网络安全创新大会
Cyber Security Innovation Summit

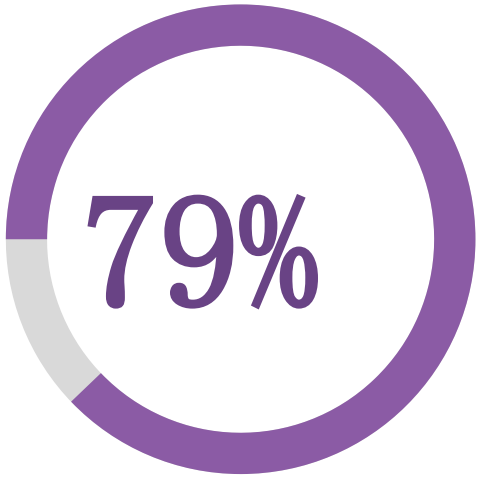
# AA的升级版
# Adaptive Applications
# 感知可控，随需而变的应用

**吴静涛 Fred WU**
**F5大中华区首席技术官**

# “95后”的主流用户要求很高 - 不安全？

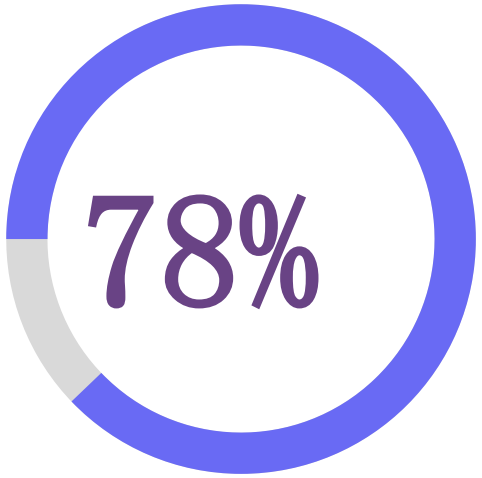


Customer expectations for digital experiences are high*



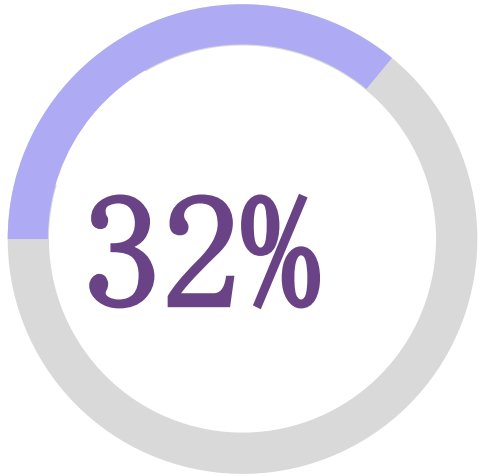

消费者表示数字服务或应用已将其引入新产品和服务

of consumers say that digital services or applications have introduced them to new products and services




消费者要求通过应用程序为差的数字体验提供经济补偿，例如优惠券或折扣

of consumers are demanding financial compensation such as coupons or discounts for poor digital experiences via applications

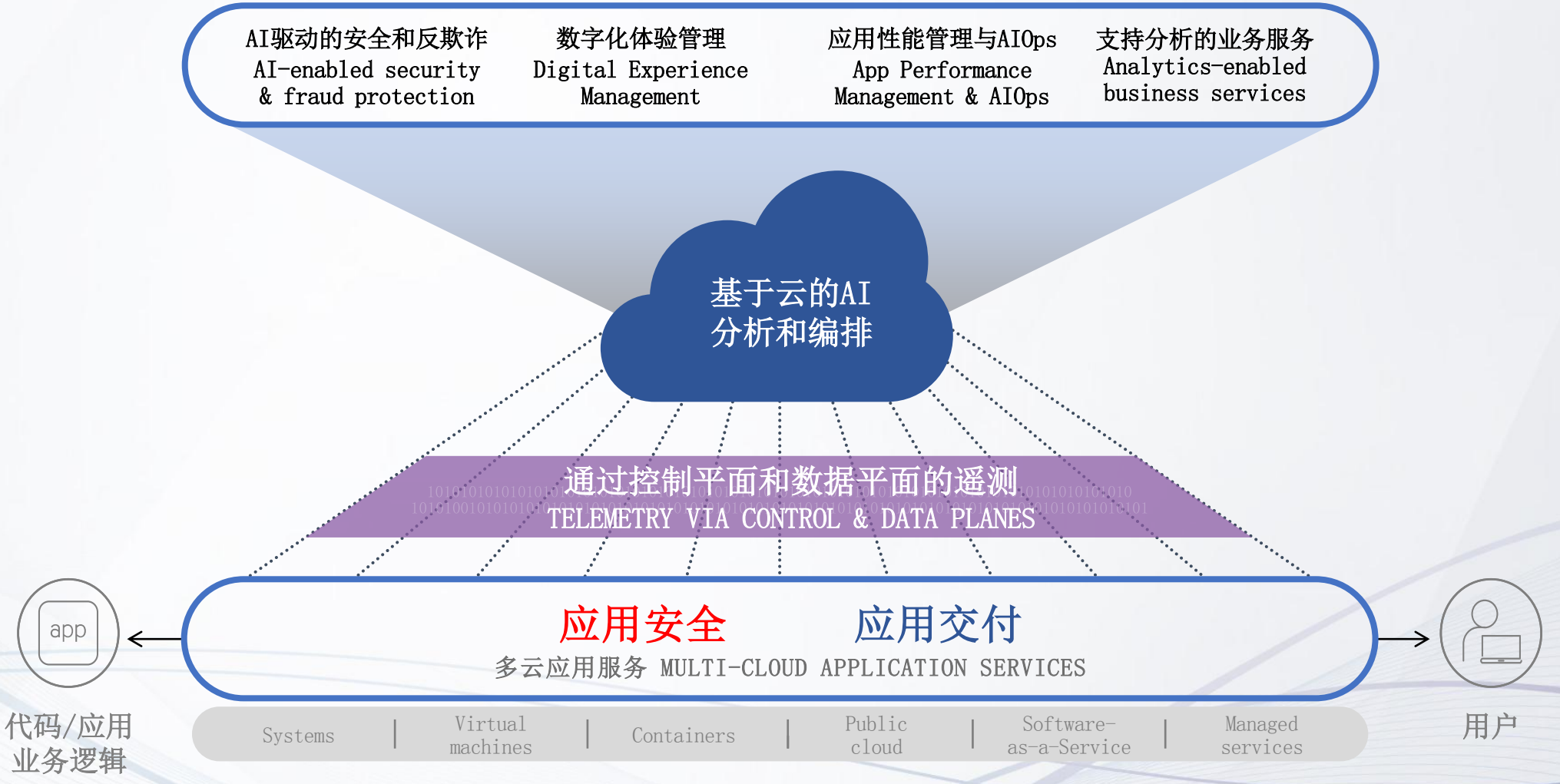



一次糟糕的经历后，用户将停止与自己喜欢的品牌开展业务

of all customers would stop doing business with a brand they loved after one bad experience

# 感知可控，随需而变的应用

Adaptive applications require that application services be automatable, with consistent policy, multi-cloud, and intelligent

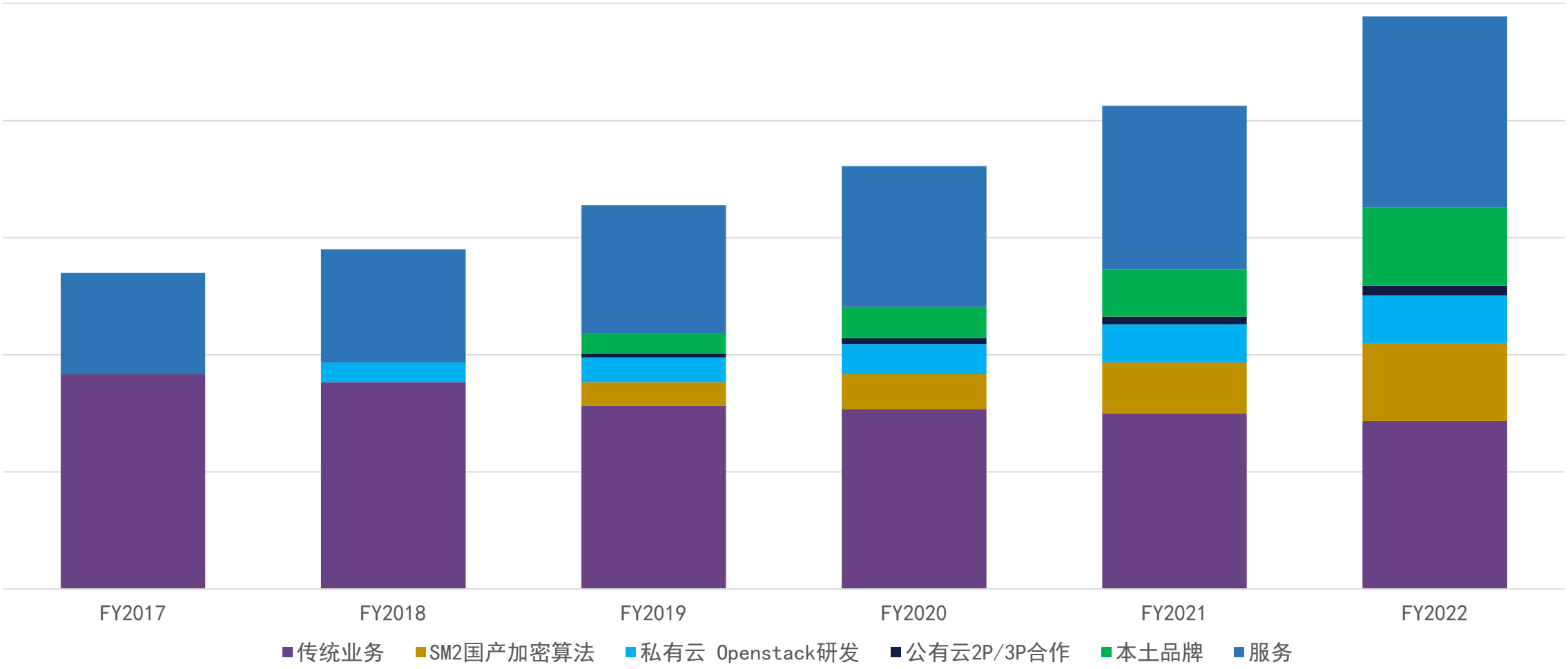


# 通过自研，收购来实现基础能力




# 投资研发适合中国的产品与方案





# Why F5

## 4亿

权威机构的统计和预测，2020年全球有12亿左右的Web service，其中4亿左右由f5公司的各种产品提供服务，是目前科技公司中覆盖最广泛的技术之一

通过大量的客户服务，f5累积了丰富的经验，服务能力，配合对技术发展的趋势判断，是最佳帮助客户实现Adaptive Applications的选择

## 1亿

2020年，在中美贸易，疫情等各种负面市场因素的影响下，f5在进入中国市场20周年后，实现了历史性的突破，正式超过100M USD，成为在中国市场上的中大型外资企业

客户遍及电信，金融，政府，企业，互联网等主要行业，营收，核心技术人员，服务能力体系都远远超过国内各友商

## 1秒

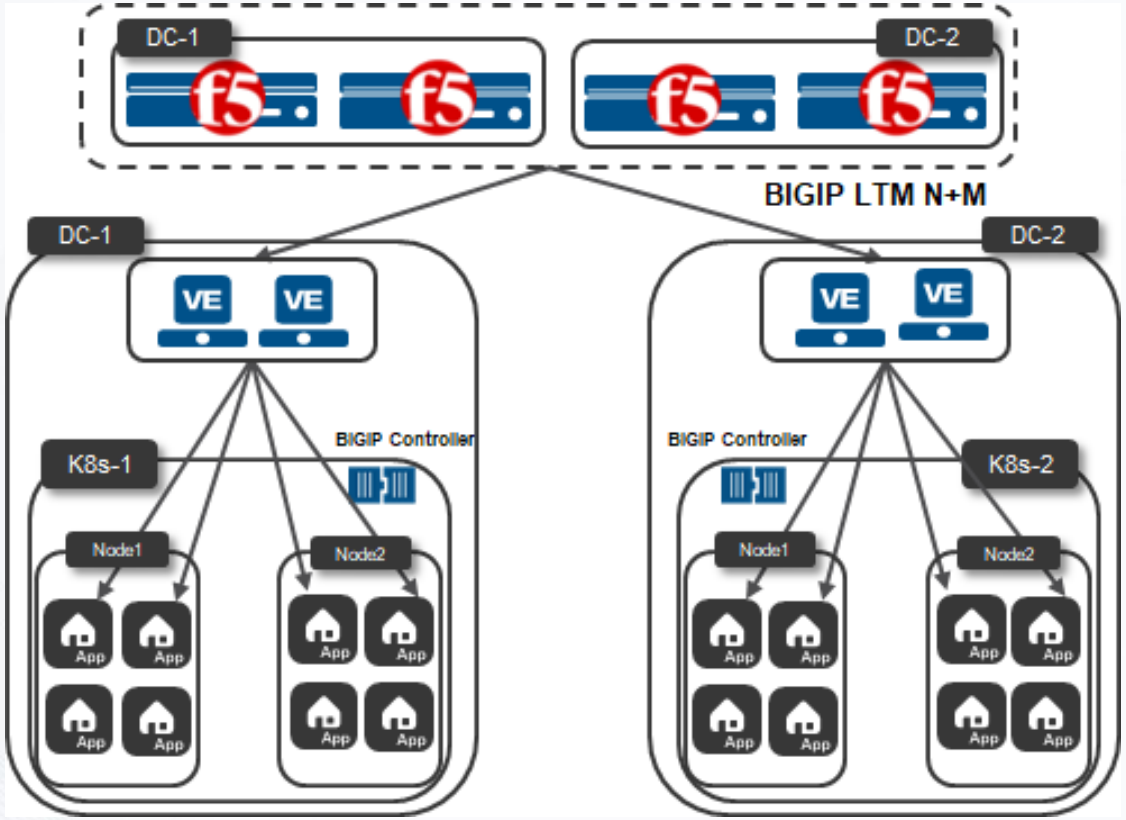
客户的实际测试表明，通过f5实现的Telemetry 无探针超热流数据采集技术，实际延迟为毫秒级别，是真正的T+0 的实时流数据

对比传统超过分钟的延迟，将超热流数据最为大数据的一个全新研究对象，成为AIOps和实时风控的稳定，准确，实时的数据源

# 在多云多活环境中的整合应用交付


| PaaS平台的多云多活 | 多活国产化分布式数据库 | 应用深度检查与故障自恢复 | 智能DNS服务保证5个9的可用 | 多云多链路资源池 |
|---|---|---|---|---|
| • 基于DNS或IP的K8S多中心多活<br>• 多中心与POD内均衡分发与高可用 | • 腾讯 TDSQL，开源的TiDB等国产化分布式数据库支持<br>• 实现同城跨园区的扩展与高可用 | • 模拟用户访问过程，确保应用可用<br>• 发现故障时触发自动化任务脚本，恢复后台应用 | • 应用的可用性探测保证99.999%的应用可用性，<br>• 就近性探测提升用户体验 | • DC ID保证在多云环境中，客户接入方式变更都能保证业务持续 |

# 基于IP的K8S PaaS平台双中心部署




## 用户需求分析：

- 用户的传统业务已经实现了双中心运行，要求以后的业务都能够支持双中心运行
- 用户部署了单中心基于K8s的PaaS平台，但基于K8s的Paas平台本身不支持双中心运行
- 基于业务会话要求，需要支持基于七层session信息的会话保持
- 双中心的K8s集群需要跨中心的高可用性和流量分担

## 方案优势：

- 通过F5 LTM实现双中心K8s的集群高可用和流量分担
- F5LTM的API接口可以对接用户的自动化运维平台
- VE的部署实现容器内Pod的高可用，并通过cookie会话保持保证容器业务的七层会话保持
- F5 VE的高灵活扩展性保障K8s集群的扩展。
- F5的CIS方案实现VE和K8s集群的自动化对接
- F5在传统双活数据中心方案中的经验，保证在Paas平台多中心方案的顺利实施和运行

## 客户收益：

- Paas平台的多中心同时运行，保证了业务的高可用性
- F5的多功能配合容器的灵活性，提升了用户业务的灵活性。
- F5在传统环境和Paas环境的整合方案降低了用户的管理成本，简单的运维方式，提升了运维效率，降低了故障排错时间。

# 在多云多活环境中的全过程应用安全


### 基于AI的反欺诈

- 基于AI实现对于机器人／人工撞库防护，滥用授权，伪造账户等新型攻击
- 仅去年就成功阻止了金额总值超 10 亿美元的欺诈行为

### 自建WAFaaS

- 利用公有云VPC实现自建DDOS防护，WAFaaS，CDN服务
- 实现弹性攻防架构，降低Capex，按需付费

### SSL 自动化编排

- 基于SSL的服务自动化编排
- 低交互协议蜜罐
- 基于用户异常的大数据筛查预警，动态引流对抗工具。

### DDOS 攻击防护

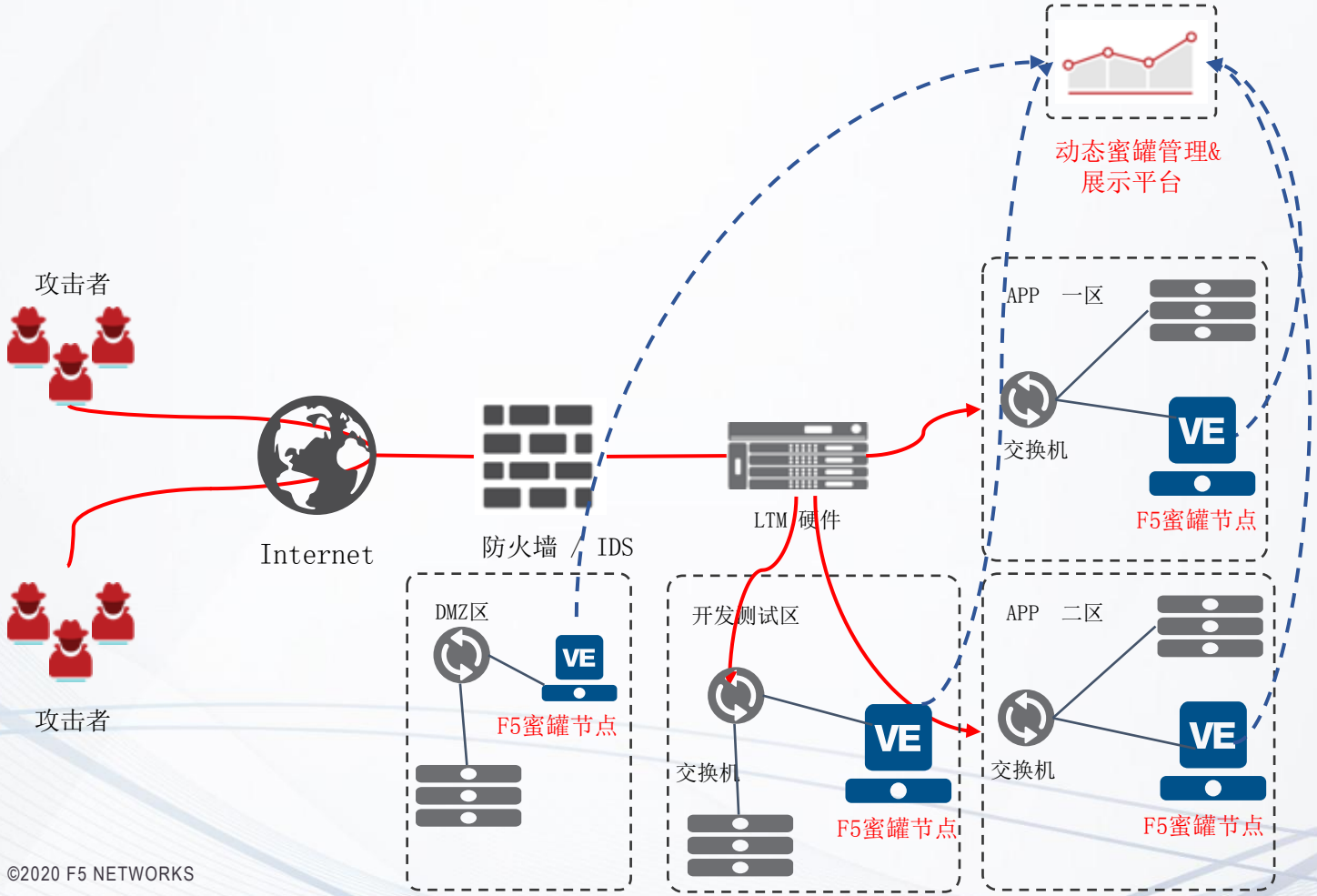
- 网络，应用层攻击的DDOS防护，特别是过库／重载类应用防护，
- 基于机器学习的用户行为判断，天网／地网结合防护。

### 零信任架构

- 内外网用户，代理商等不同用户的认证，鉴权
- 全过程加密传输
- 与应用紧密结合的统一登陆认证

# 护网攻防利器：全覆盖低成本蜜罐

低交互协议蜜罐： 常态化，以高性能，全网覆盖为特色，基于用户异常访问的大数据筛查预警，动态引流对抗的工具。




# 应用可视化与自动化，攻防过程的利器

基于云的AI分析和编排
来实现应用洞察与自动化

### 一键配置，一键变更，一键容灾

- 预先验证，基于场景的一键式配置，割接，容灾处理
- 分钟级别实现数据中心或应用切换，降低RTO，降低故障级别

### 多云环境的自动化管理

- 中国研发中心为中国客户定制，基于Openstack私有云或公有云的自动化
- 开源，可选厂商服务保障

### 交易过程可视化实时风控数据源

- 提供T+0的现网流数据，采集过滤和格式转换后与风控平台紧密结合
- 实时，全量，超级精准的数据源

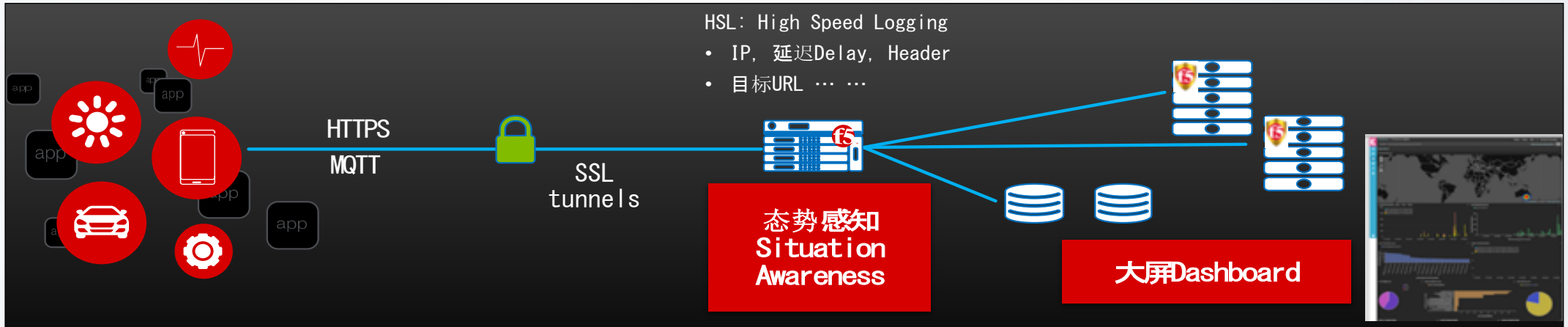
### 主动拨测的应用状态判断

- 免开发自建拨测节点，
- 模拟用户访问拨测确认应用可用性与性能
- 与CI／CD集成，简化变更验证与灰度发布。

### Bigdata Engine大数据引擎

- A,B,C,D,E
- 通过AI和Bigdata大数据的机器学习，在Cloud云环境中实现DevOps的可视化，来提升用户体验user Experience

# Bigdata Engine ： iRules+HSL
# Telemetry ： 无探针的实时应用Streaming – 超热流数据采集

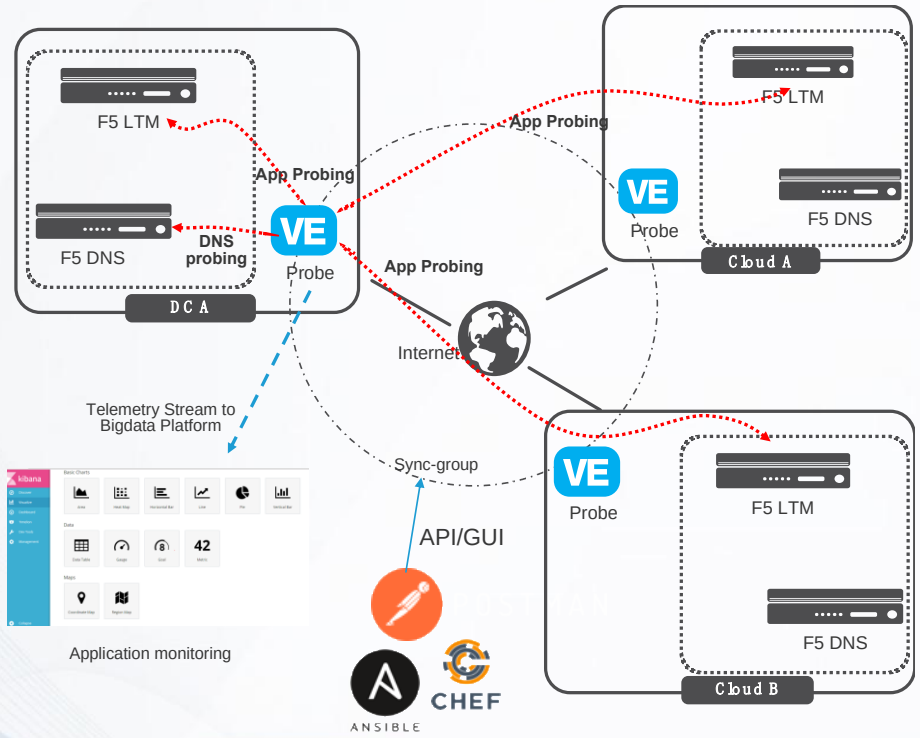



| 用户／网络体验监控<br>User experience /Network Performance Management | 用户行为分析<br>User Behavior analyze | 应用性能管理<br>Application Performance Management | 财务语言谈DC运营<br>Data Center KPI |
|---|---|---|---|
| • 根据用户网络体验的地图来快速发现和定位问题，是用户，数据中心还是应用。<br>• 用户网络体验均值评分，设立形容词到量词的转换，参考行业均值设定预期目标。 | • 用户源IP地址导出全球／中国热力地图，并可以Drill down 钻取到单一用户网络体验<br>• 目标URL的/Search，/Items，/payment等就是登陆，搜索，产品详情，支付等客户留存 | • 服务器的TCP窗口，首包时间实际就是每个东西流量API调用的次数，性能体现。<br>• 突发的API调用提升，根据趋势预测调用API FW的连接限制，保障系统可用 | • 数据中心追加投资加一年努力，如何证明价值：<br>• 历史主营业务的可用性提升验证97% ～ 98%， 1%的提升参考月活和ARPU，可以计算增加多少营业额，数据中心运维的价值<br>• 用户体验的多链路应用路由，可验证的用户体验提升，投资效果可见 |

# DevOps – 主动拨测，攻瘫前的预警

for CI/CD grey release by telemetry stream

云化的应用运行环境需要更多的应用监控，特别是主动拨测，减少配置变更和应用灰度发布后的业务确认




F5 Solution:

- 与客户的研发部门合作确认每个应用的probing point: domain, port, URI, parameter
- 通过VE 的自动健康检查工具来模拟客户的访问过程实现主动拨测
- 把拨测结果通过Telemetry stream out 给后台的bigdata platform
- 作为应用的校验工具，与客户的CI/CD grey release process紧密结合

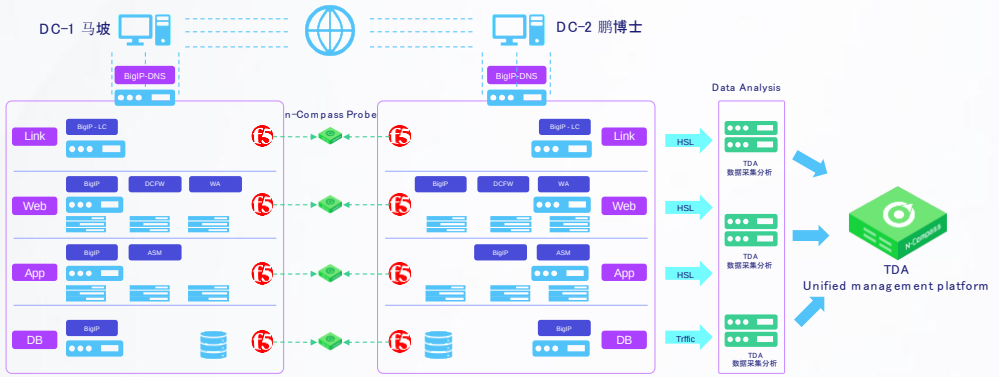
为客户带来的业务价值:

- 在不需要应用打点log和字节码注入的情况下实现运行监控，提升应用可视化
- 与CI / CD整合实现在灰度发布前后的应用校验与应用性能变化，将传统网络工程师的作用提升接近为SRE – Site Reliability Engineer

# AIOps- 关键业务过程追踪，被攻击API的根因分析

Application deep tracing,
root cause analysis by AI, “1 key fix“ automation tools

关键应用的API访问可视化需要提升，来提高客户投诉后的快速判断，自动发现问题和“一键”解决



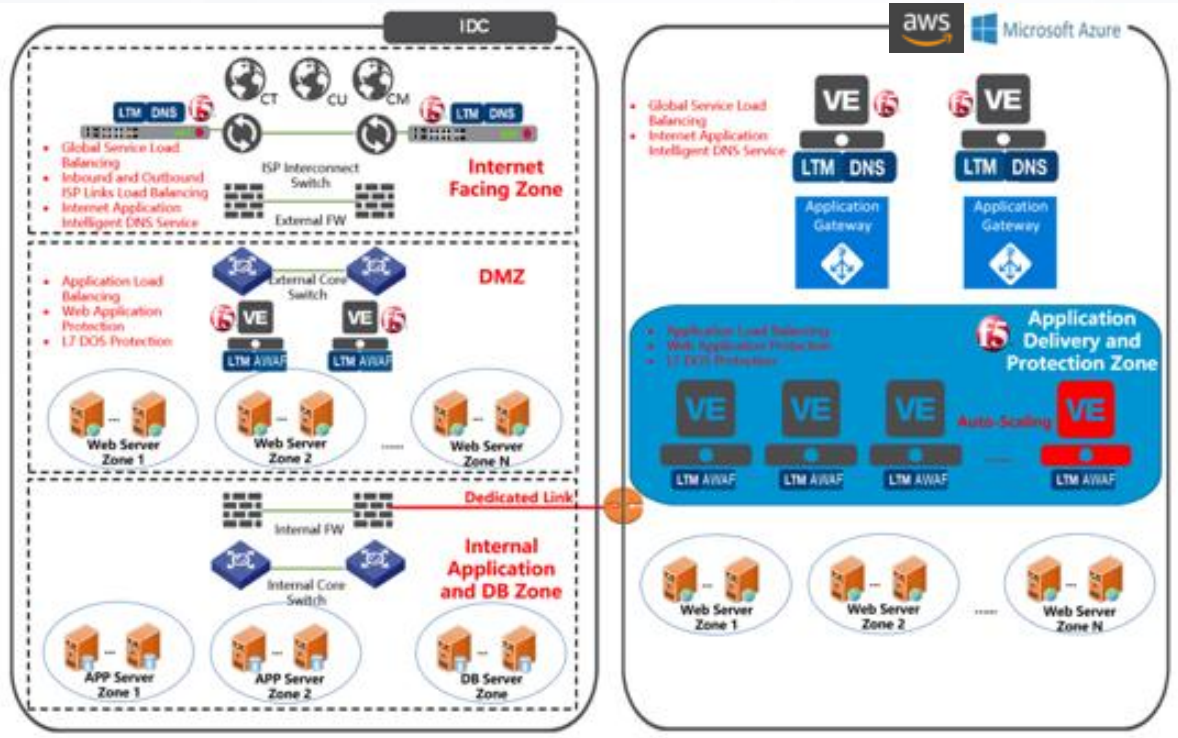

F5 Solution:

- 和n-Compass合作构建“Application Command Center”
- 通过f5的实时无探针数据采集telemetry技术，与 n-Compass的机器学习结合，在客户访问性能下降投诉前提供智能预警
- 自动发现应用API调用的逻辑关系，并通过AI的根因分析来发现问题根源
- “1 key 配置 / 变更”在客户投诉前解决问题。

为客户带来的业务价值:

- 在客户投诉前预警，并快速发现问题根源，提升用户体验与降低故障恢复时间
- 利用自动应用调用拓扑能力与互相调用的次数，性能能指标，实现应用可视化视图大屏，提升传统网络运维到与应用结合的应用运维

# 攻防架构，天网+地网（Private WAFaaS）+AI




Customer Challenge ： 利用天网的公有云清洗和安全服务在应用识别和定制化上有待提升，引入更加灵捷与定制的地网-私有WAFaaS服务，和用户行为分析与判断的AI 迫在眉睫

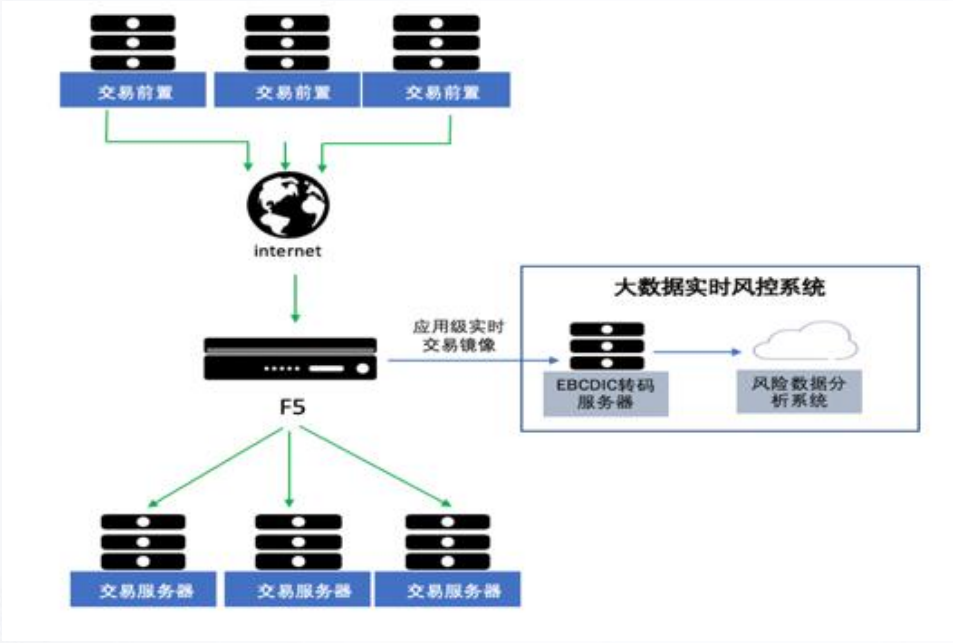
Solution: GTM, LTM, VE AWAF in multi-cloud VPC.

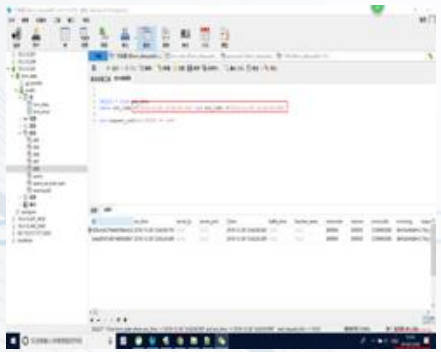
客户可以利用多云VPC自建私有部署的CDN，AWAF构成地网平台；并依托f5的大数据引擎Telemetry技术实现无探针数据采集技术，通过Data lake与AI实现智能判断，并通过API控制f5实现基于应用灰度／用户类型的在线应用路由

Customers feedback:

我主要是喜欢这个方案的ROI，利用公有云的VPC技术，低成本构建私有化CDN与AWAF防护平台，投入成本和运营成本都很低，但能够实现弹性与定制的防护体系。

# 业务安全：实时风控数据源



Customer Challenge ： 客户的信用卡系统，希望不动现有架构，并保障数据安全的情况下实现新的风控管理

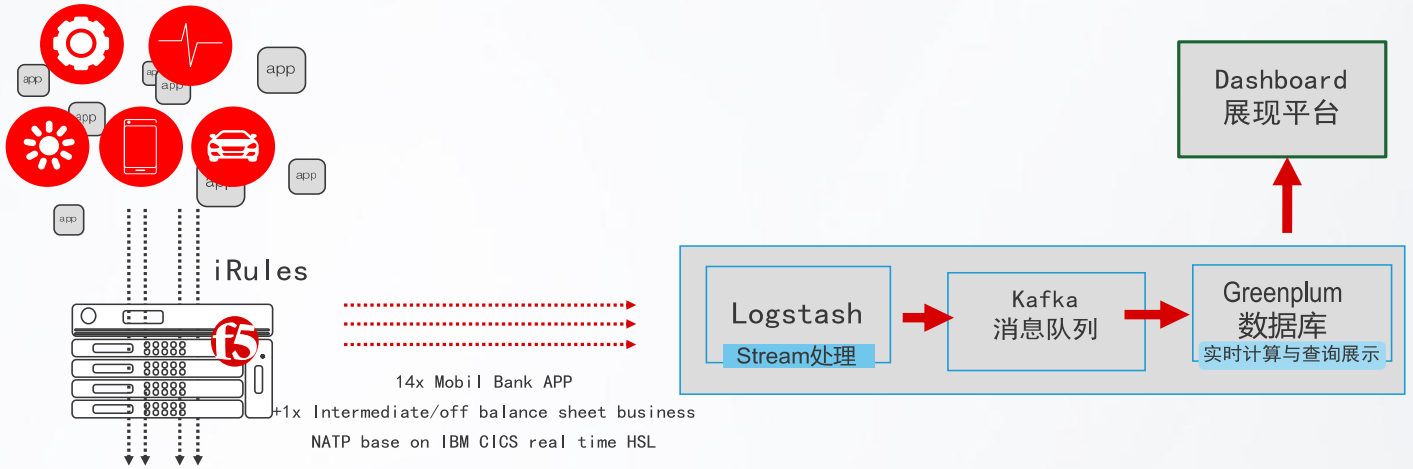
Solution: VE with iRules, HSL， Telemetry streaming

客户利用现网f5来实现无探针的数据采集，解码，并重新编码为后台需要的Json format，把应用信息提取给后台的大数据与AI平台

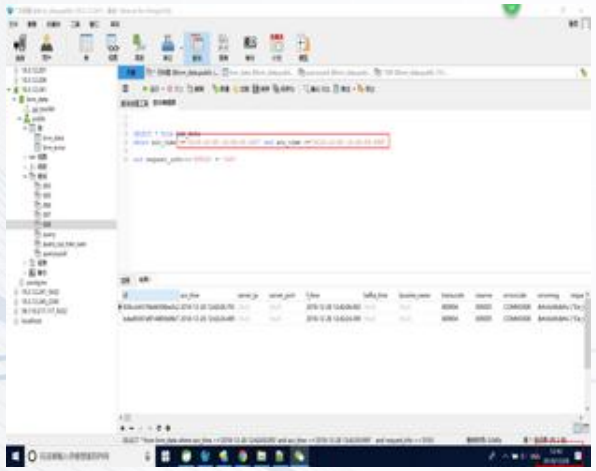
Customers feedback:

1. 测试表明，这是真正的“超热T+0”实时数据源
2. F5的工程师健健，帮忙优化iRules，提升了采集准确率100% hit from 99.99%,
3. 这才是自主可控，iRules代码咱们的工程师就可读，可改，对比传统NPM技术依靠付费的厂商应用识别，可是一大进步

# 客户的报告：采用f5作为无探针的应用大数据采集




**真正实时T+0 的数据，对比1分钟延迟的NPM BI/BPM**



**可读可改的 iRules 代码**
**没有额外为应用定制标识的成本**

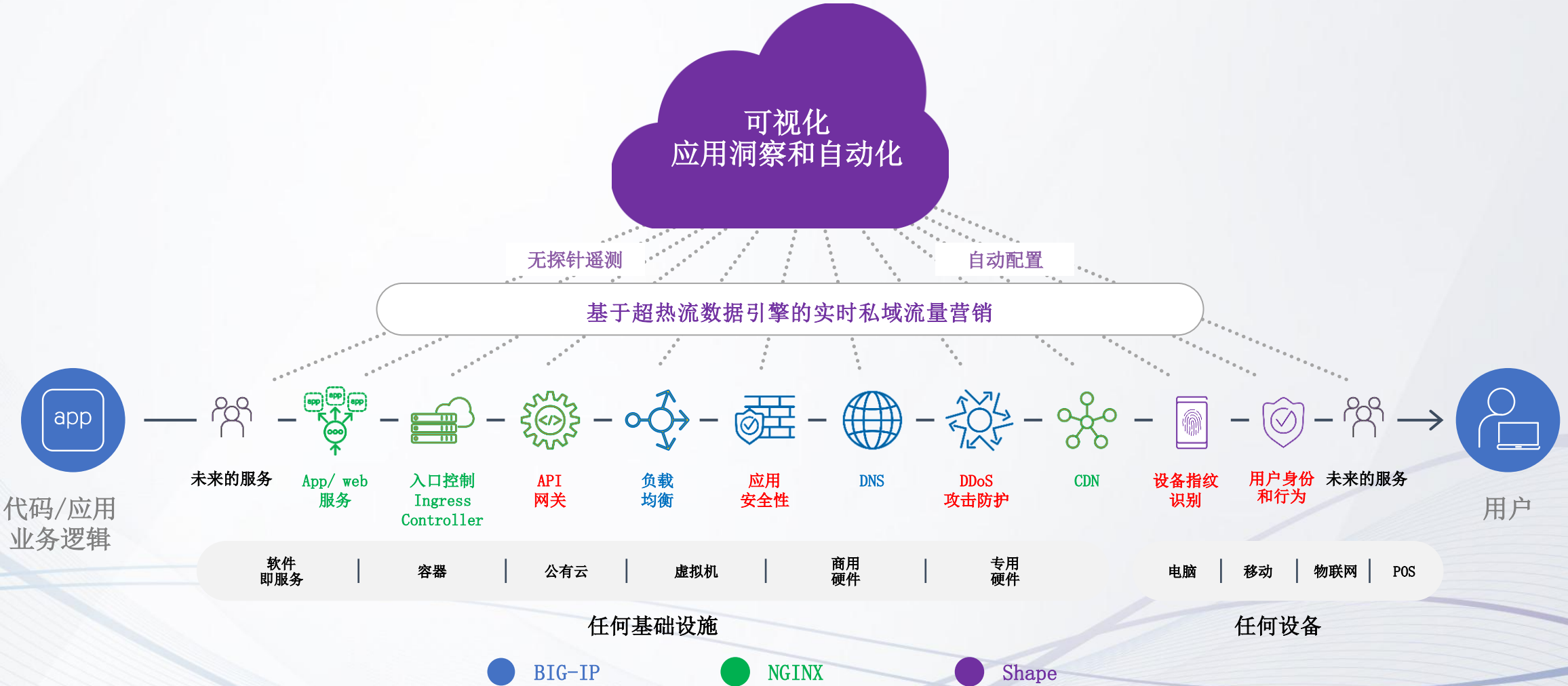
```
when RULE_INIT {
            set static::payload_dbg 1
            set static::max_collect_len 4999
            set static::hsl_pool
"my_hsl_udp_pool"
```

**支持 90%以上的银行应用**
**Native App, H5/WebView, B/S, C/S**

```
Global parameter TCP/HTTP/UDP protocol compliance
   verification

Client Side / Server Side :
         TCP    XML/FTP/Socket/TNS    Mobil App
         http     html/Json/Node.js/XML/JSP   Online
   banking
         UDP    DNS service
         ISO8583    dedicate for China Union pay
         MQ    FTE   PBOC support
         Tuxedo  WTC/WSL  Old core banking

Output: HSL Json / Syslog / XML

Alert: HSL W3C/syslog/Json/XML
```

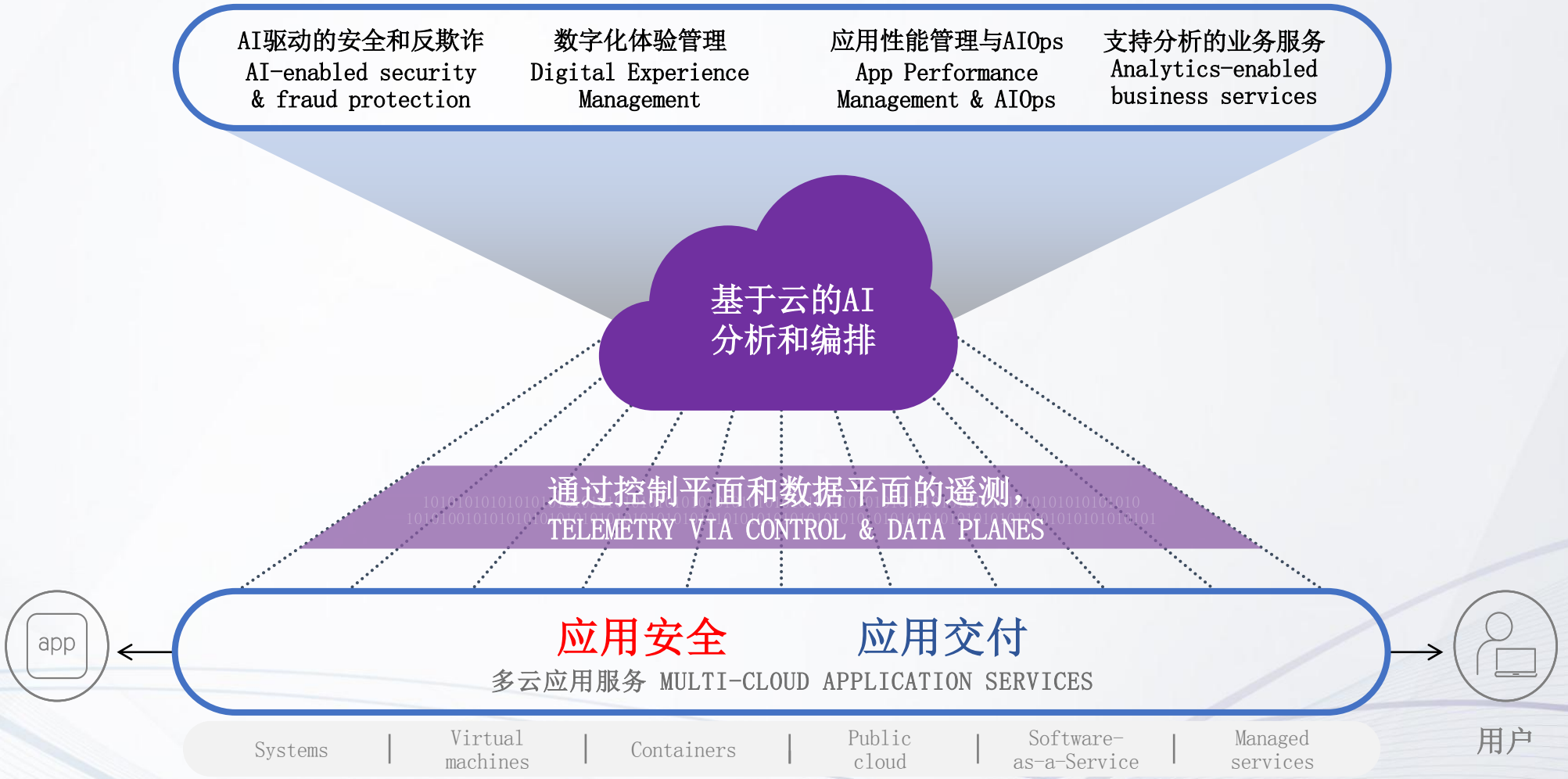
F5 以代码到用户的全数据路径应用服务为基础，通过telemetry 无探针的关键应用信息采集技术，与Data Lake&AI合作，通过超热流数据的私域流量营销 ，来实现可用，安全，应用的洞察与自动化，

# 帮助客户构建 Adaptive Application 感知可控，随需而变的应用



# 感知可控-随需而变的应用

Adaptive Applications require that application services be automatable, with consistent policy, multi-cloud, and intelligent



网络安全创新大会
Cyber Security Innovation Summit

# THANKS

吴静涛 Fred WU
F5大中华区首席技术官
f.wu@f5.com