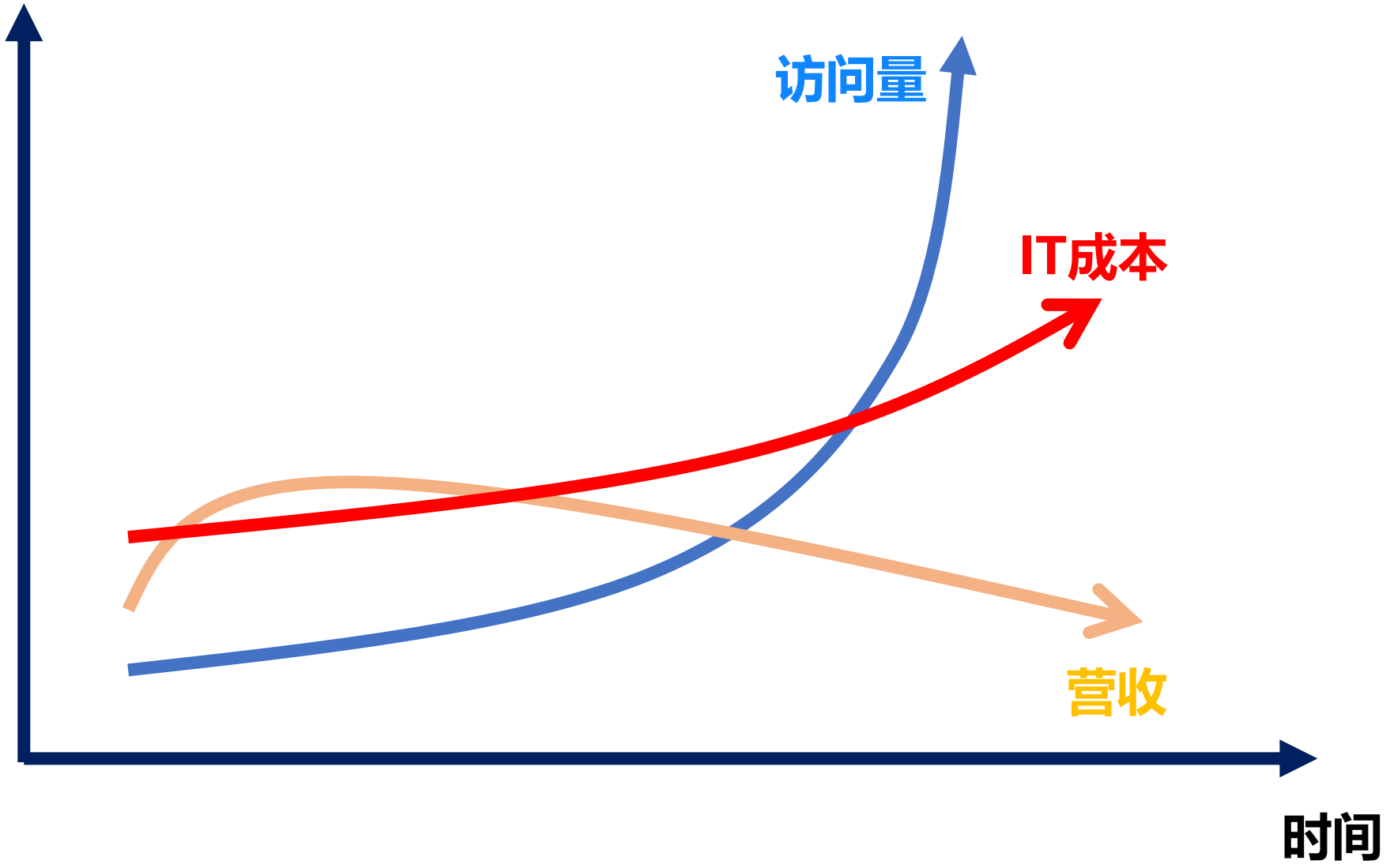
# 基于加密流量精分策略的安全业务优化

陈玉奇
F5安全业务经理

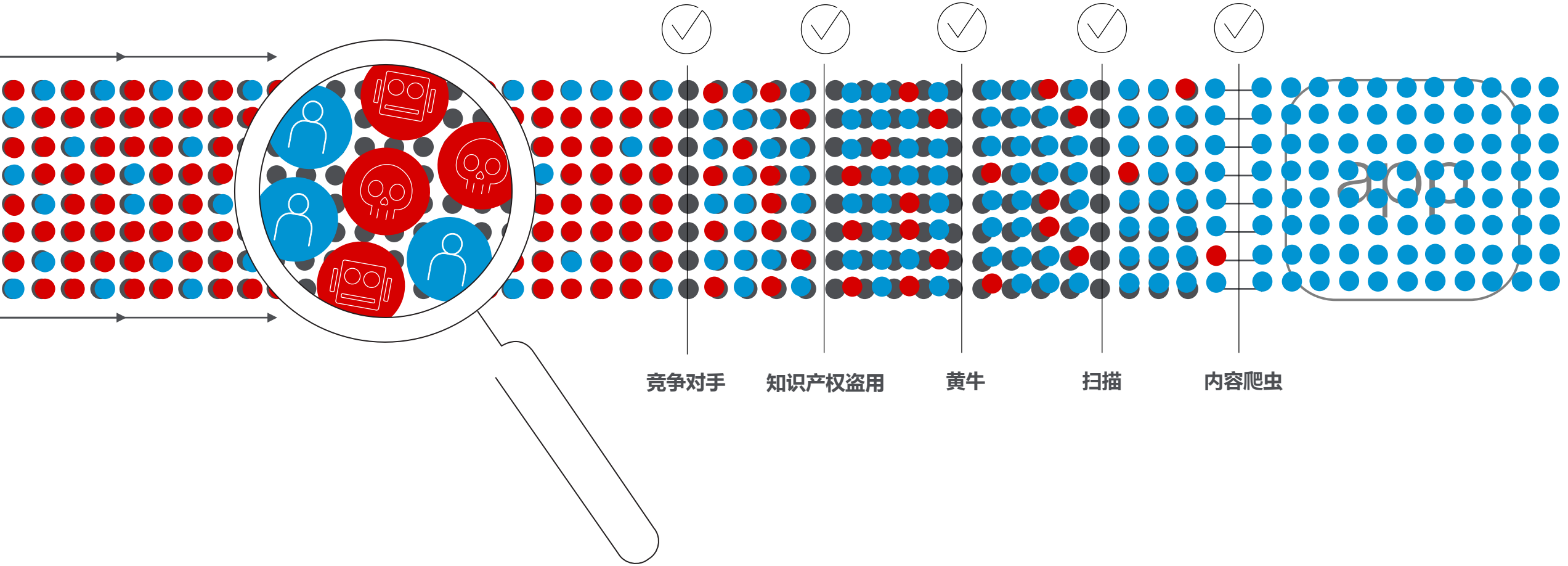

“安全
脱离了个人英雄主义的年代”

# 乐观的客户场景



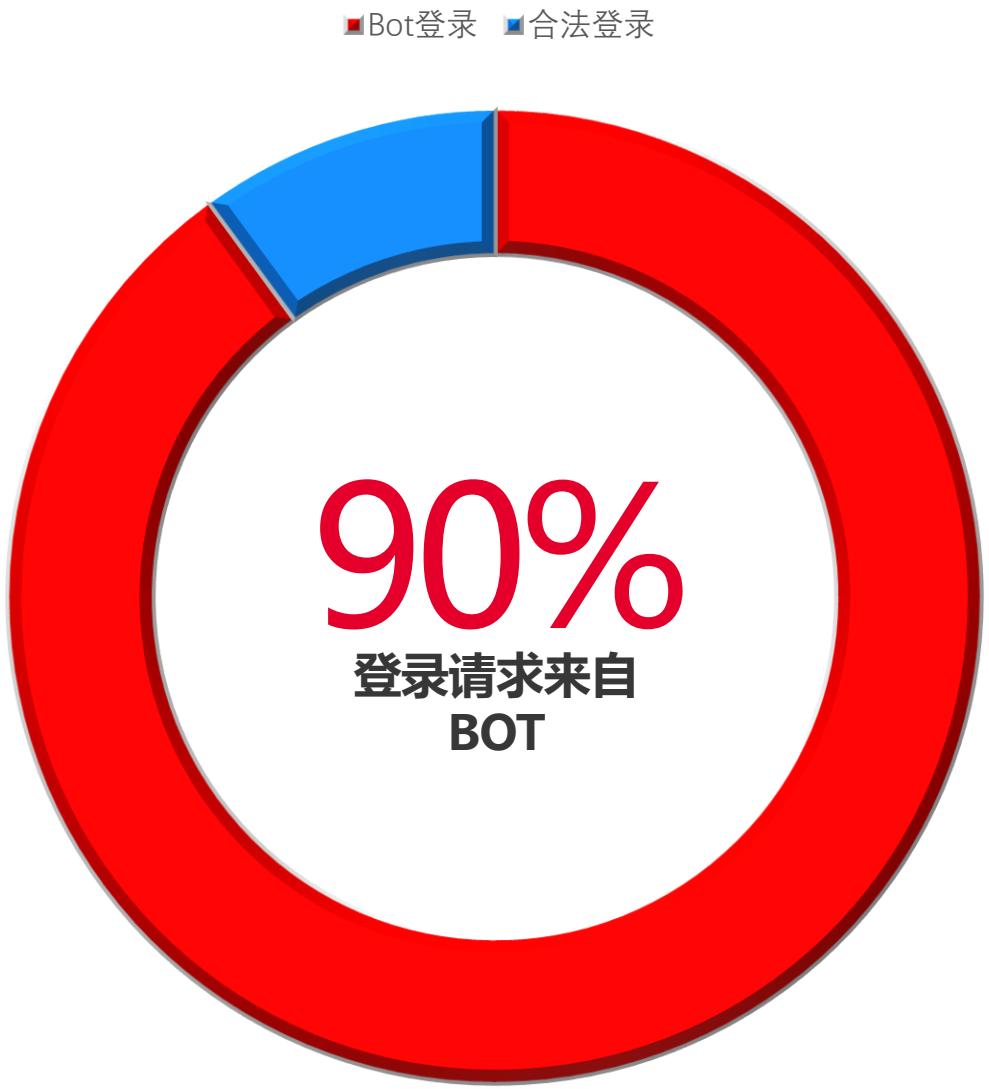
# 您的投入为谁服务





# 合法登录真的很难

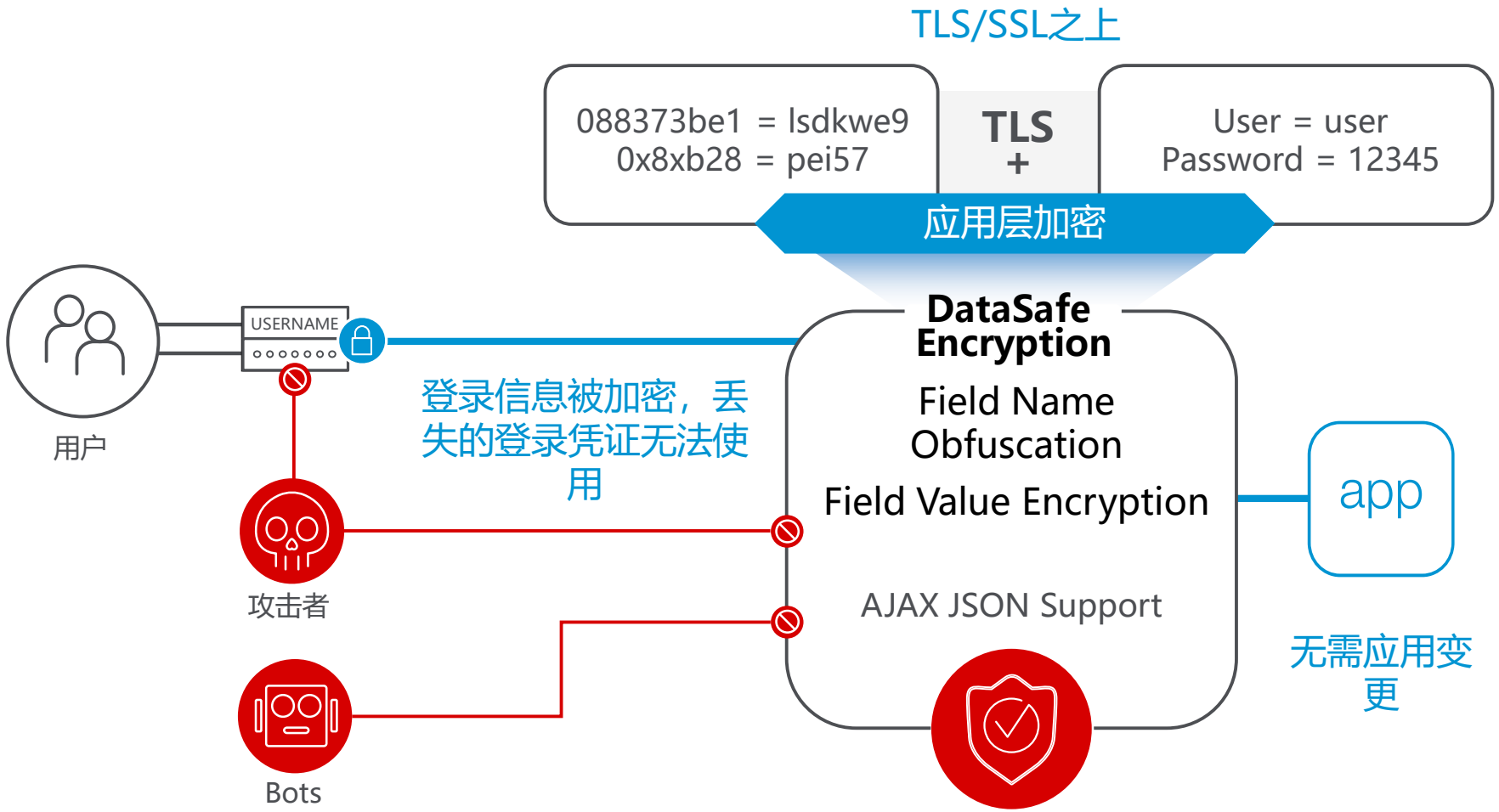





Verizon 2017 Data Breach Investigations Report

# 阻止登录凭证的攻击

- ✓ 应用层加密
- ✓ 混淆与躲避检测
- ✓ 完整的撞库/暴力破解防御



# 机器人是业务巨大的威胁



**50%**

互联网流量来自于机器人

**30%**

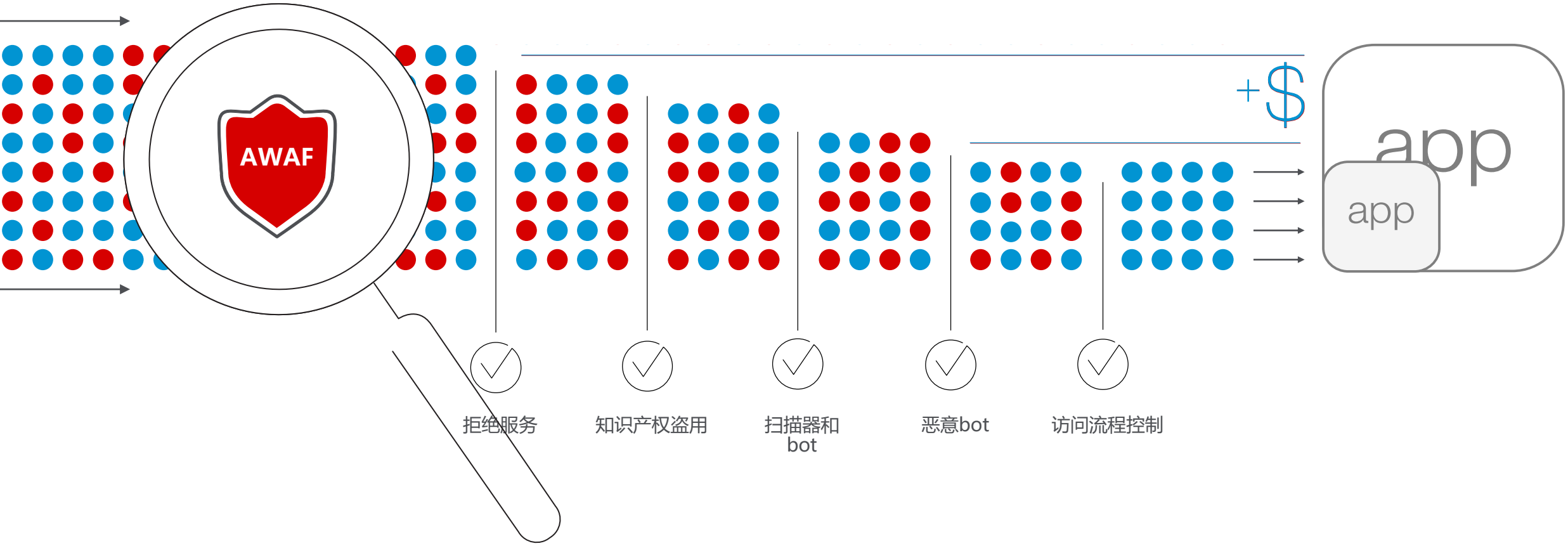
机器人流量是恶意的

**77%**

Web攻击来自于机器人网络

# 全面缓解机器人（BOT）

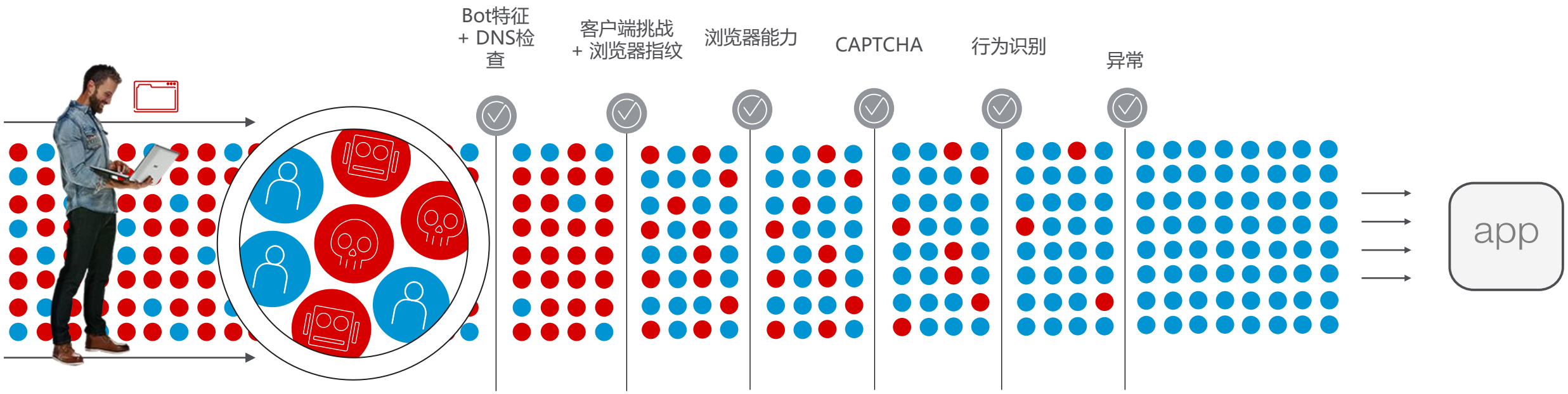




# 阻断BOT的第一个请求



- ✓ 从特征到行为分析的多维度分析处理
- ✓ 请求到达应用之前阻断
- ✓ 全代理架构的威力




后端服务器不处理流量


“攻击
进入了万物加密的时代”

**70%**

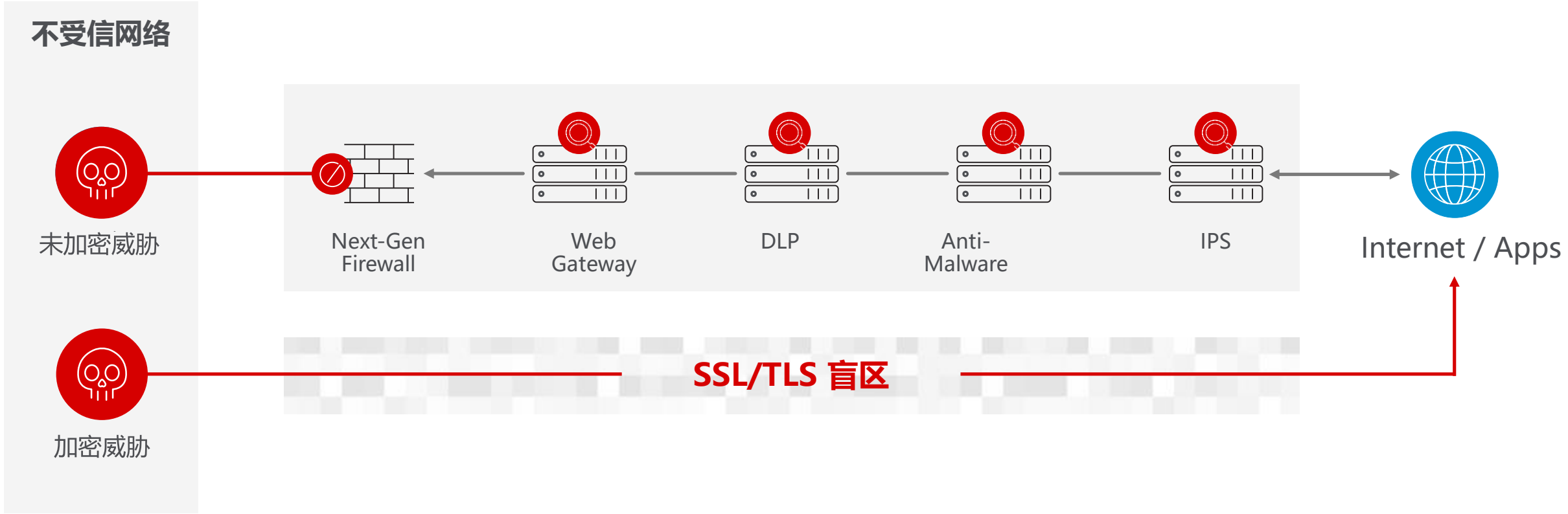
互联网流量是加密的

**80%**

页面访问SSL/TLS加密

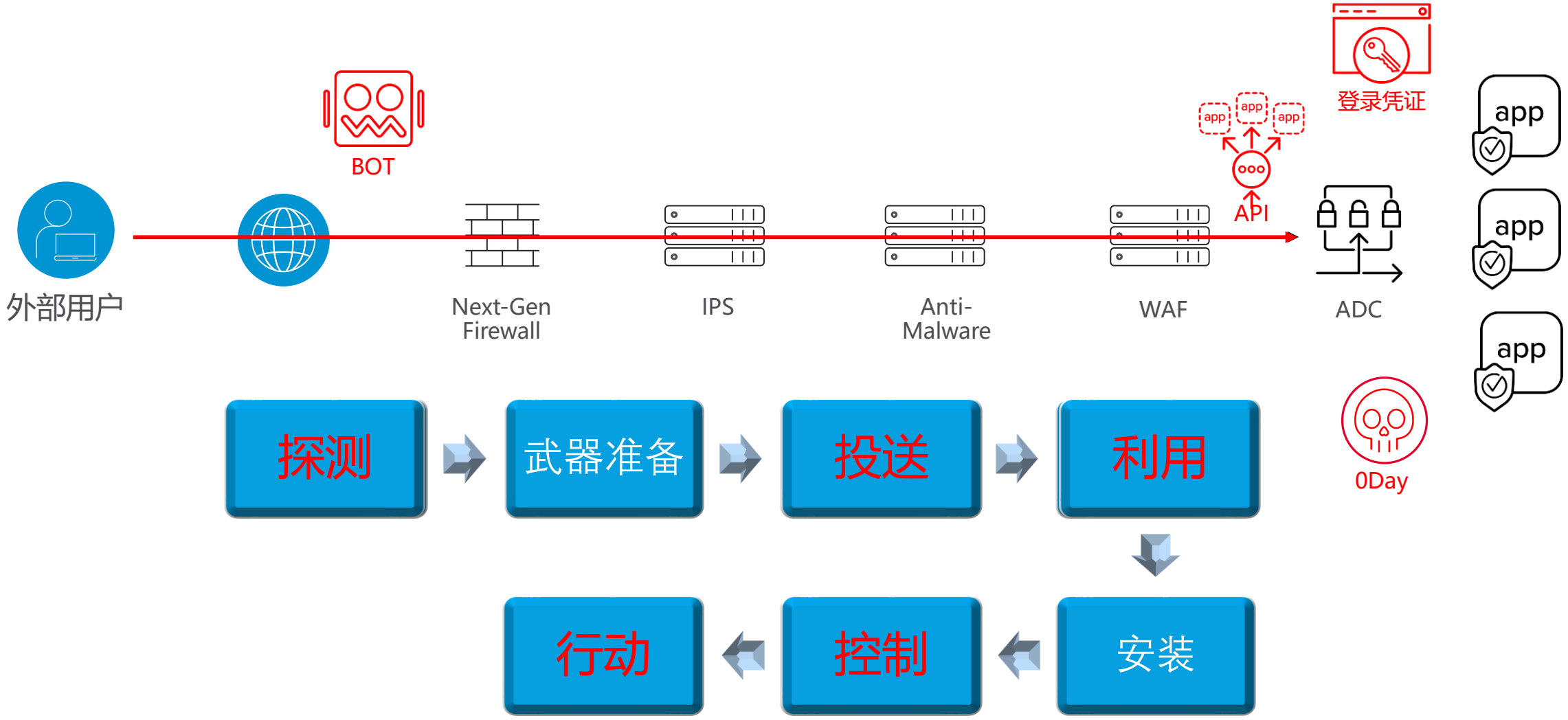
F5 Labs https://www.f5.com/content/dam/f5/corp/global/pdf/products/2017_TLS_Telemetry_Report.pdf

# 安全盲点


不受信网络
未加密威胁
加密威胁
Next-Gen Firewall
Web Gateway
DLP
Anti-Malware
IPS
Internet / Apps
SSL/TLS 盲区

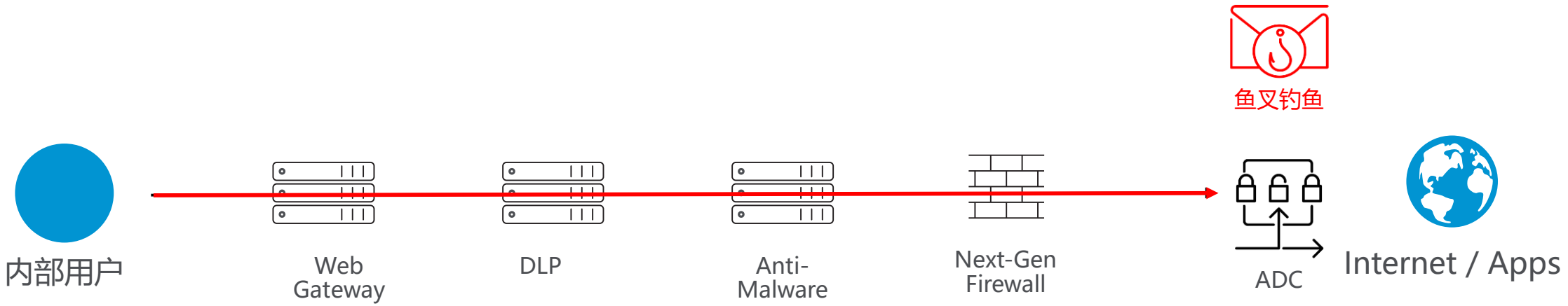
# SSL下面的APT攻击模型





# 水坑攻击与信息泄露

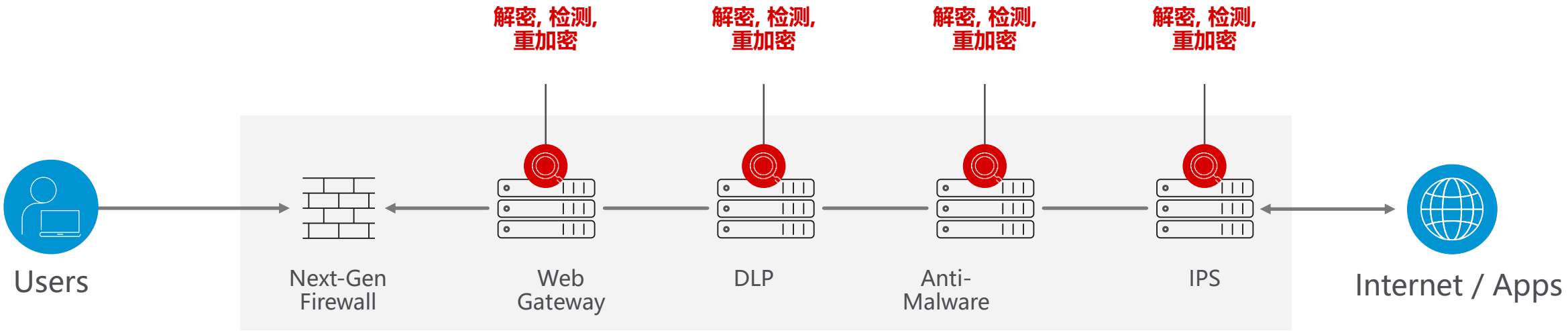



鱼叉钓鱼
内部用户
Web Gateway
DLP
Anti-Malware
Next-Gen Firewall
ADC
Internet / Apps


目标明确
防护薄弱
成功率高
持续生效
利于隐蔽

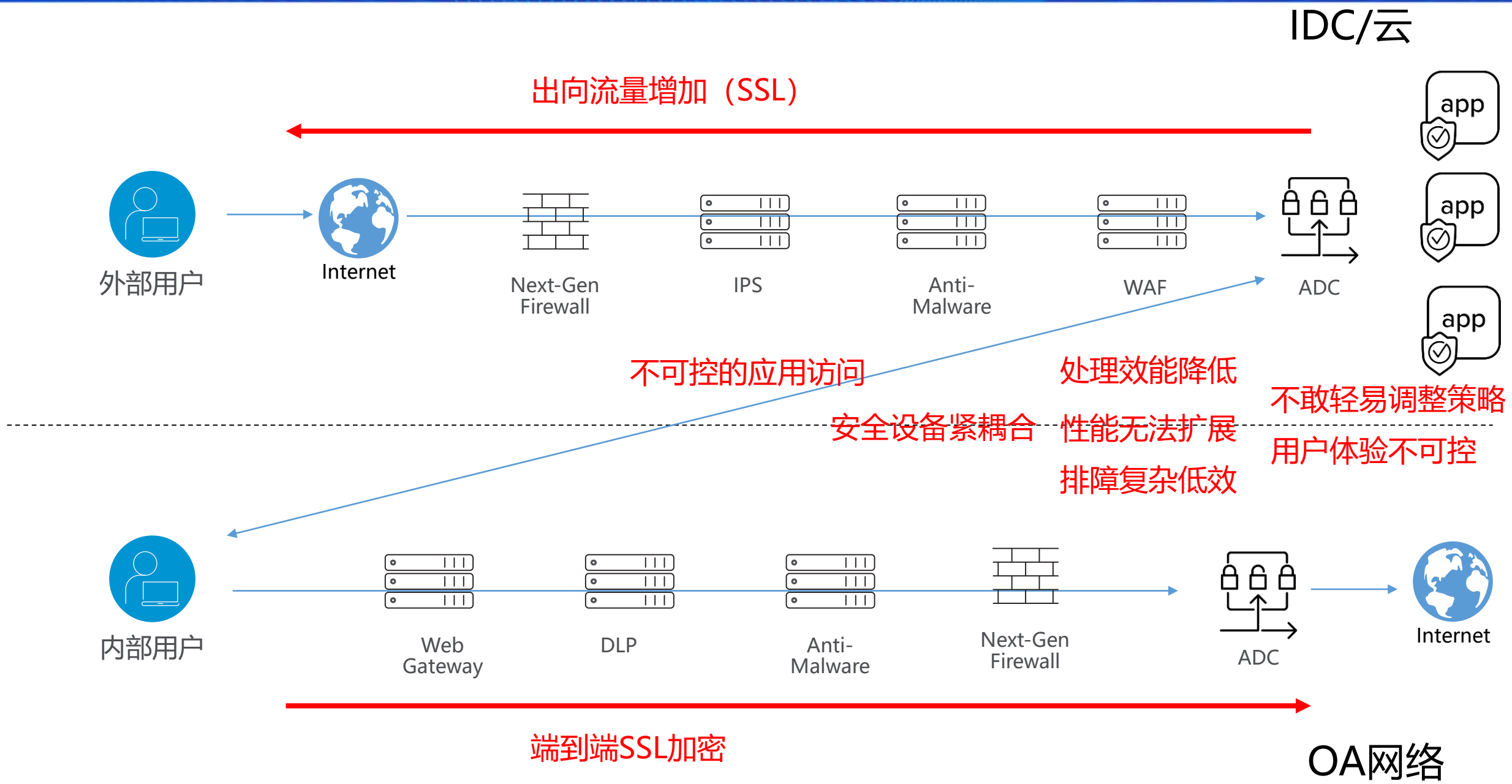
# 菊链——无奈的选择





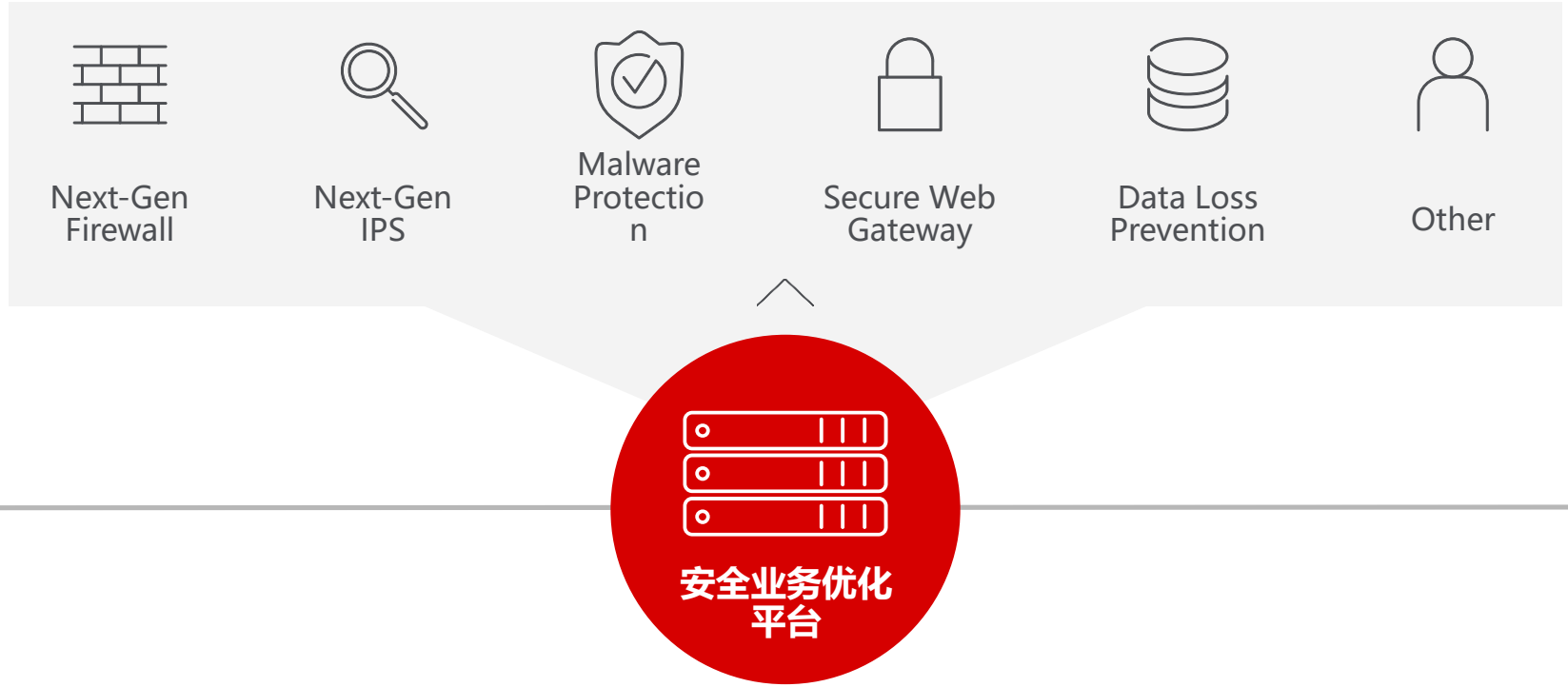

- 部署复杂，排障是噩梦
- 多重加解密，效率低下
- 故障点多，性能低下，可用性低
- 固化的网络，无法扩展

# 企业安全模型现状


IDC/云
出向流量增加（SSL）
app
app
app
外部用户
Internet
Next-Gen Firewall
IPS
Anti-Malware
WAF
ADC
不可控的应用访问
处理效能降低
不敢轻易调整策略
安全设备紧耦合
性能无法扩展
用户体验不可控
排障复杂低效
内部用户
Web Gateway
DLP
Anti-Malware
Next-Gen Firewall
ADC
Internet
端到端SSL加密
OA网络

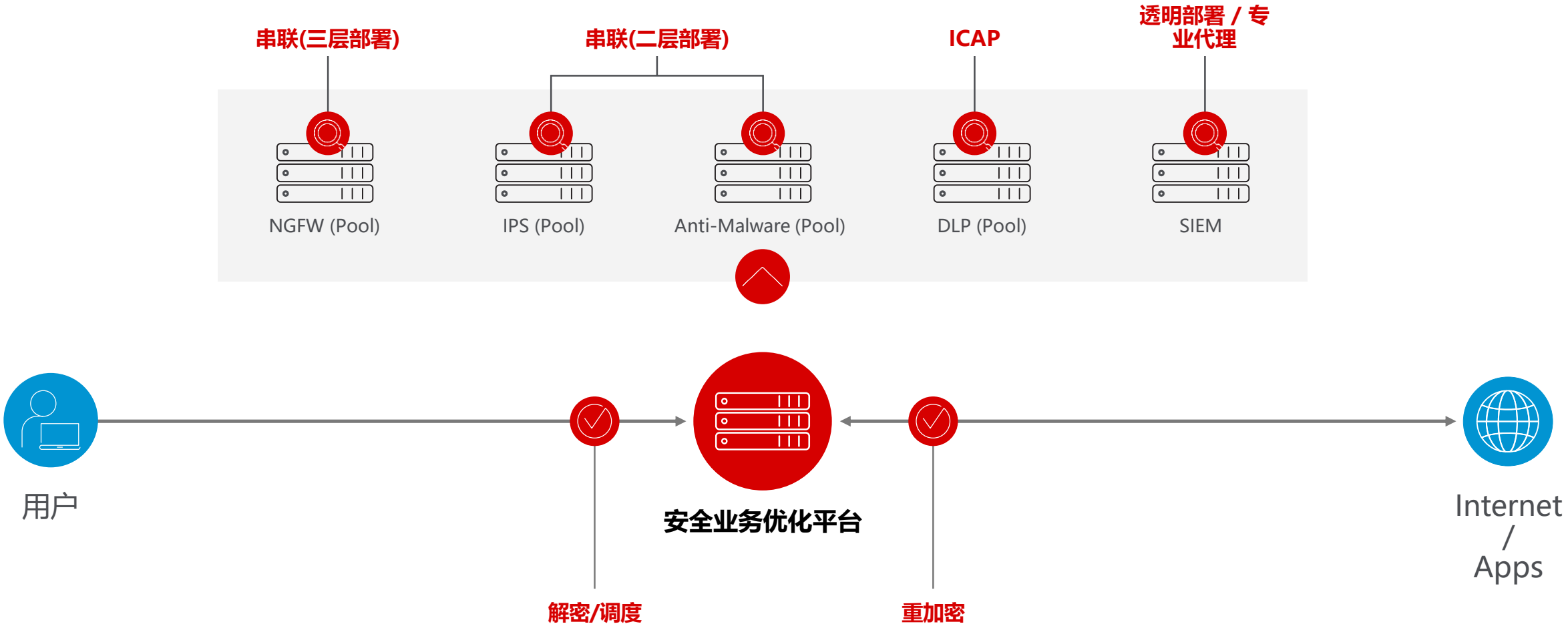
# 安全优化调度

## 针对双向SSL/TLS加密流量的安全业务优化调度



# 优化调度的设备无关性

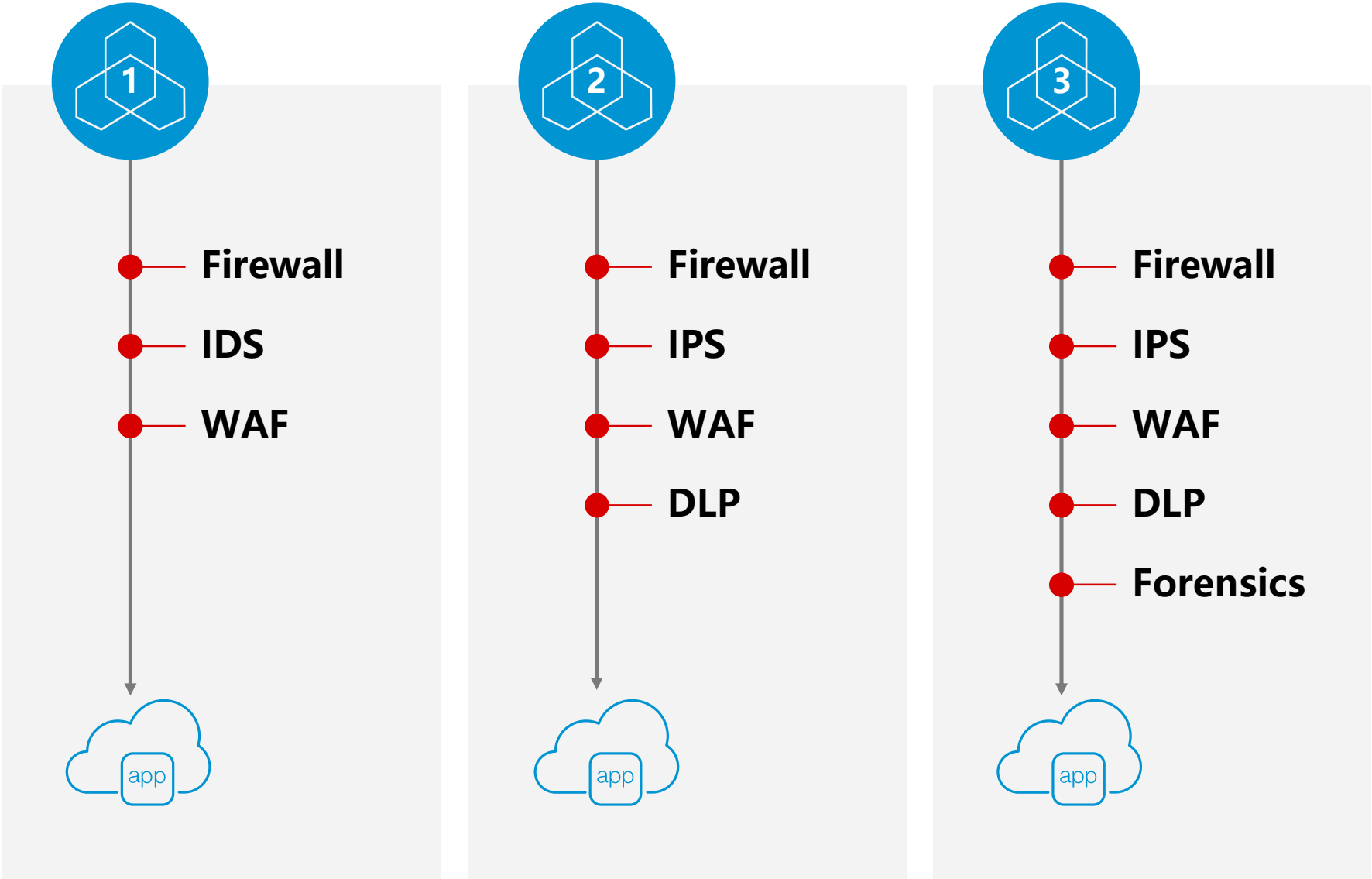



串联(三层部署)
串联(二层部署)
ICAP
透明部署 / 专业代理
NGFW (Pool)
IPS (Pool)
Anti-Malware (Pool)
DLP (Pool)
SIEM
用户
安全业务优化平台
Internet / Apps
解密/调度
重加密

# 优化调度的动态服务链



- ✓ 安全设备动态分组
- ✓ 物理拓扑无关性
- ✓ 最大化安全投资
- ✓ 高度灵活的安全服务的插入、监控和扩展



# 优化调度的策略精分



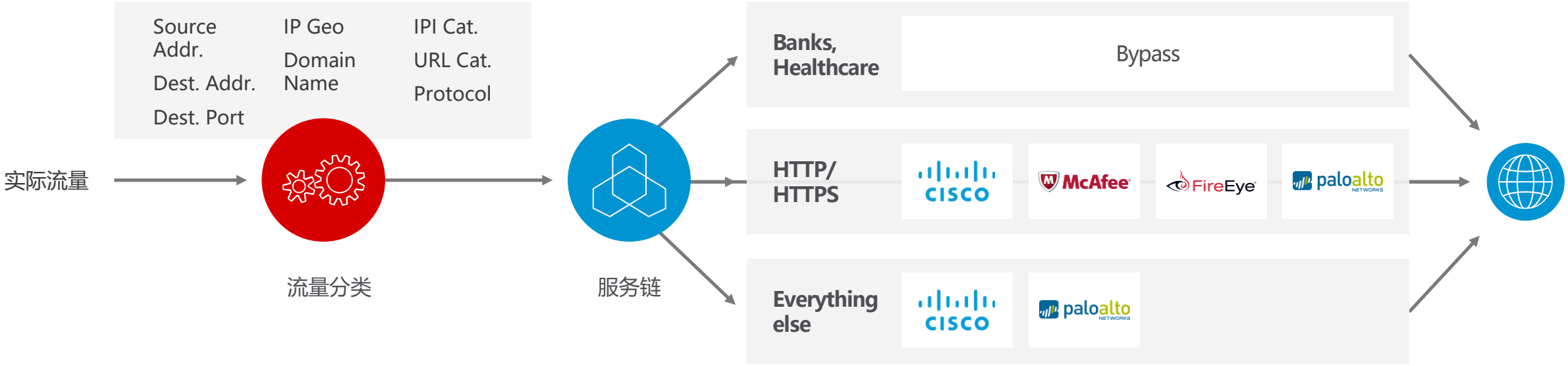
上下文分类引擎

丰富的流量选择

基于策略的解密和流量调度

Bypass, 阻断, 检测等多种行为

高级业务监控和可扩展



# 安全业务优化的普适性

## 超越可视化

解决可视化困境，提升整体安全水平，保护用户安全投资

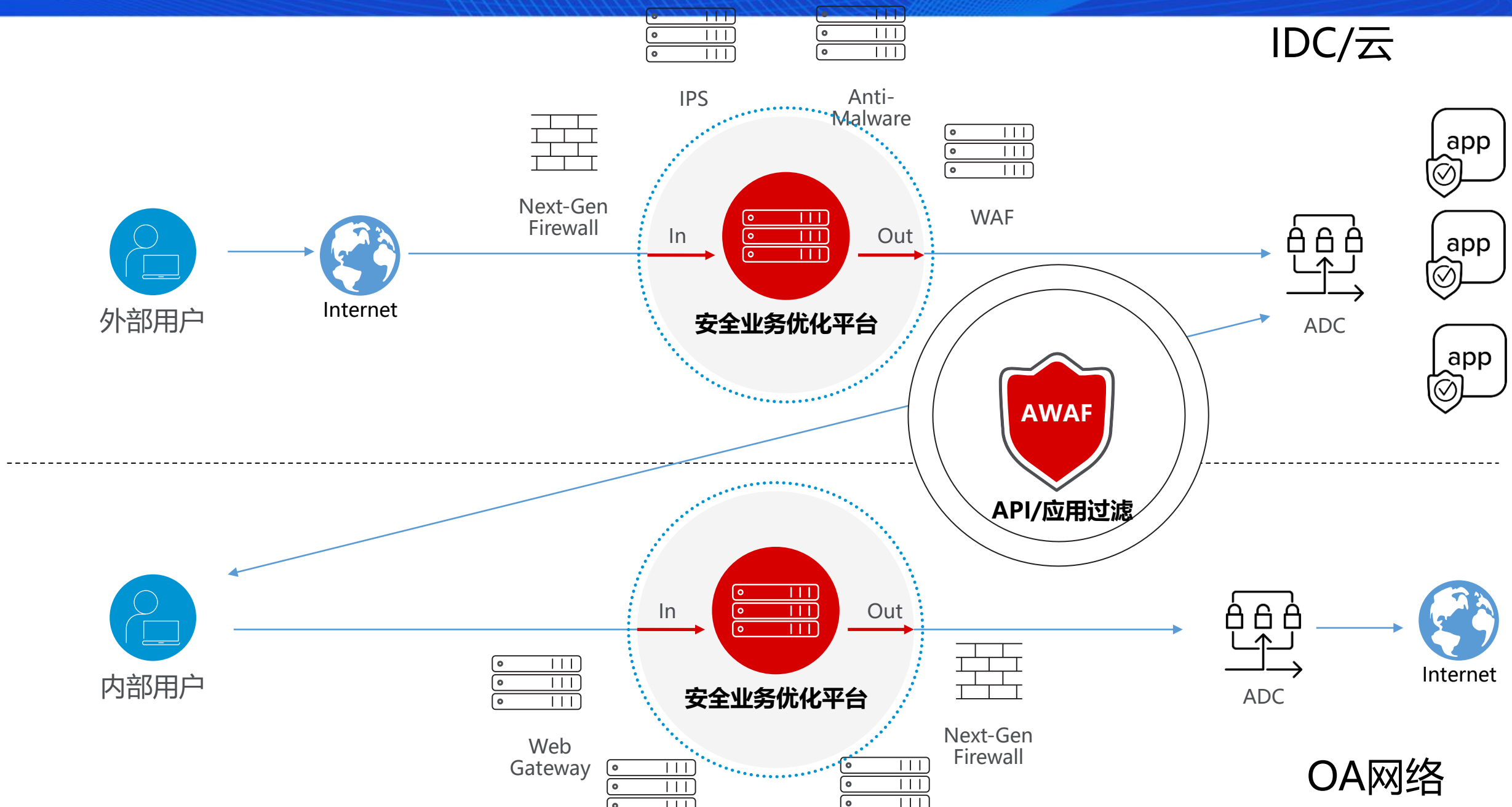
## 任意环境部署

降低部署排障复杂度，整合所有安全产品，提升处理性能

## 动态服务链

提升安全效能，提升可靠性，帮助客户快速处理故障

# 企业安全模型


IDC/云
IPS
Anti-Malware
Next-Gen Firewall
WAF
app
app
app
外部用户
Internet
In
Out
安全业务优化平台
ADC
AWAF
API/应用过滤
内部用户
In
Out
安全业务优化平台
Web Gateway
Next-Gen Firewall
ADC
Internet
OA网络

# THANKS

2019北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE