- WinRM
- Syslog
- nPoint

nGeniusPULSE nPoint

执行主动性服务测试

- Web
- VOIP
- 数据中心
- 云服务
- 网络健康性
- Wireless
- 网络路径发现

产品架构

PULSE服务器和Collector

- 仪表盘，报告，告警
- 内置Virtual PULSE Collector
- 硬件设备或虚拟化软件

PULSE nPoint

- 主动拨测设备
- 应用、网络、VoIP、自定义测试
- 硬件设备或虚拟化软件

nPLUSE的特点

设备状态的自动巡检

7x24不间断地对IDC中的业务进行综合测试

实时告警

- SLA报告
- 仪表盘直观显示测试结果
- 测试报告

识别问题域

- 主动测试
- 识别问题发生区域。客户端侧网络，广域网/互联网，应用问题，数据传输问题

便捷部署

- 支持硬件 或软件方式部署
- 支持云端服务器或本地服务器

灵活扩展

- 支持通过脚本扩展测试功能
- 支持Restful API

对业务系统、语音服务主动探测的SLA监控解决方案

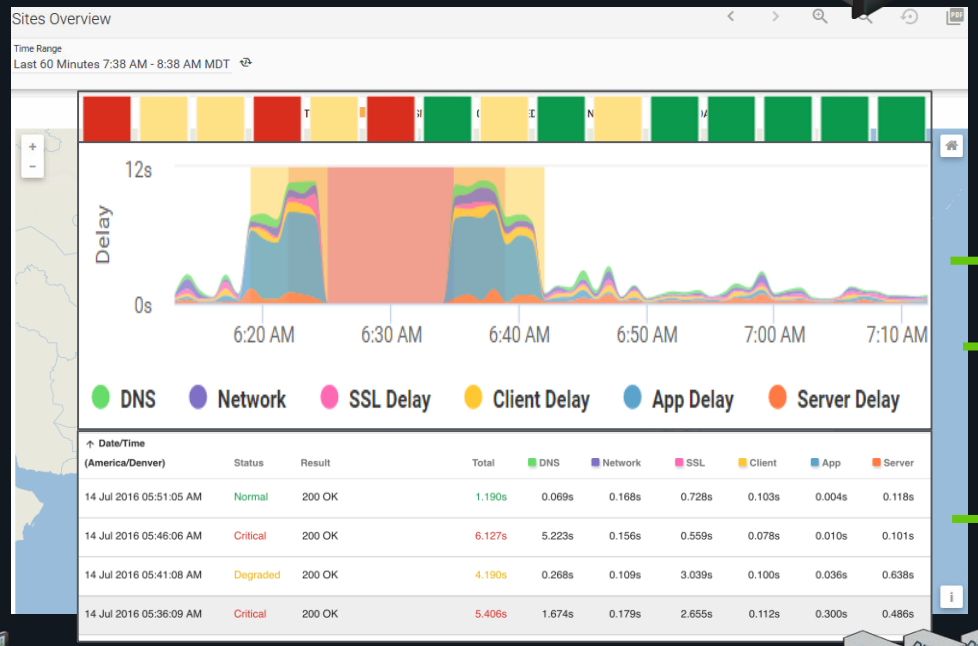
nPULSE工作示意

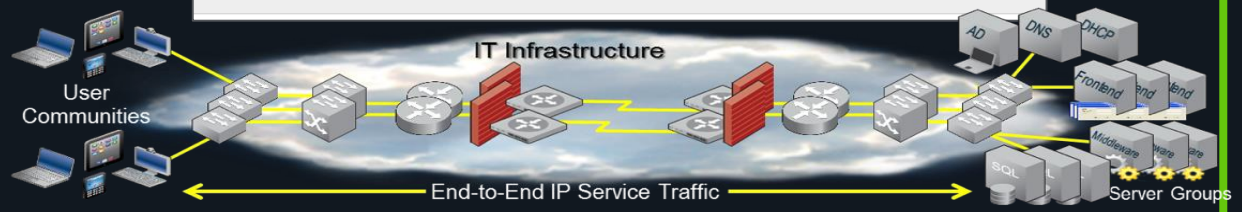
主动拨测，增强用户体验感知

nPULSE服务器

nPoint
硬件或软件

分支或任意站点





公有云

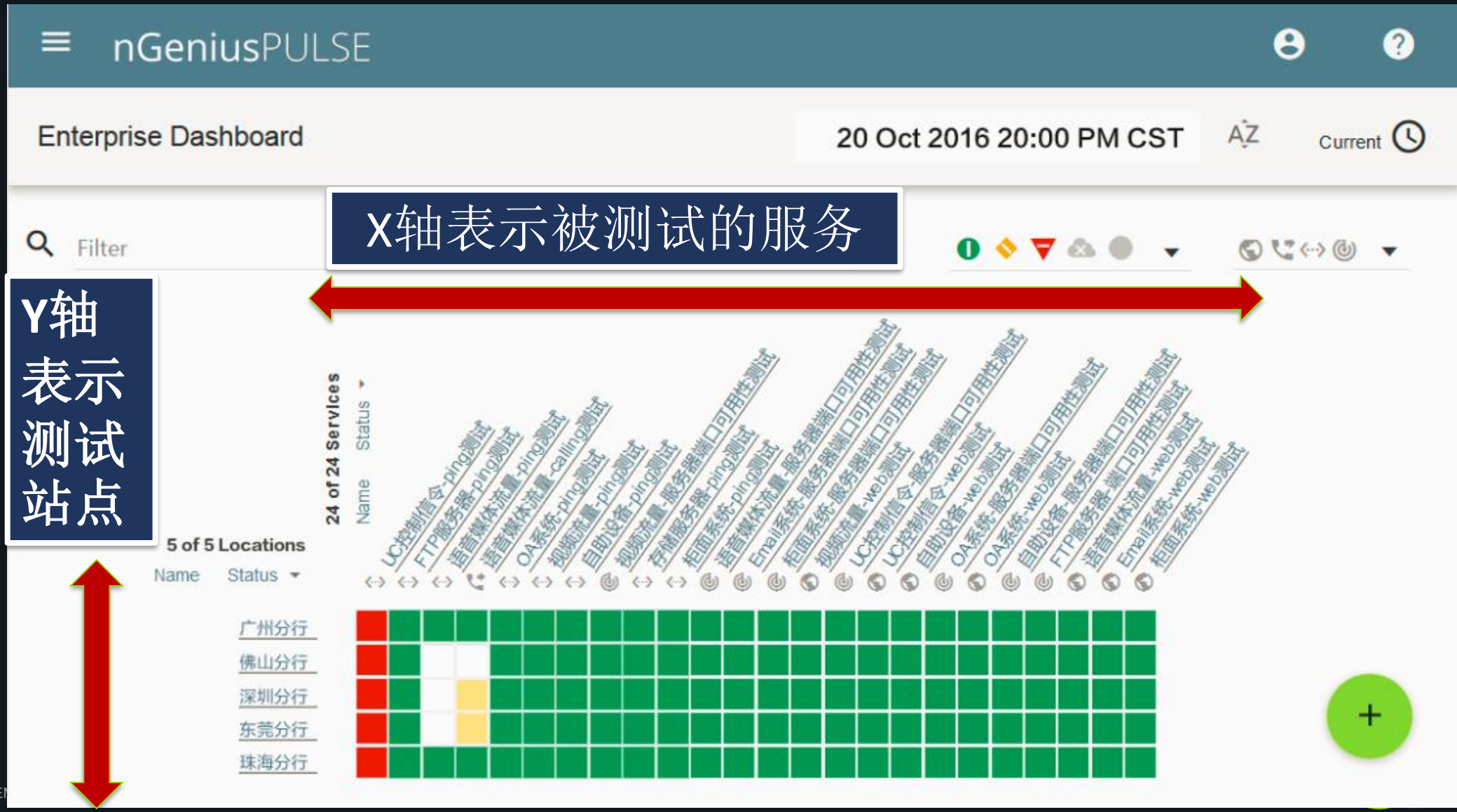
SaaS 应用

传统数据中心/
私有云

- 部署---将nPoint部署在任意位置 (网口, 服务器柜, 台式机, 笔记本或者服务器)
- 测试---从Pulse服务器下载并运行配置的云应用或自定义测试指标的测试
- 跟踪---持续不间断的跟踪从每个位置到每个服务的可用性和性能
- 告警---当服务/云应用访问性能下降时进行告警

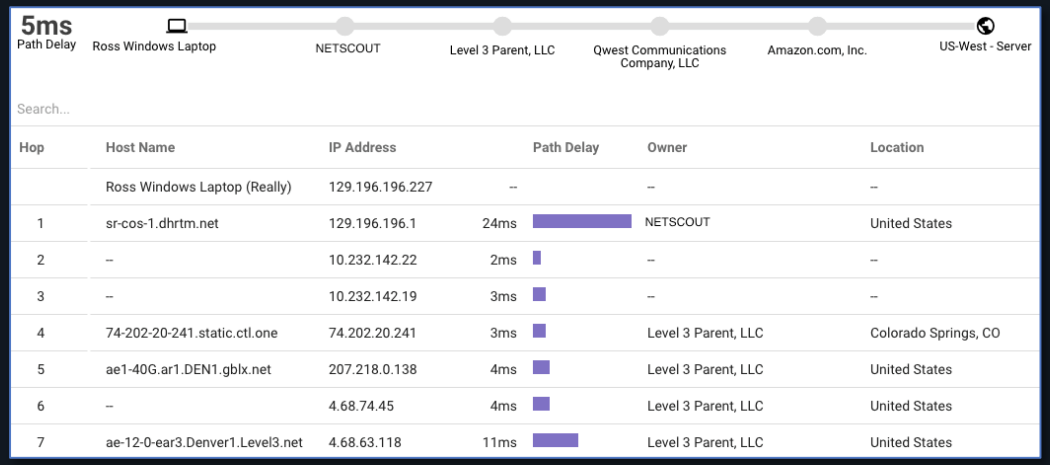
从站点到服务的端到端测试

SLA仪表板

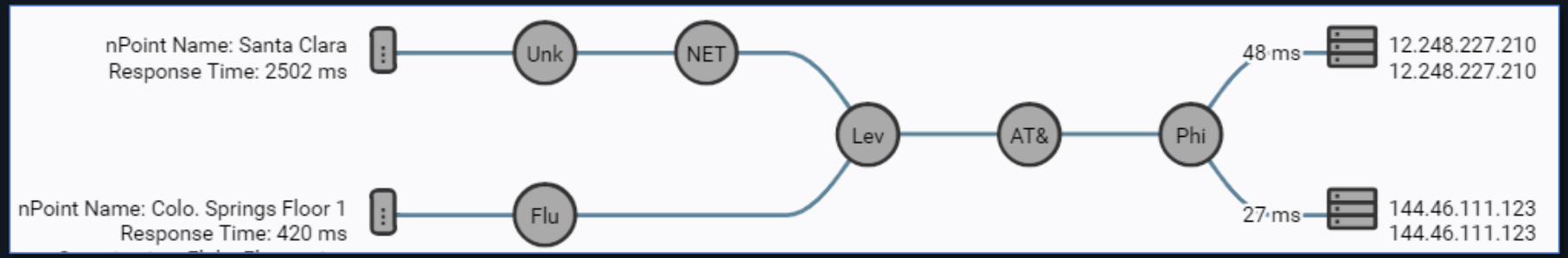


路径监测（Path Monitoring）

- 从站点到服务的连续路径发现
- 排除由于路径路由和延迟问题导致的服务退化
- 界定问题到服务提供商、网络、位置节点或配置



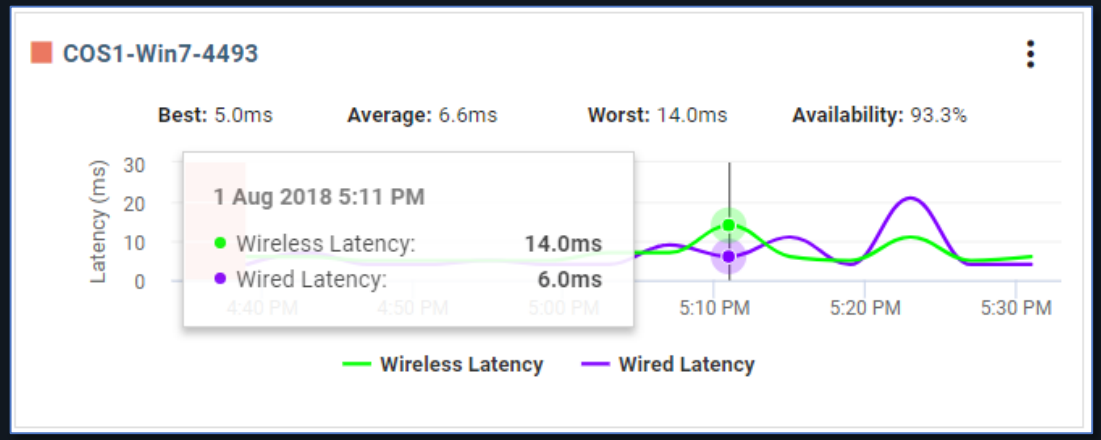
Hop	Host Name	IP Address		Path Delay	Owner	Location
	Ross Windows Laptop (Really)	129.196.196.227	--		--	--
1	sr-cos-1.dhrtm.net	129.196.196.1	24ms		NETSCOUT	United States
2	--	10.232.142.22	2ms		--	--
3	--	10.232.142.19	3ms		--	--
4	74-202-20-241.static.ctl.one	74.202.20.241	3ms		Level 3 Parent, LLC	Colorado Springs, CO
5	ae1-40G.ar1.DEN1.gblx.net	207.218.0.138	4ms		Level 3 Parent, LLC	United States
6	--	4.68.74.45	4ms		Level 3 Parent, LLC	United States
7	ae-12-0-ear3.Denver1.Level3.net	4.68.63.118	11ms		Level 3 Parent, LLC	United States

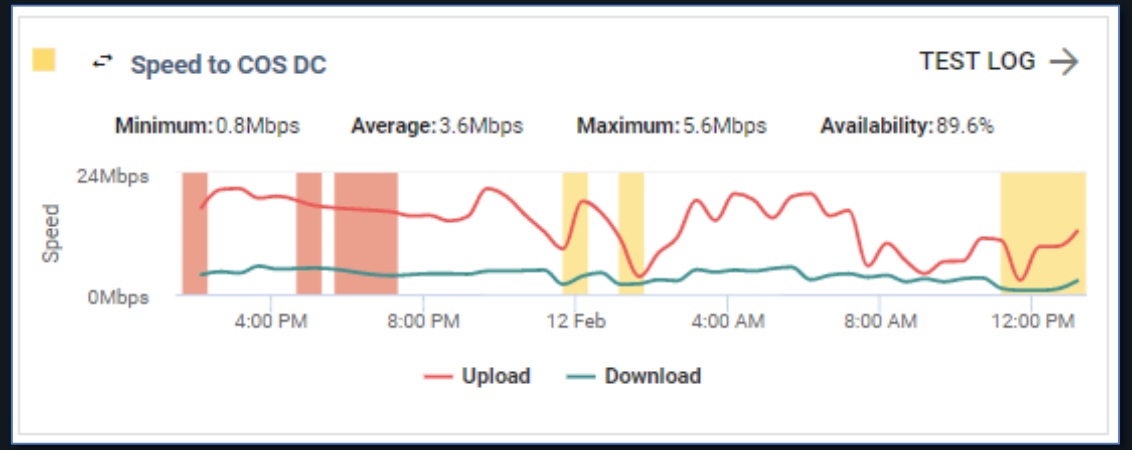


广域网路径的可视性提供问题区域的界定

网络性能监控

- 监控广域网、局域网和Wi-Fi网络的性能
- 隔离有线和无线网络性能问题
- 诊断Wi-Fi基础设施问题
- 建立网络性能基线，包括丢包、延迟、抖动，以及吞吐量测试

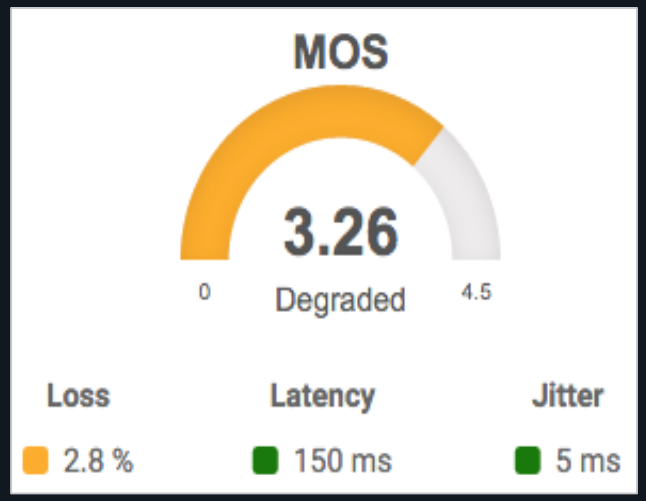




识别由网络性能问题引起的服务交付问题

VoIP服务监控

- 识别VoIP服务的可用性和呼叫质量问题
- 在业务用户抱怨之前获得告警
- 测试呼叫中心的站点到站点和外部可用性
- 按需测试进行故障排除

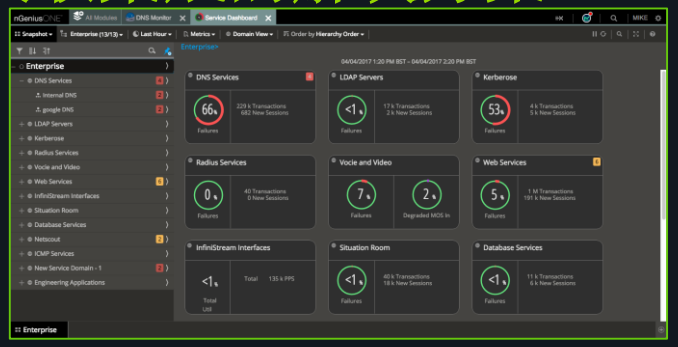


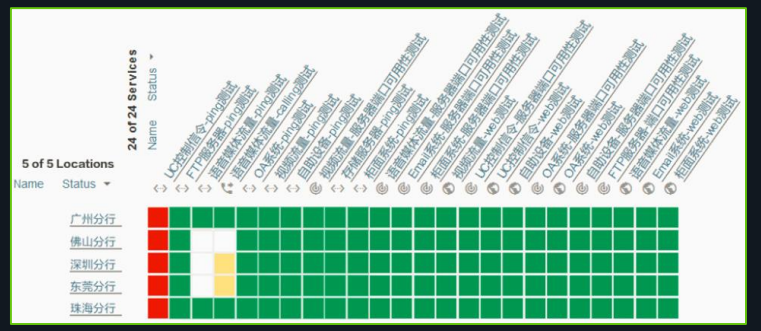
3.45	LQ MOS
1.91 %	Loss (%)
50.17 ms	Latency
1.28 ms	Jitter
50 ms	Jitter Buffer
62775 bps	Data Rate
PCMU @8kHz	Codec
822 ms	Dial Delay
3315 ms	Ring Delay

确保VoIP服务的可用性

融合基础架构监测数据

多数据源关联集成的解决方案





nGeniusONE

服务分诊

自上而下的分析

关联分析

nGeniusPULSE

服务可用性监测

网络性能分析

应用性能分析

服务主动性测试

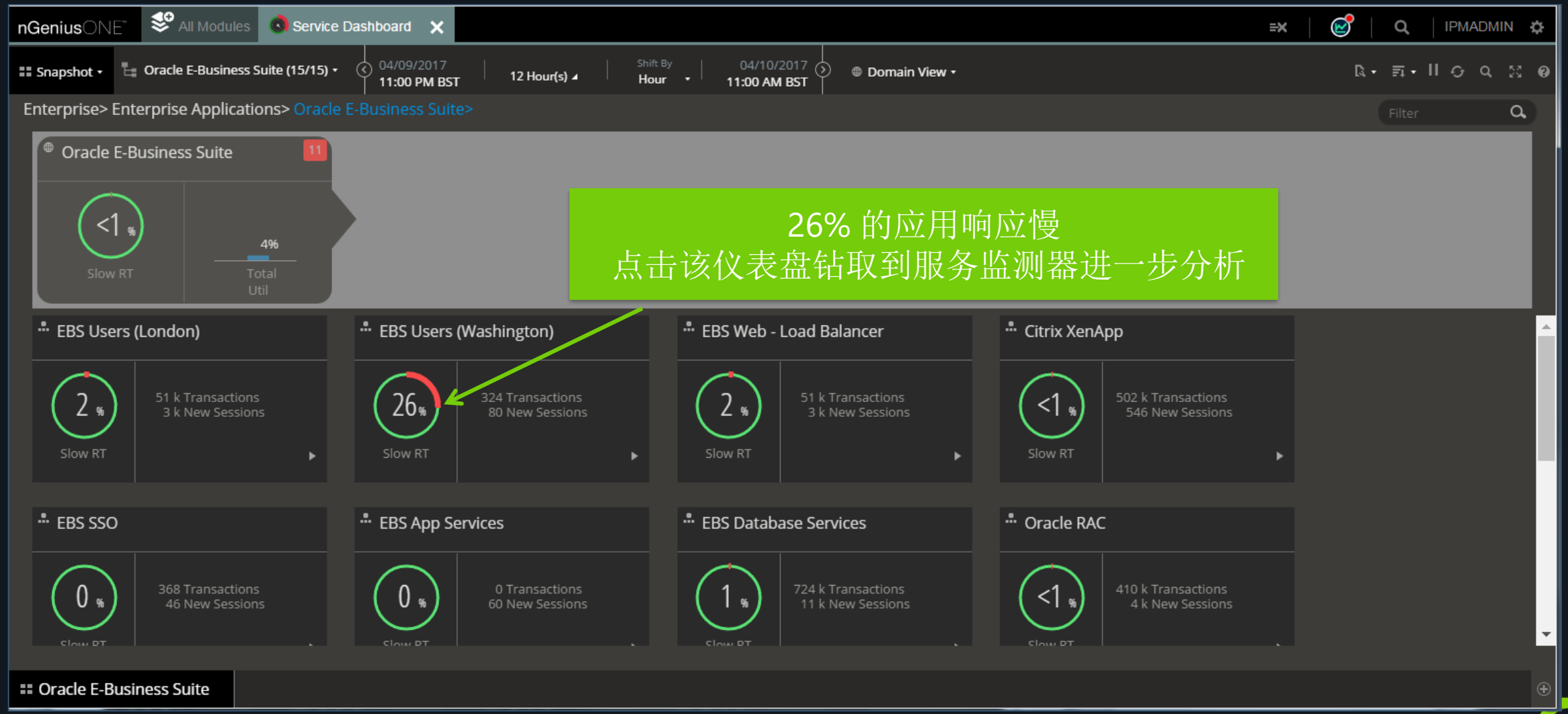
服务器健康性

网络设备健康性

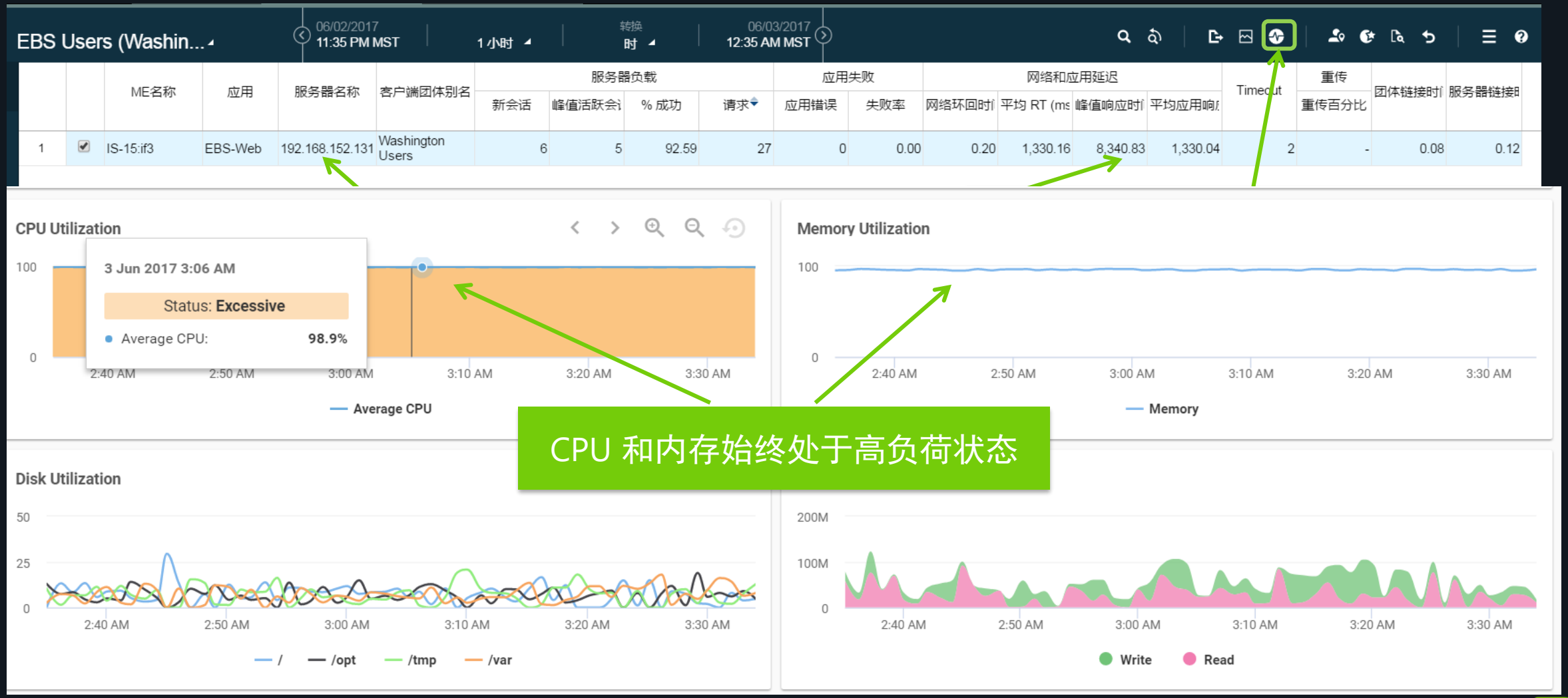
Syslog事件

nGeniusPULSE与nGeniusONE集成，为服务分诊提供服务器问题定位和根源调查

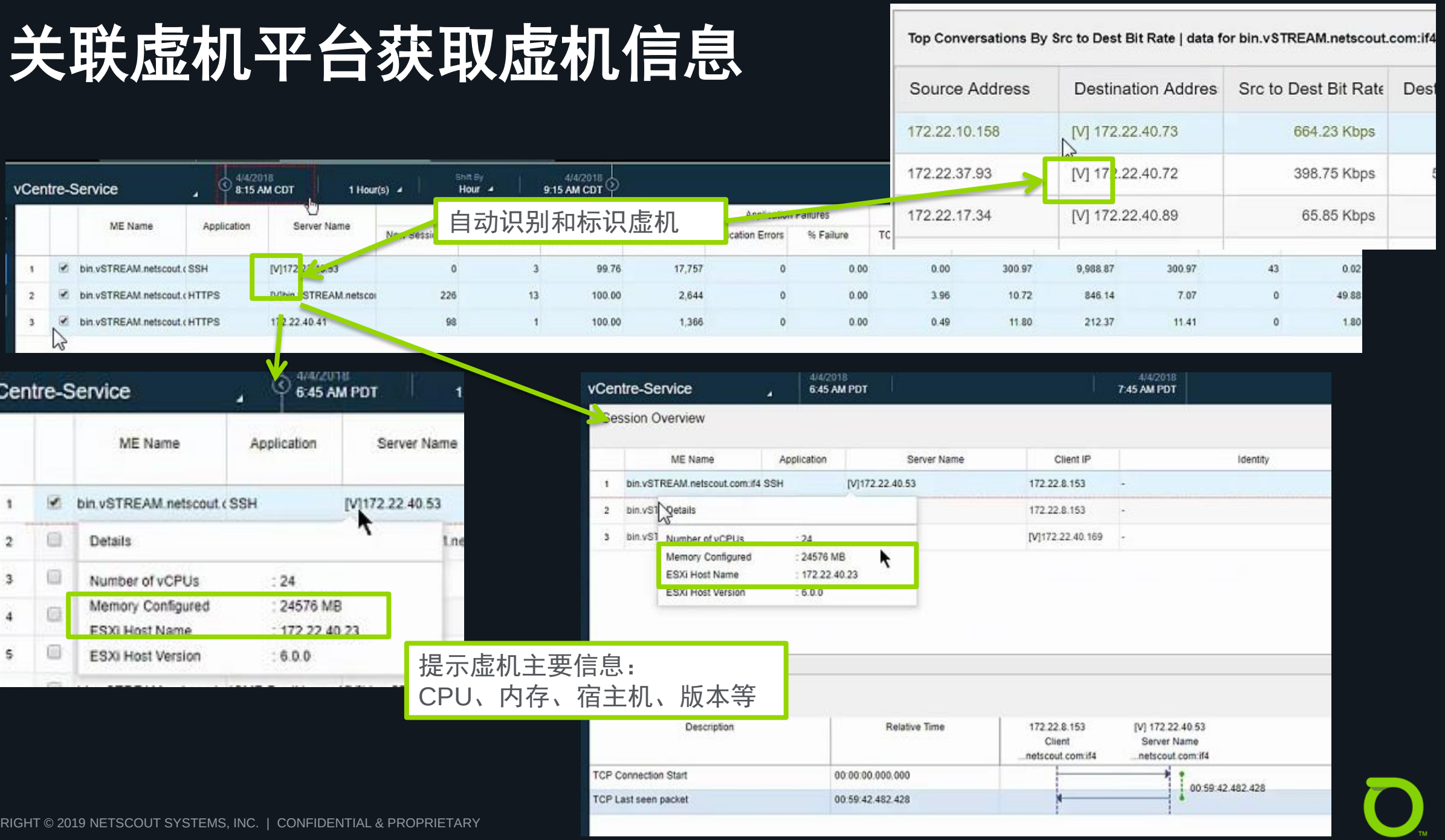
服务仪表盘—发现Oracle EBS问题



关联基础架构监控数据快速判断服务器状态



关联虚机平台获取虚机信息



NETSCOUT服务保障解决方案总结

端到端的业务保障

- 从开始到结束：完整覆盖故障发生的全过程
- 从数据中心到云
- 从分支到总部
- 从无线到有线
- 从网络到服务器到应用
- 从数据到语音、视频的联合分析
- 从被动监控到主动测试
- 助力大数据平台的完善

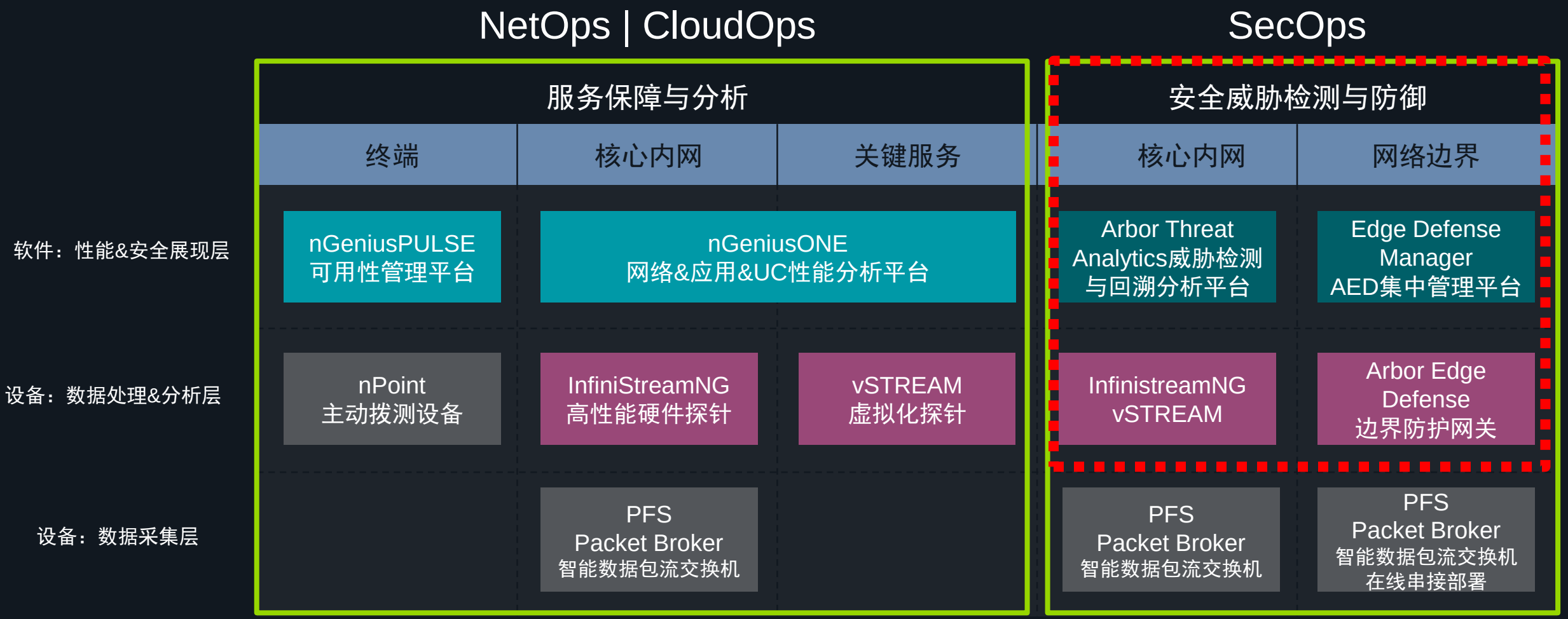
NETSCOUT

安全保障解决方案

Arbor Edge Defense 和Arbor Threat Analytics

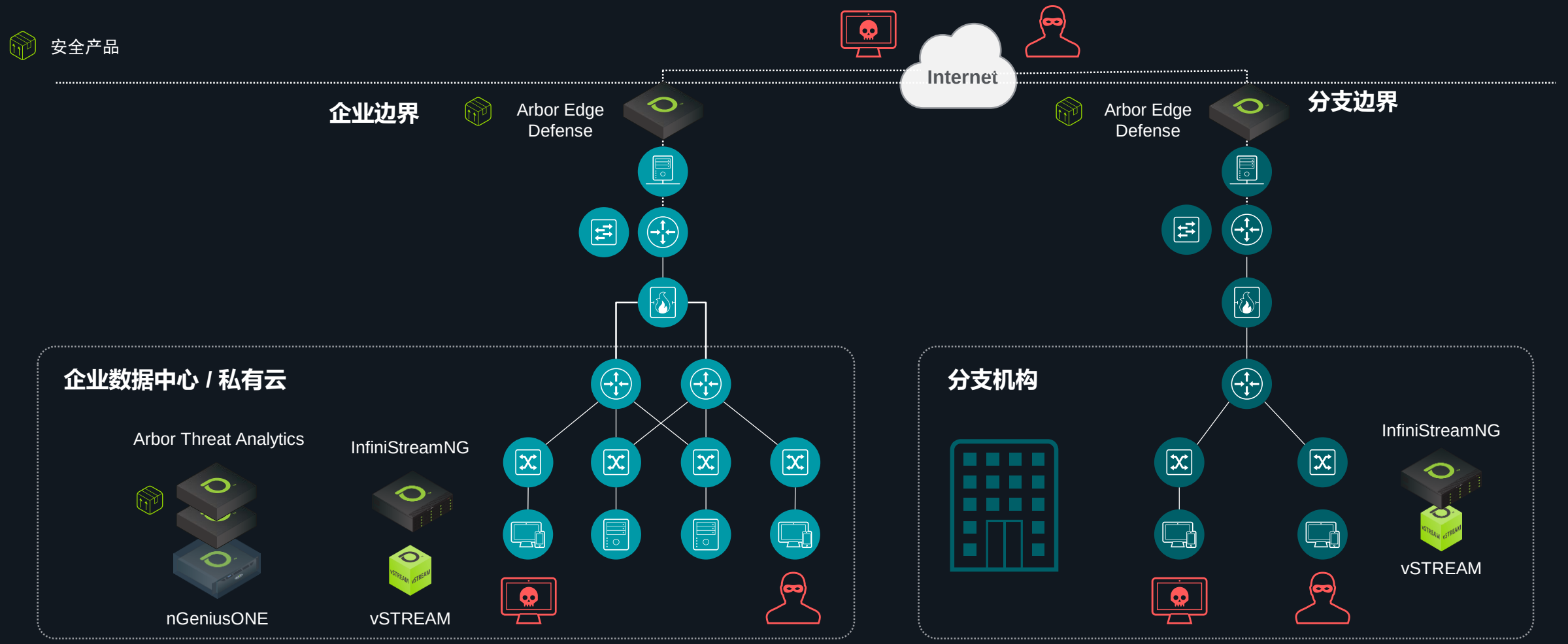
NETSCOUT安全解决方案

为企业网络提供边界和内网安全保障



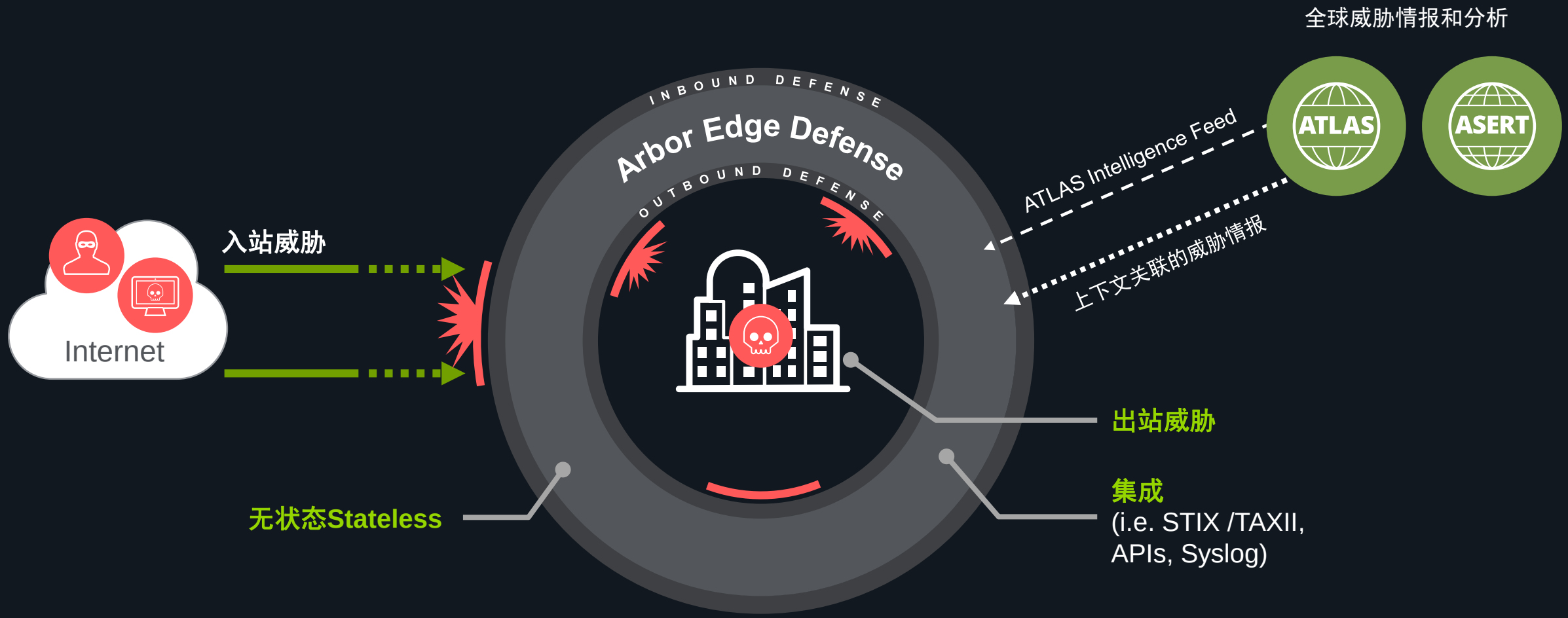
NETSCOUT企业网络安全解决方案

Arbor Threat Analytics 和 Arbor Edge Defense



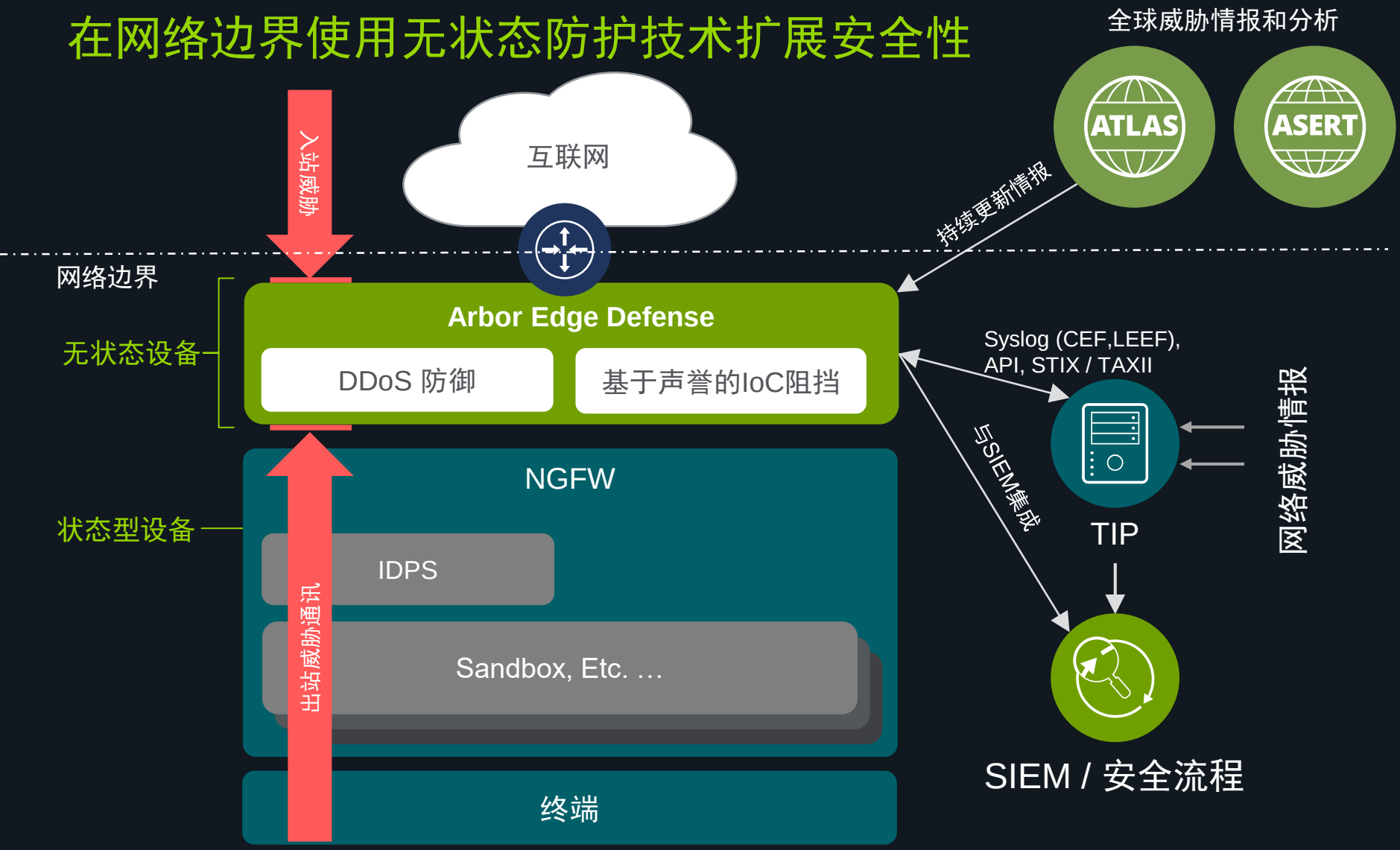
Arbor Edge Defense (AED)

智能、自动化的边界防御，第一道和最后一道安全防线



Arbor Edge Defense (AED)

在网络边界使用无状态防护技术扩展安全性



无状态的网络边界防御
（融合DDoS防御和类似威胁情报网关TIG的功能）

保护和增强NGFW

与现有安全堆栈和流程集成

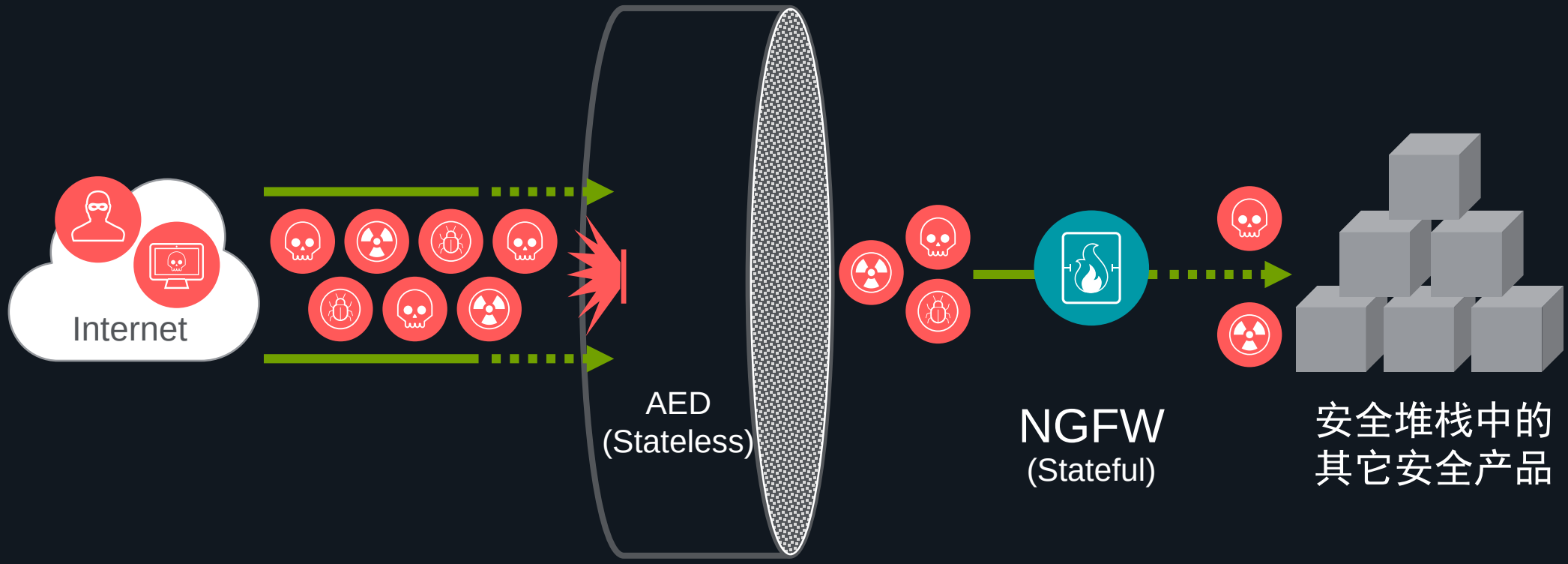
IoC：Indicator of Compromise 入侵指标

Arbor Edge Defense 使用场景

- 防御入站TCP状态耗尽DDoS攻击
  - 作为第一道安全防线
  - 保护状态型设备（如NGFW）
- 防御入站IoC
  - 作为第一道安全防线
  - 缓解状态型设备的负载（如NGFW）
- 阻止出站IoC
  - 作为最后一道安全防线
  - 阻止可能被安全堆栈错过的IoC，避免数据泄漏

无状态包处理以停止入站威胁

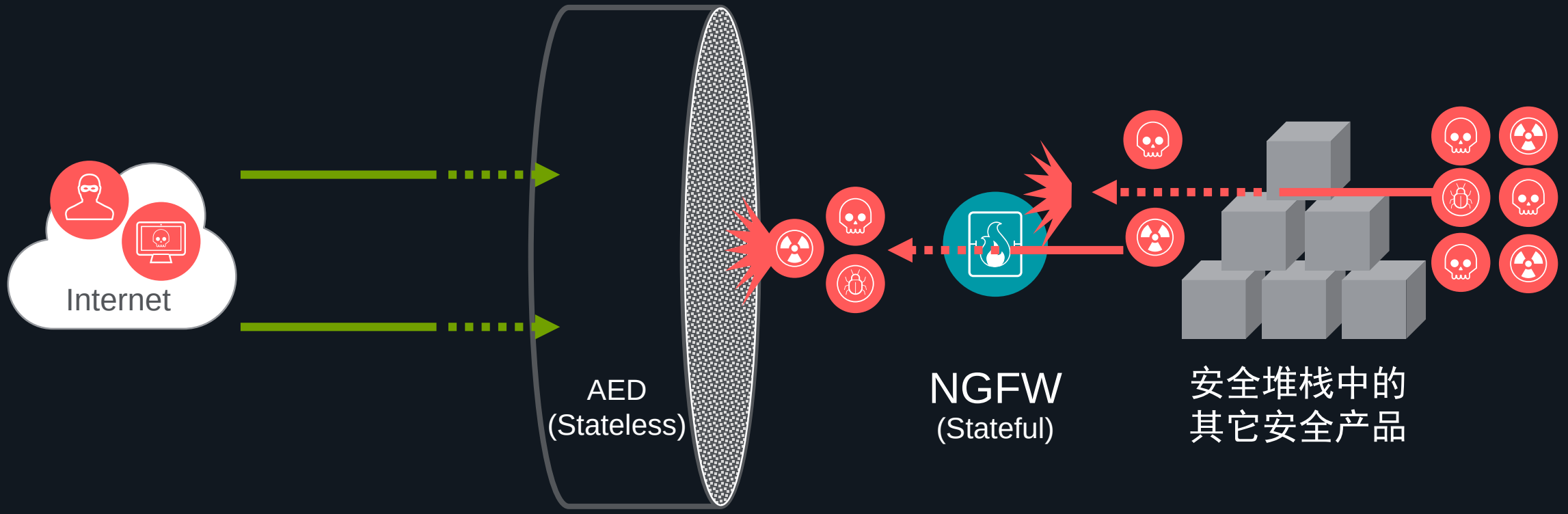
停止入站DDoS攻击和大量的商业威胁



- 拥有数百万基于声誉的IoC，无状态的边界防御就像一个“粗过滤器”，使有状态的防火墙更加高效

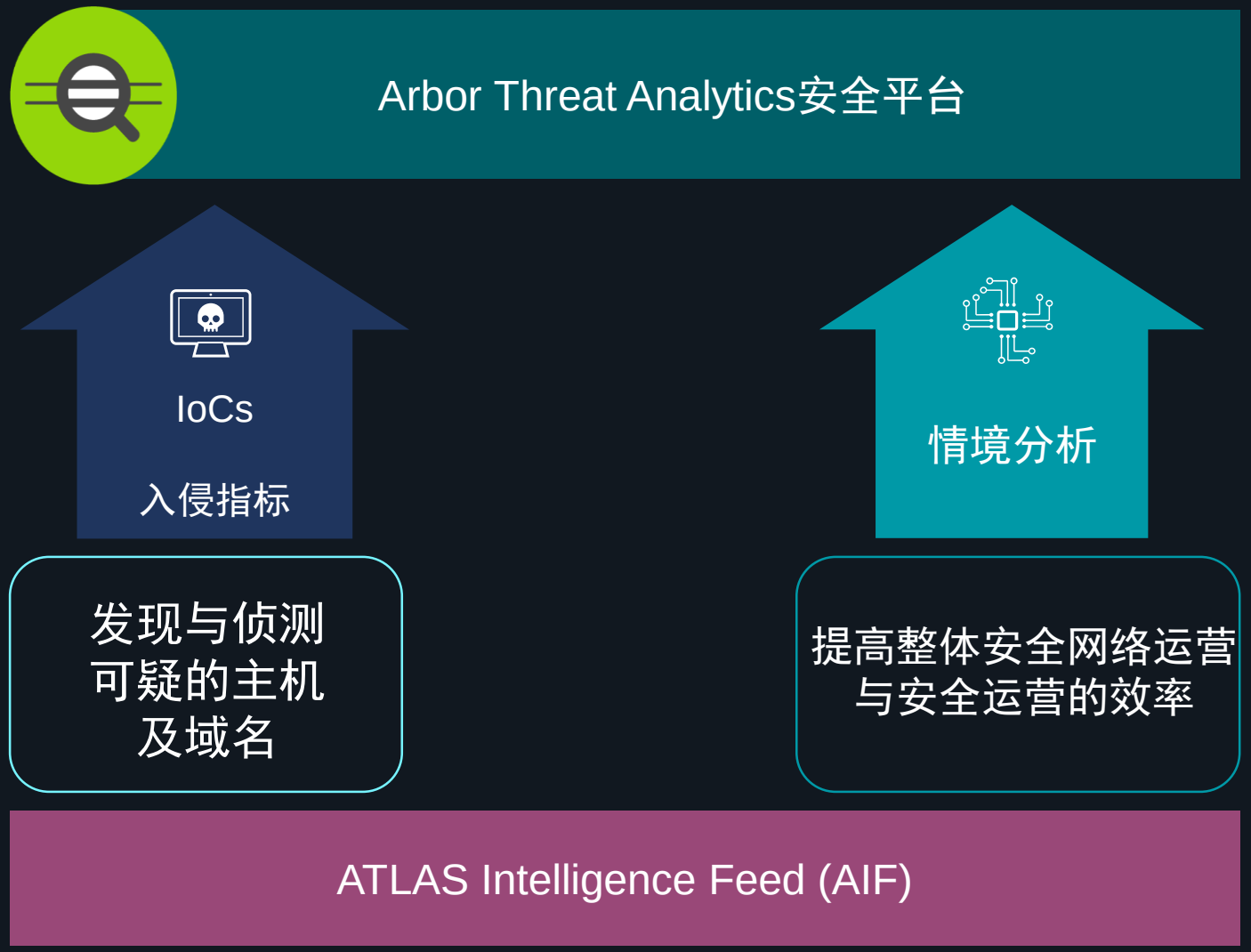
无状态包处理停止出站IoC

最后的防线阻止与外部的恶意威胁通讯



- 拥有数以百万计的基于声誉的IoC，无状态的边界防御作为最后的防线或“过滤器”，停止安全堆栈可能已经错过的IoC

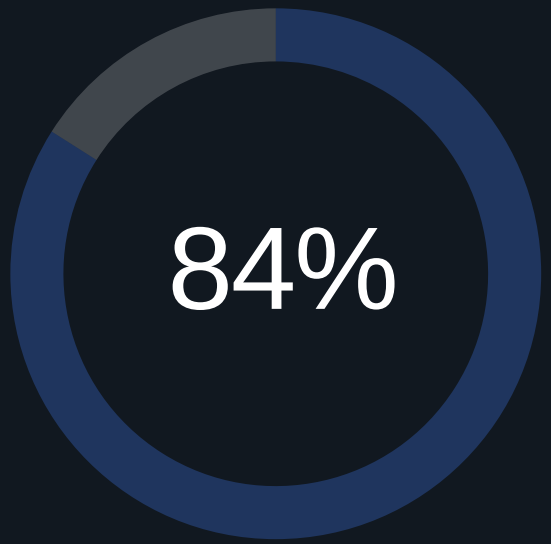
基于全球ATLAS Intelligence Feed (AIF)的情报签名匹配



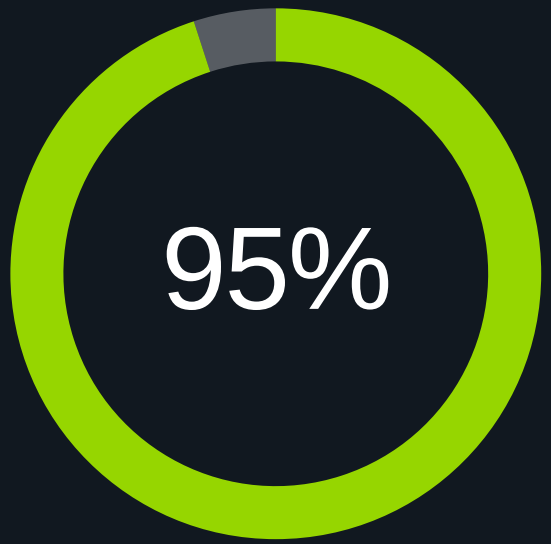
AIF - NETSCOUT 全球IoC指标

通过深度行为分析和递归检查/提取实现全面的IoC

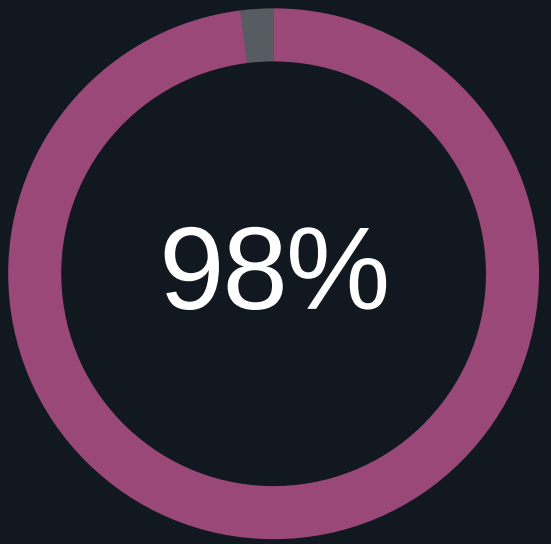
针对35种以上的非商业和商业产品进行基准测试，唯一性：



IPs

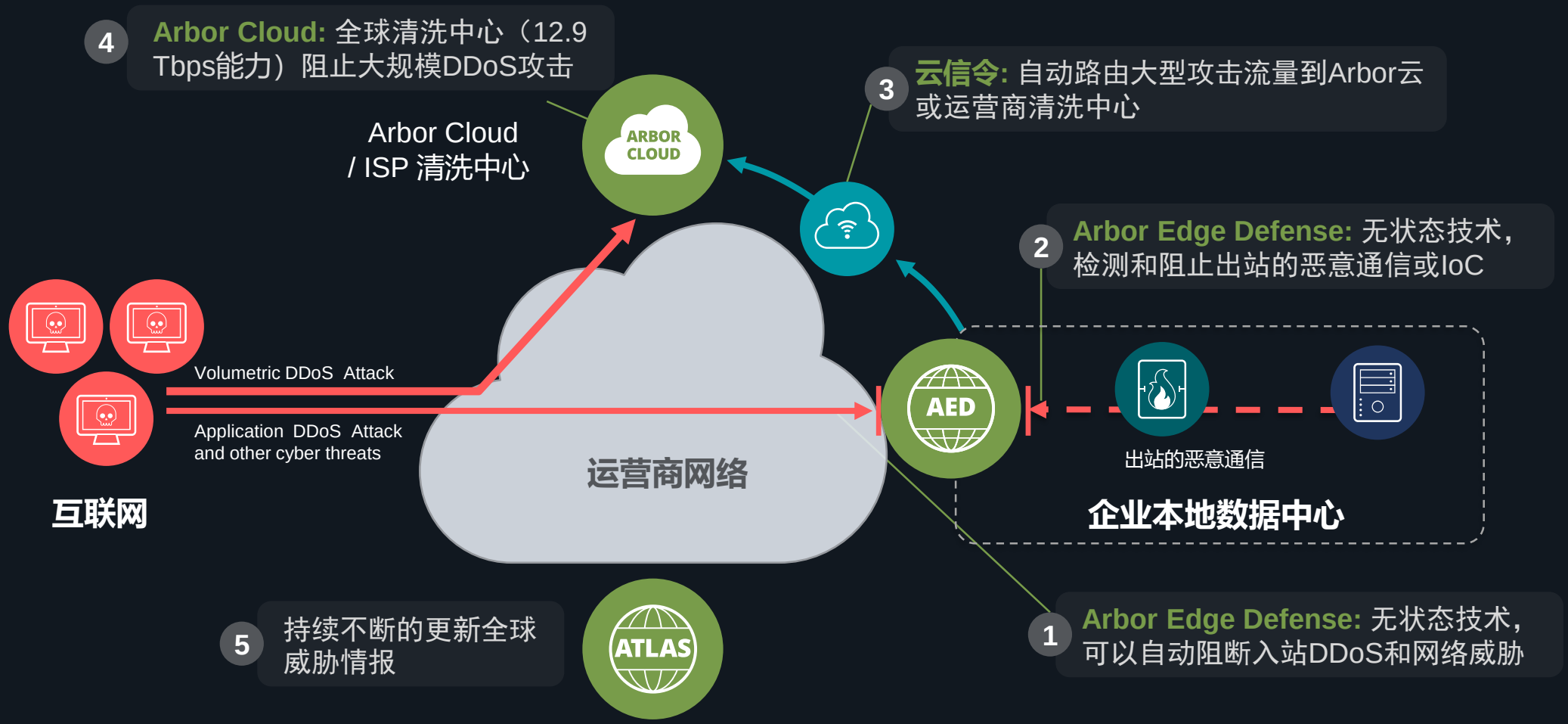


Domains



URLs

完整的DDoS 和网络威胁防御生态链



传统网络威胁调查的挑战

问题

SIEM

Logs Configs Alerts Changes Tickets Activities

Windows Applications Cloud Databases Firewalls Networking

检测 调查 缓解

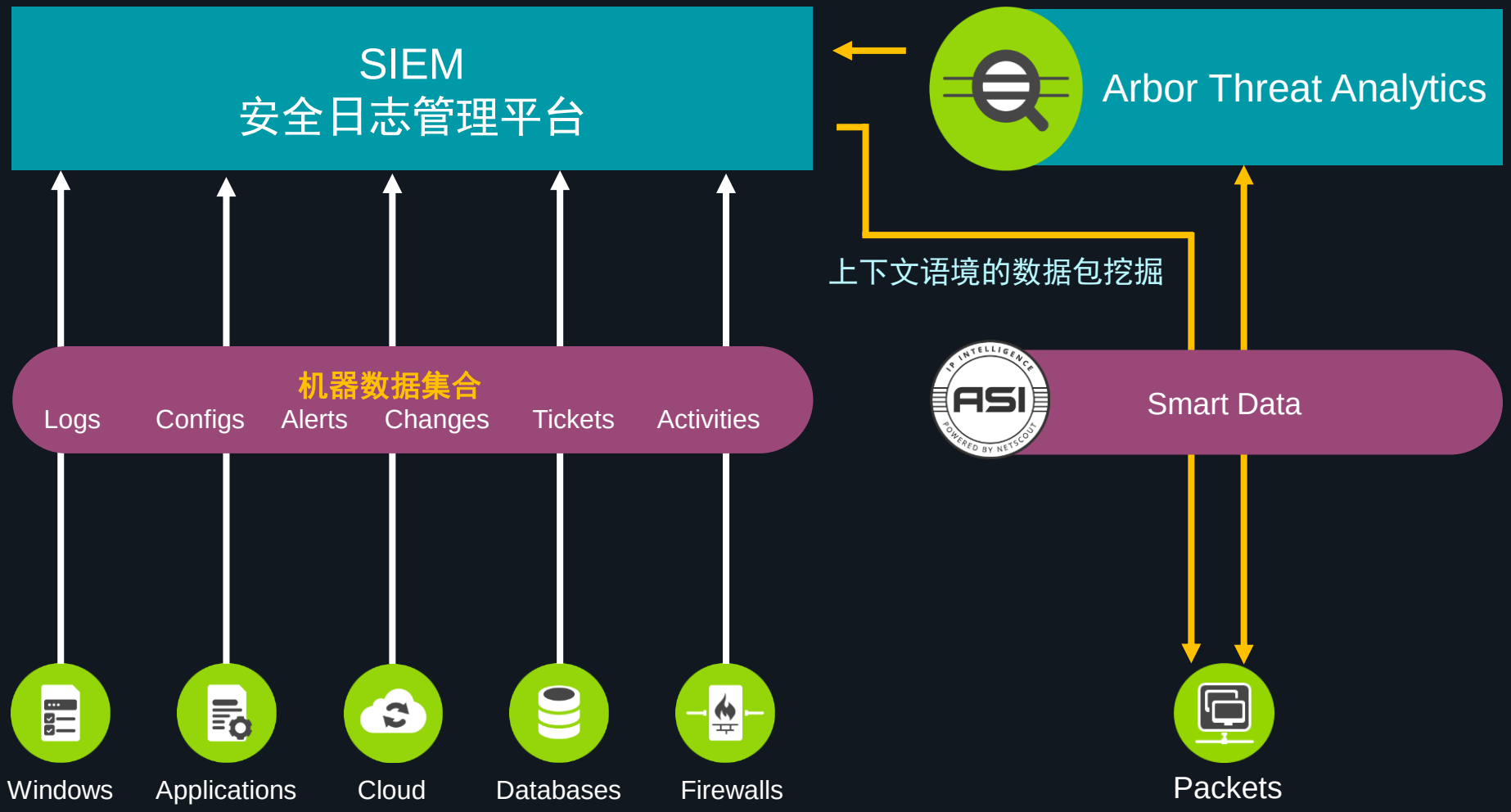
SOC中的网络威胁调查的挑战：

- 增长的复杂性
  - 太多的工具和错误警报
  - 不同且不一致的数据集
  - 可视性的差距
  - 缺乏：
    - 单一事实源（一致的数据集）
    - 确凿的调查
    - 威胁影响评估
    - 快速获取证据

- 增长的MTTR
  - 浪费分析时间

Arbor Threat Analytics(ATA)安全分析与追溯平台

基于NETSCOUT专利技术的全新安全分析与威胁追溯平台



01 **检测**

- 攻击识别
- 流量异常
- 应用风险

02 **分析**

- 事件还原
- 安全分诊

03 **回溯&调查**

- 真实数据验证
- 审计与合规验证

ATA的价值与主张

更低的风险调查成本及投资成本

01 从企业边界到核心的全网安全可视化与检测手段

02 全量的流量，最真实的数据进行分析与告警

03 通过闭环调查减少对整个事件的调查开销成本

企业及云环境的典型部署架构

协同工作的网络运营与安全运营平台

数据中心/
混合云网络

Packet Data

高性能硬件探针

虚拟化探针

Smart Data

Arbor Threat Analytics
安全分析与追溯

nGeniusONE
网络应用分析

ATA的典型功能

预警、事件调查、原始数据以及第三方集成

发现与预警

- 基于安全风险与威胁指标的攻击发现
- 签名与指标匹配
- ATLAS Intelligent Feed (AIF) 威胁情报库

情境调查

- 基于主机IP与时间上下文的主机调查
- 基于服务器、应用、会话明细的时间调查
- 原始数据包的回溯与审计

第三方安全平台集成

- SOC 集成
集成第三方安全平台进行关键敏感数据的挖掘与调查
- ARIN确定安全威胁的来源与组织

Arbor Threat Analytics

检测网络安全风险和内部攻击

内部攻击

- Volumetric流量攻击
- State Exhaustion状态耗尽攻击
- Application Layer应用层攻击

应用协议风险 （举例）

- SMB v1
- Telnet / RDP
- Certificate
- SSL
- DNS
- NTP
- Insecure File Transfer Protocols

Arbor Threat Analytics

可检测的内部攻击种类

VOLUMETRIC流量攻击

- Total Traffic
- Chargen Amplification
- DNS Amplification
- ICMP
- IP Fragment
- IPv4 Protocol 0
- L2TP
- mDNS
- DNS
- MS SQL RS Amplification
- NetBIOS
- NTP Amplification
- RIPv1
- Rpcbind
- SNMP Amplification
- SSDP Amplification
- TCP ACK
- TCP RST
- TCP SYN / ACK Amplification
- UDP
- TCP

检测内部DDoS

STATE EXHAUSTION 状态耗尽攻击

- TCP SYN
- New Sessions
- Connect Time
- Total Active Sessions

APP LAYER 应用层攻击

- HTTP Flood
- DNS Flood

Arbor Threat Analytics

应用协议风险检测

证书Certificates

- 自签名，不可信
- 超期证书

SSL / TLS

- 过时的版本
- 弱密文

DNS 安全

- 反向查寻
- 非企业DNS服务器

确保企业内部安全

不安全的应用

- SMB v1
- Telnet / RDP
- SNMP v1 / v2

扫描事件

- 网络扫描(ARP / ICMP)
- 端口扫描

NTP

- 非企业的NTP服务器

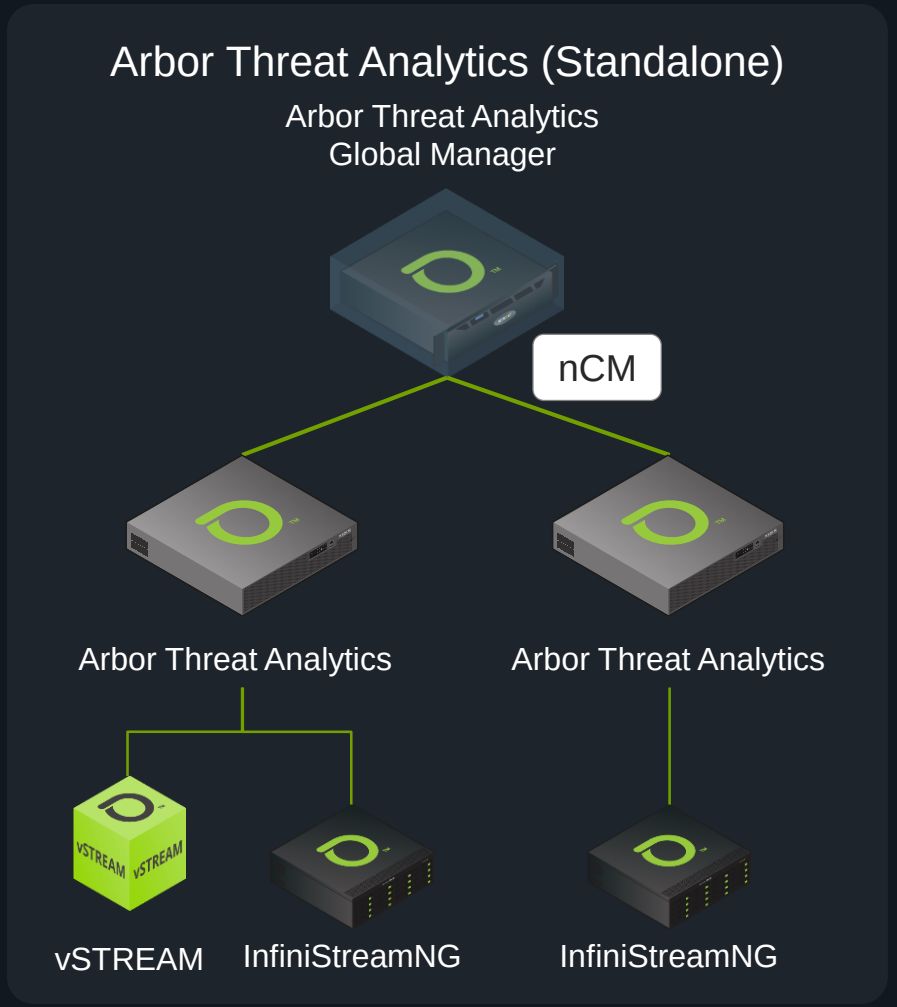
不安全的文件传输协议

- CIFS / FTP

ATA部署架构

独立模式

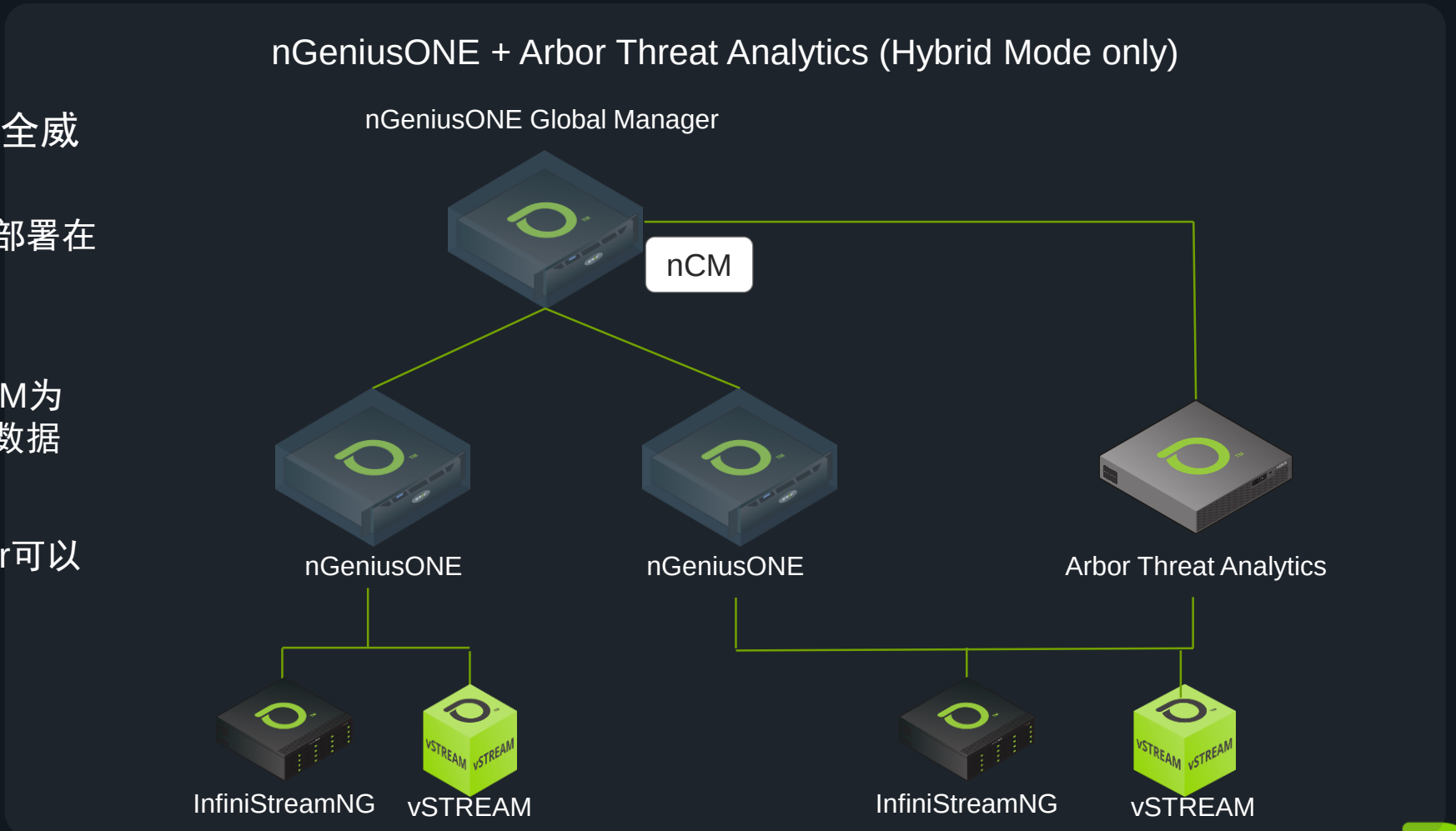
- 分布式部署探针
  - ✓ 多台InfiniStreamNG/vSTREAM分布式部署于网络中的各个监测点
  - ✓ 为ATA提供分析数据
- 集中管理
  - ✓ ATA服务器集中管理分布式部署的探针
  - ✓ ATA服务器集中呈现分析结果
- 支持全局模式
  - ✓ 多台ATA服务器分布式部署
  - ✓ ATA Global Manager集中管理所有的ATA服务器
  - ✓ 适用于多数据中心或多区域环境



ATA部署架构

混合模式：与nG1并存

- 单一平台实现服务保障和安全威胁分析
  - ✓ ATA软件和nG1软件分别部署在不同的服务器上
- 共用数据源
  - ✓ InfiniStreamNG/vSTREAM为ATA和nG1同时提供分析数据
- 集中管理
  - ✓ 通过nG1 Global Manager可以同时管理ATA和nG1



ATA解决方案的独特价值

- 为NetOps和SecOps提供单一平台
  - 服务保障和安全检测
- 适用于所有环境—可视性无边界
- 双向SIEM集成
- 基于数据包高保真的威胁分析、威胁情报和取证系统
- 早期检测预警，为上下文调查提供丰富的信息
- 对安全事件进行分诊，以避免War Room，并减少MTTR
- 独特的AIF可以避免误报，获得不良行动者的来源
- 大型企业部署，成本更低

NETSCOUT安全产品的优势

19

多年来，Arbor一直致力于提供创新的安全和网络可视性技术和产品

~200

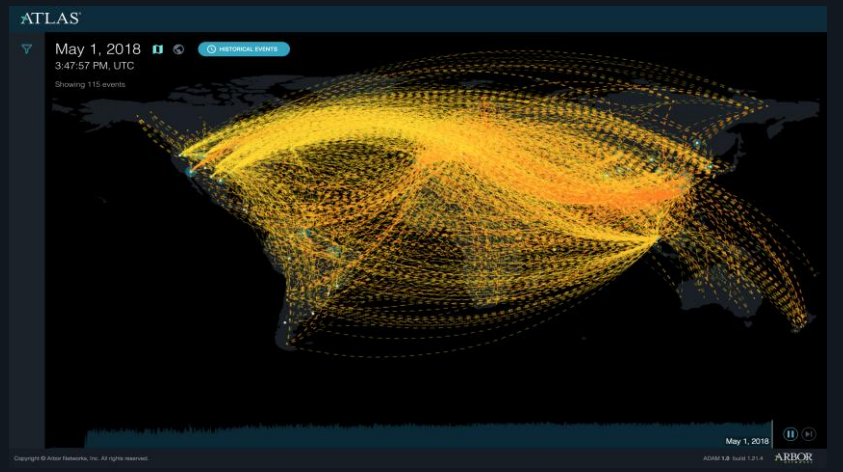
致力于DDoS和网络威胁的工程师、研究人员和分析师

95%

Arbor客户占全球一级服务提供商的比例

NTT · at&t · TATA · verizon · 中国电信 CHINA TELECOM · T-Com · Telefónica · vodafone · BT · france telecom

1/3 of Internet Traffic = 由ATLAS监控的全球流量



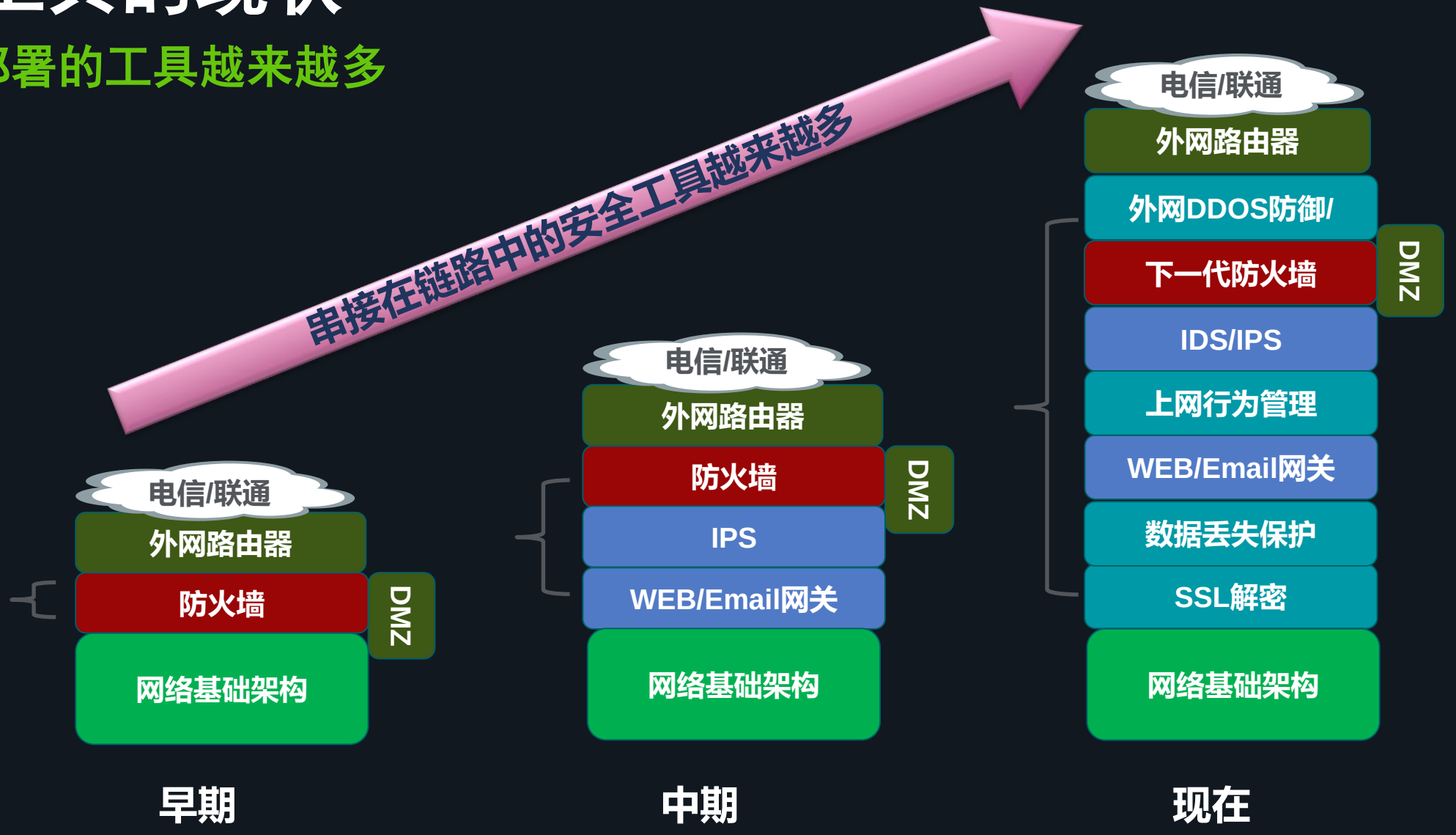
NETSCOUT

流量安全调度平台

PFS Inline部署解决方案

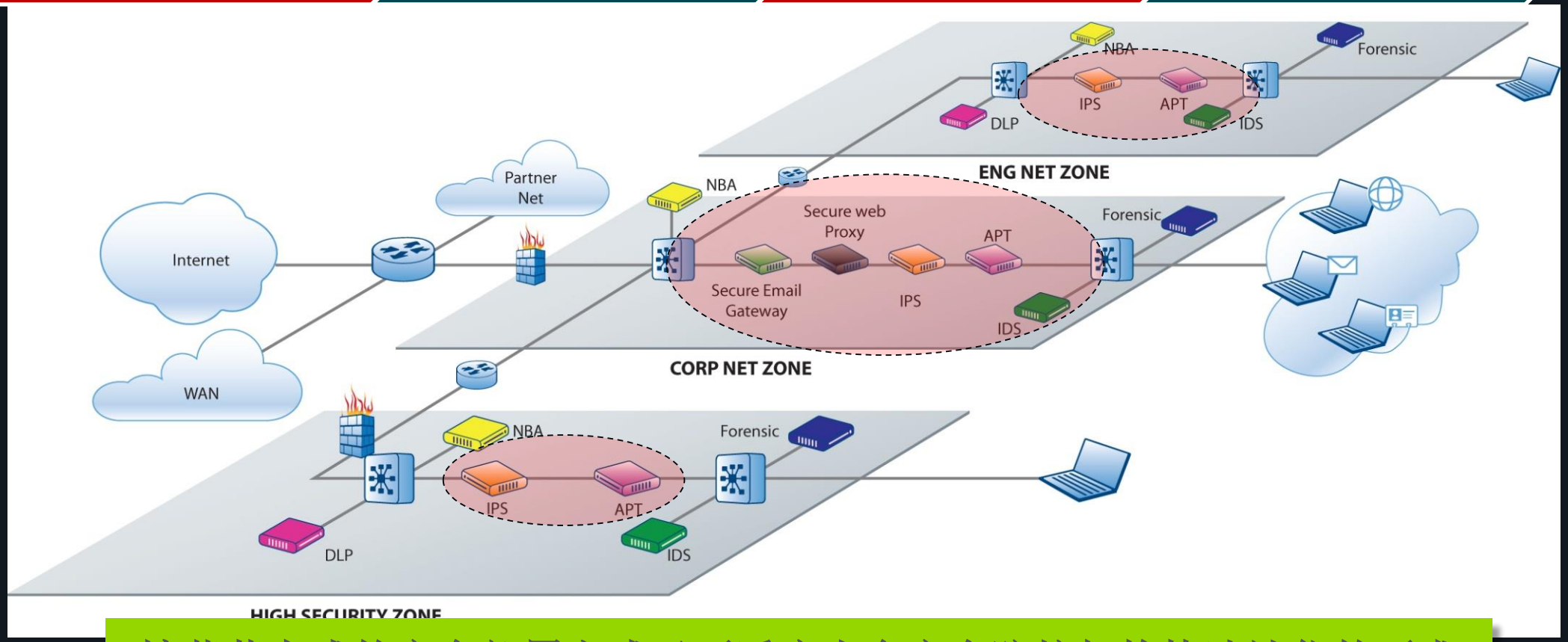
安全工具的现状

串接型部署的工具越来越多



安全部署现状—糖葫芦串

单点故障 | 可扩展性问题 | 安全防护效率 | 管理维护问题



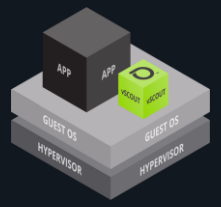
糖葫芦串式的安全部署方式已不适应当今安全防护架构快速迭代的要求

PFS助力企业安全治理

构建统一安全流量调度平台

nGeniusOne Dashboard

生产网络



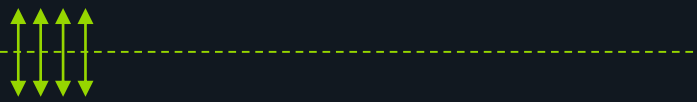
vSTREAM-EMB

HD Fiber TAP

PFS Fabric Manager

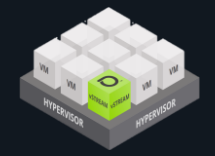
- ✓ 软件驱动
- ✓ 按需扩展
- ✓ 成本可控

Packet Flow
eXtender (PFX)



Packet Flow
OS (PFOS)

监测和安全工具



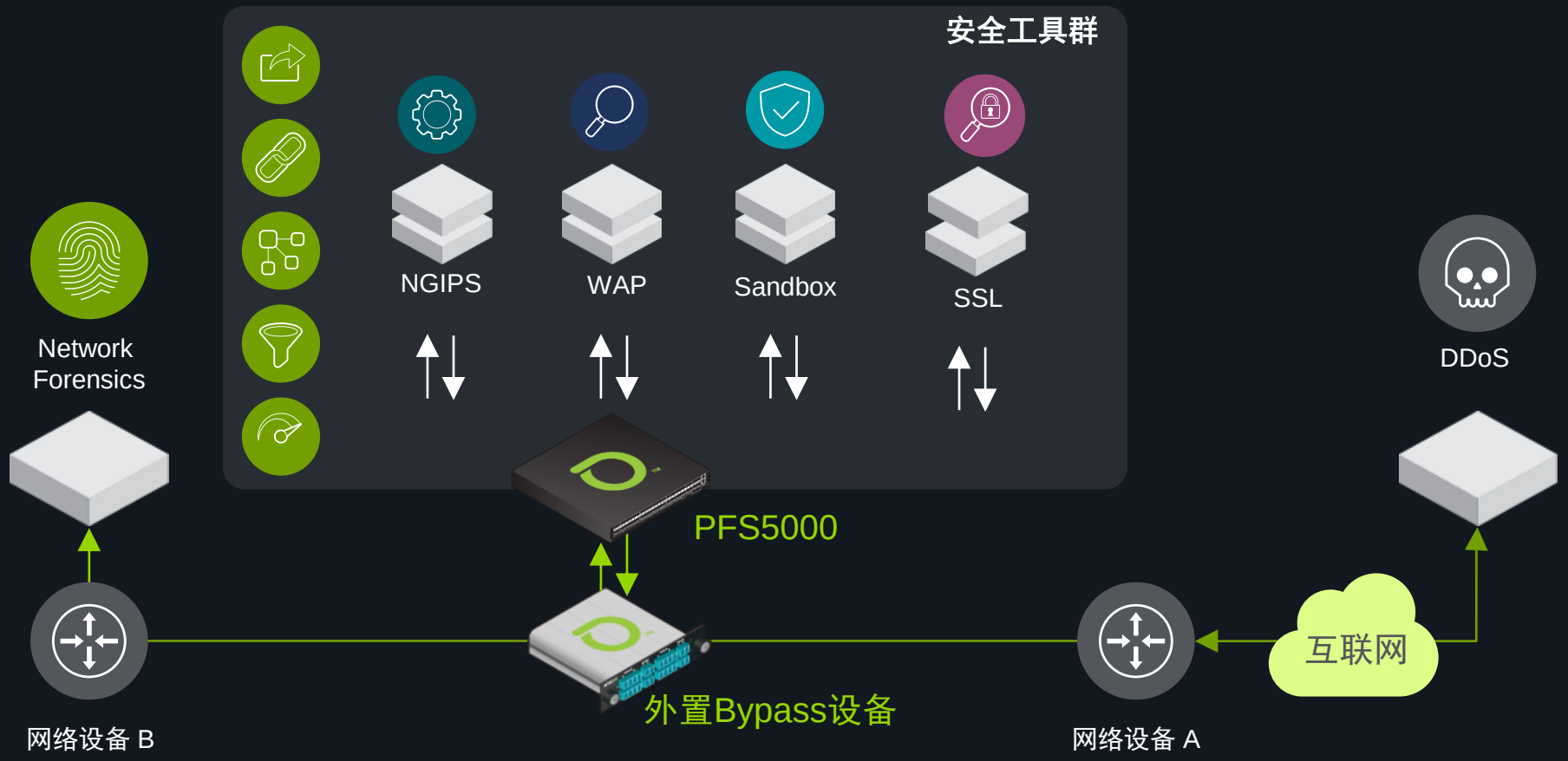
vSTREAM

Application
Performance
Management

Network
Performance
Management

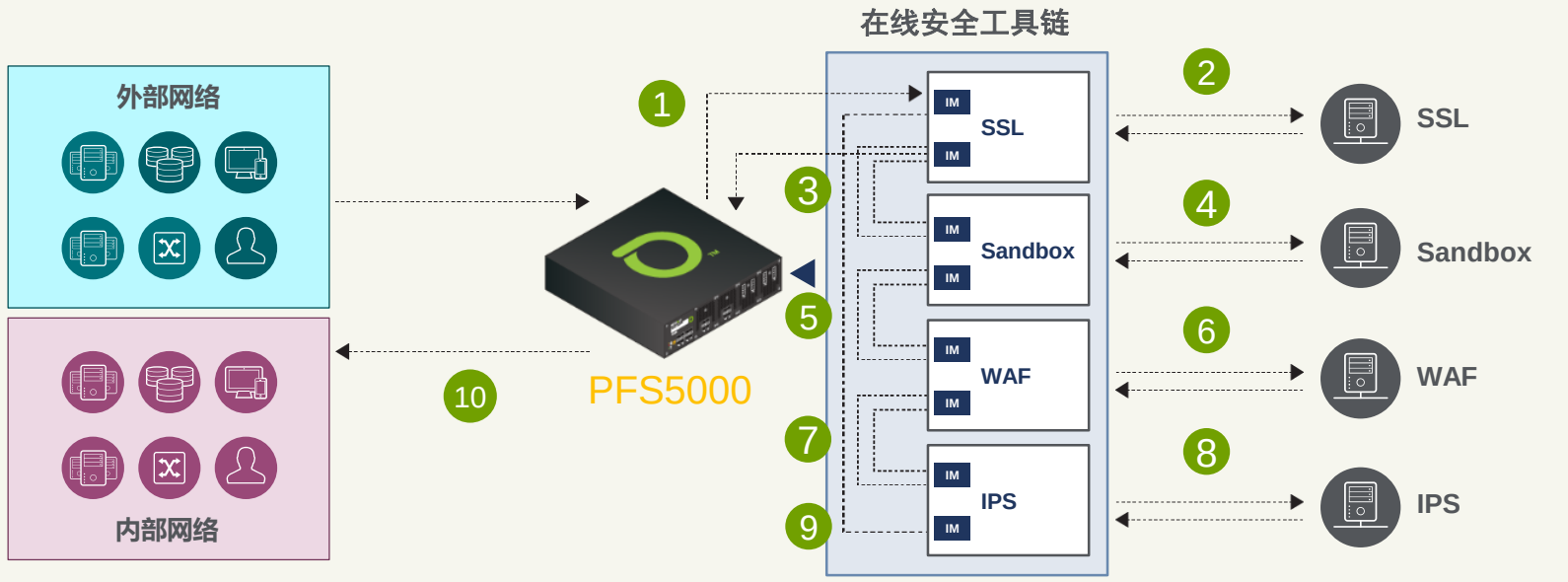
Security

PFS串接部署示意



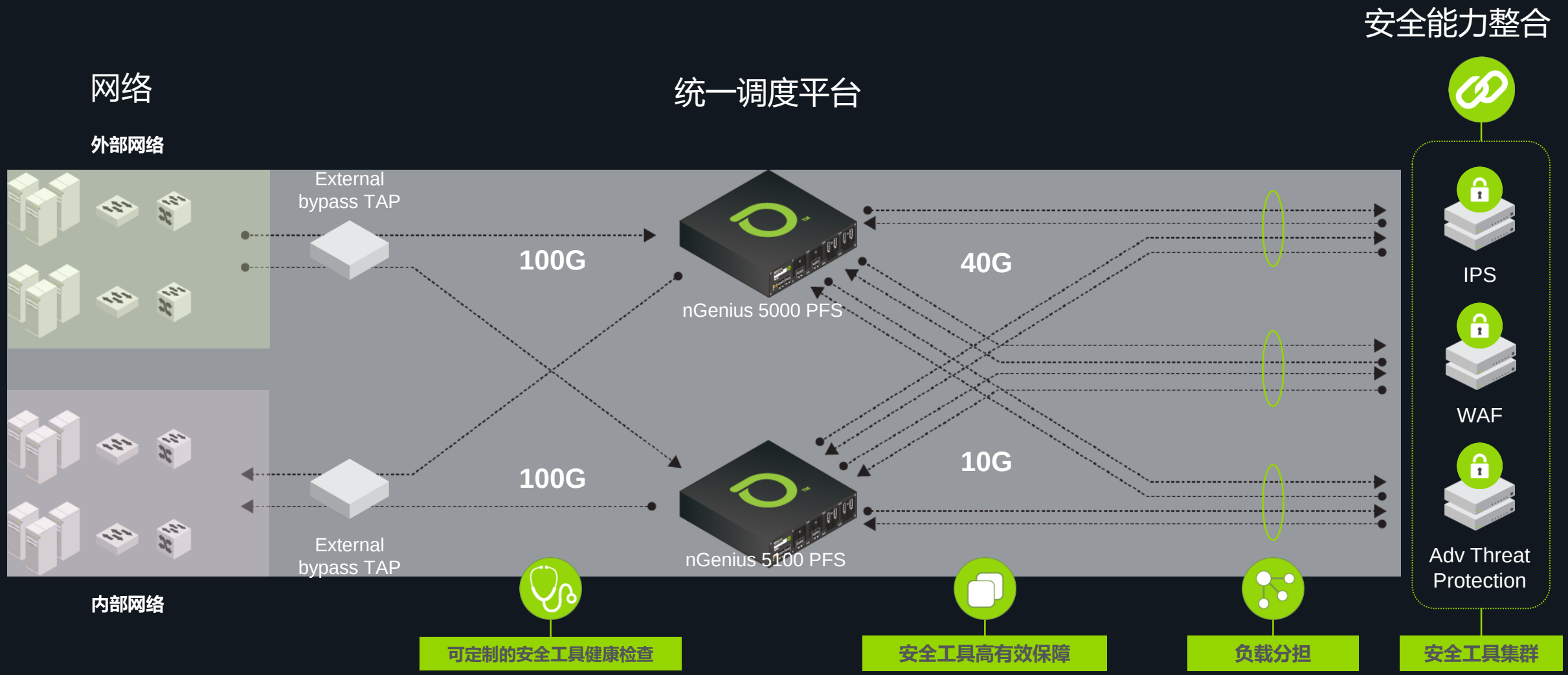
安全流量调度示意

PFS工具链降低了服务和操作风险



1. 聚合的流量被发送到安全工具链，其中每个工具可以在下一个工具之前检查任何或所有流量c
2. SSL设备接收流量并解密
3. 解密后的通信流量对工具链上的所有系统都可用
4. 解密后的流量发送到Sandbox设备进行处理
5. 过滤出HTTP流量发送给WAF设备处理
6. WAF接收HTTP流量并过滤威胁
7. 流量发送给IPS
8. IPS检查恶意威胁并阻断它
9. 流量回到SSL设备，并重新加密
10. ‘干净’ 的流量发送给目标网络

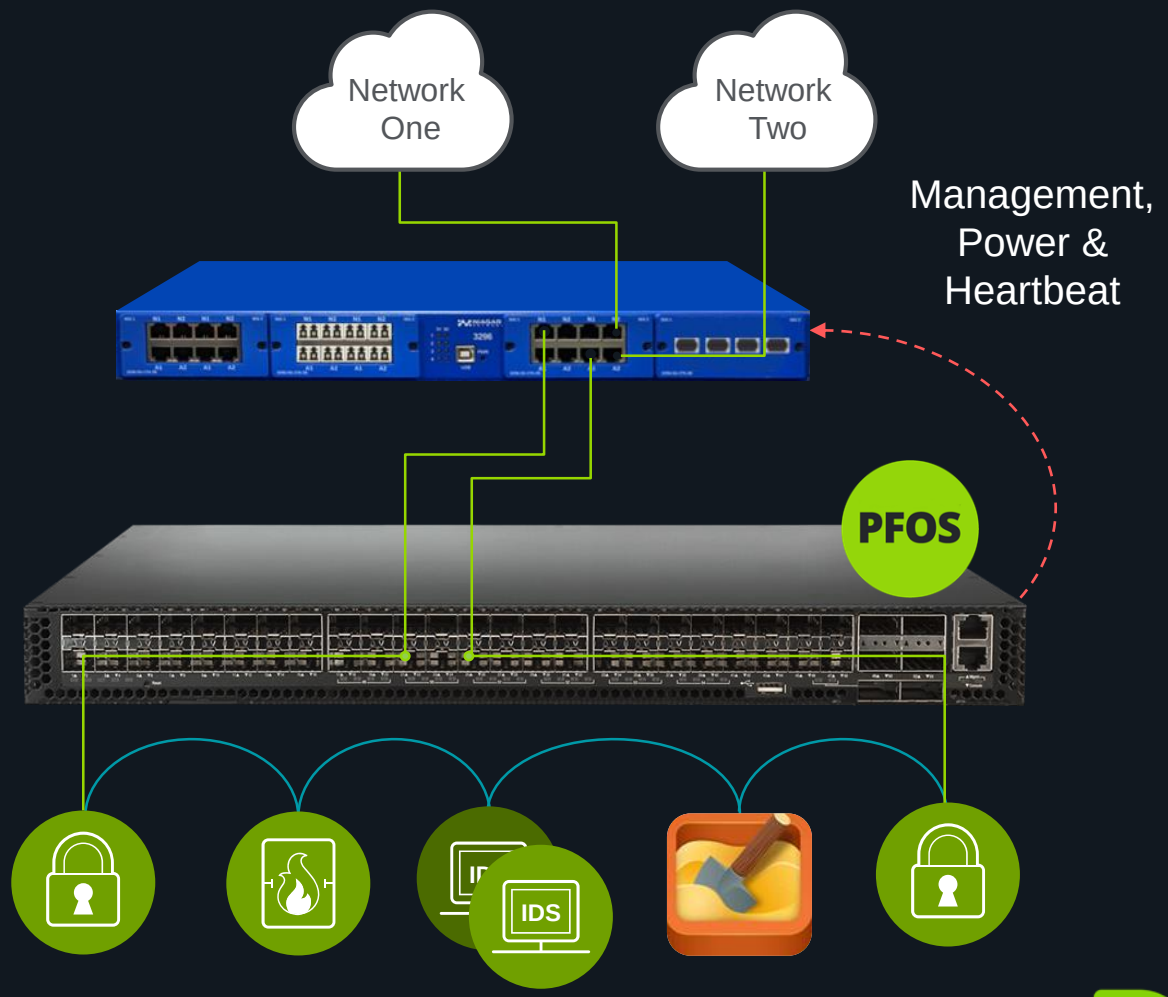
全面提升安全防护架构的可靠性



External PowerSafe TAP (EPT)

外置Bypass设备

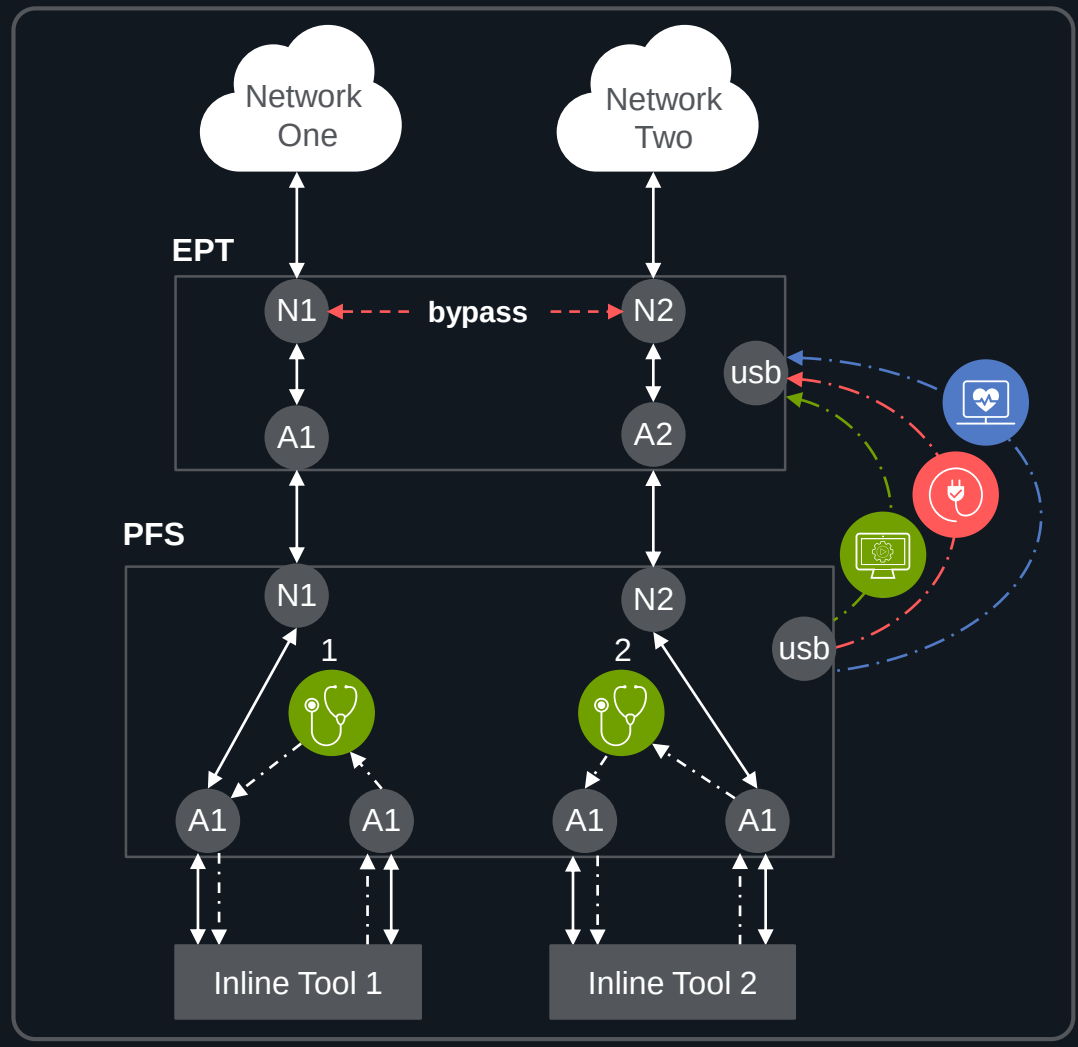
- EPT模块化（4）提供灵活性
- 一个EPT支持多个网段
- PFOS管理实现无缝集成
- 通过USB连接到PFS供电



EPT 和 PFS 协同完成安全串接

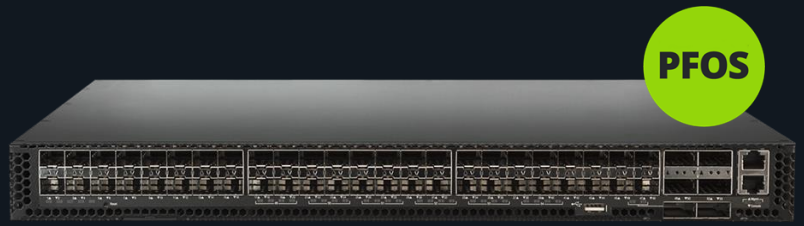
工作示意

- External PowerSafe Tap (EPT)
  - 通过USB从PFS接收心跳、电源和管理
  - 支持Active bypass，如果心跳检查失败后可确保网络流量继续
- PFS 5000 系列
  - 安全工具链
    - 允许数据包从一个工具到另一个工具的智能调度
  - 触发策略 / 健康检查
    - 用户定义包来测试工具的健康状况
    - 旁路健康性有问题的工具



统一的网络和安全可视性

利用PFS实现主动安全性和被动监控



- 开放的计算平台，提高成本效益
- 对1-100G网络链路提供线速处理能力
- 安全流量调度的具体功能，以帮助降低风险，提高可视性和规模的需求
- 架起网络和安全监控之间的桥梁
- 单点管理用于管理、调节和引导流量到被动和主动监控工具
- 在Active Inline的安全部署中，工具链中的负载平衡组允许扩展、维护、更新等，而不会中断

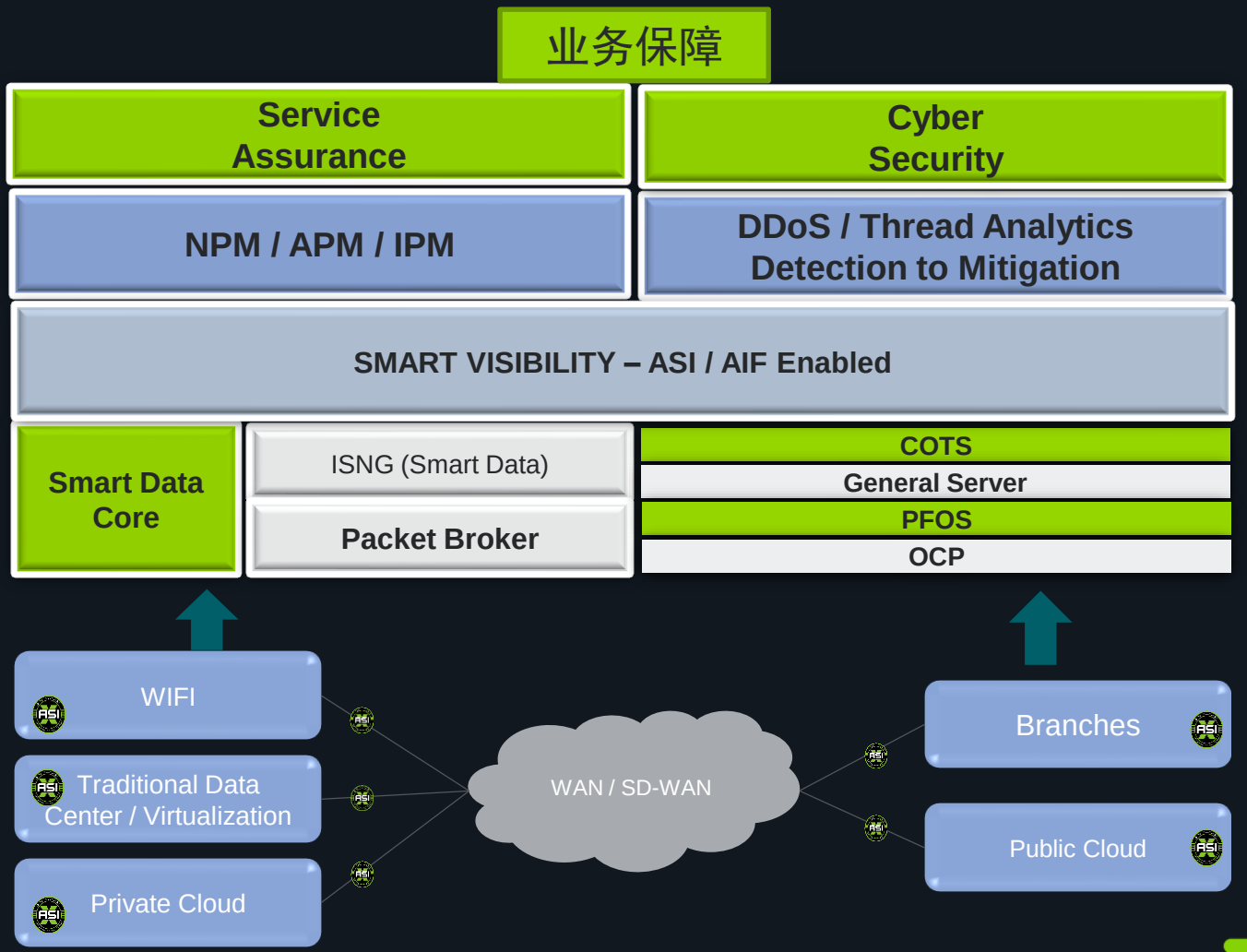
NETSCOUT

NETSCOUT优势总结

NETSCOUT打造智能数据价值的完整生态圈

竞争差异化

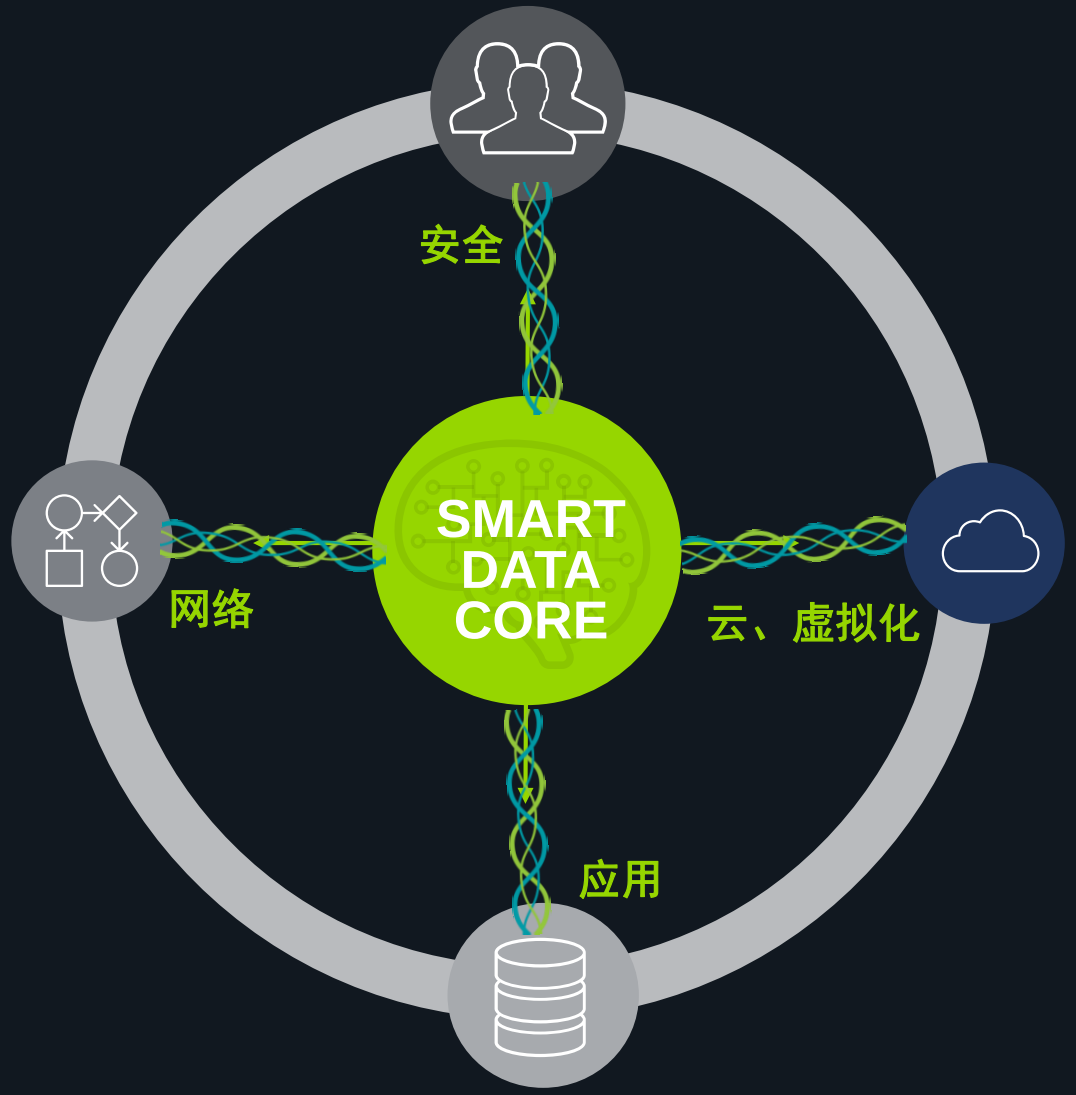
- 可视性无边界
  - 端到端可视性
  - Single Pane of Glass
- 工具整合
  - Smart Data Core
  - 业务保障
- 高性价比
  - 价值领导
  - 成本节约 (Capex/Opex)
  - 无所不在的部署



Smart Data Core解决方案

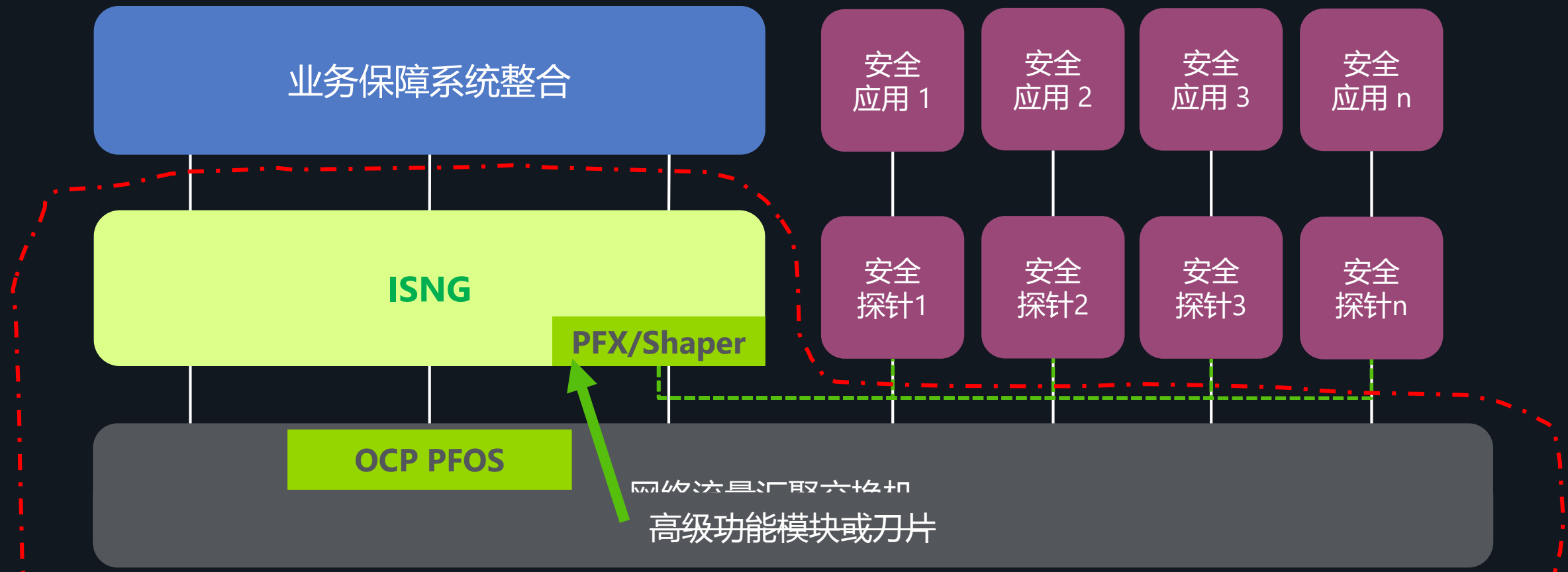
智能数据平台提供通用的智能数据：

- Wire Data → Smart Data
- 软件为中心的解决方案
  - 软、硬分离
  - 降低TCO
- 端到端的网络可视性
  - 全面覆盖物理网络和虚拟网络
  - Underlay和Overlay网络(物理/虚拟)、服务和应用性能的相关联的视图
- 安全威胁分析
- 数据优化后的流量
- 大数据Ready



为智能化运维、业务保障、用户体验分析以及安全防护提供统一的量化数据

智能数据平台 (Smart Data Core)



Smart Data Core：功能软件化、硬件通用化！

NETSCOUT的技术生态圈

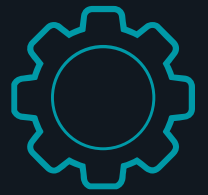
VMware技术联盟与认证，深入耦合vSphere与NSX SDN环境，原生API兼容

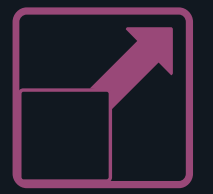
Redhat技术联盟，无缝兼容OpenStack、Docker容器环境，并通过Certified认证

IBM大数据战略合作伙伴，网络指标算法、应用指标算法以及硬件架构提供者

NETSCOUT 解决方案优势总结

智能数据、敏态可视





业界领导

- 超过30年的业界经验，专注于IP数据包的智能
- 服务保障行业的市场和技术领导者
- 创新的Smart Data，融合了服务保障和威胁分析解决方案

成本优化

- 软、硬件解耦，开放的硬件平台
- 投资保护，提供多样化的交付模式
- 降低CAPEX，控制OPEX

软件驱动

- 基于软件的架构，符合未来的需求
- 单一厂商支持传统数据中心、私有云、公有云
- 开放，支持业务编排、模板和REST API用于运维和管理

按需扩展

- 适用于大中型企业的产品架构，高扩展性
- 软件定义分析，适用于各种云环境的按需扩展要求
- 可视性无边界

谢谢

恒景科技