软件定义边界和安全行业趋势

李雨航 Yale Li
云安全联盟中国区理事长
中国云体系联盟常务理事

许舟平
云安全联盟中国区专家
华为DevOps软件架构师

CLOUD CONNECT
全球云计算大会 · 中国站

关于软件定义边界SDP

- 构建端到端的、高度安全和可信的网络，覆盖…
  - BYOD 以及 物联网（IOT）
  - 保护虚拟私有云（VPC）
  - 对未认证个体隐藏网络
  - 在客户端、应用和主机之间创建动态边界
- 更重要的，SDP和SDN相辅相成

SDP™ Software Defined Perimeter Working Group

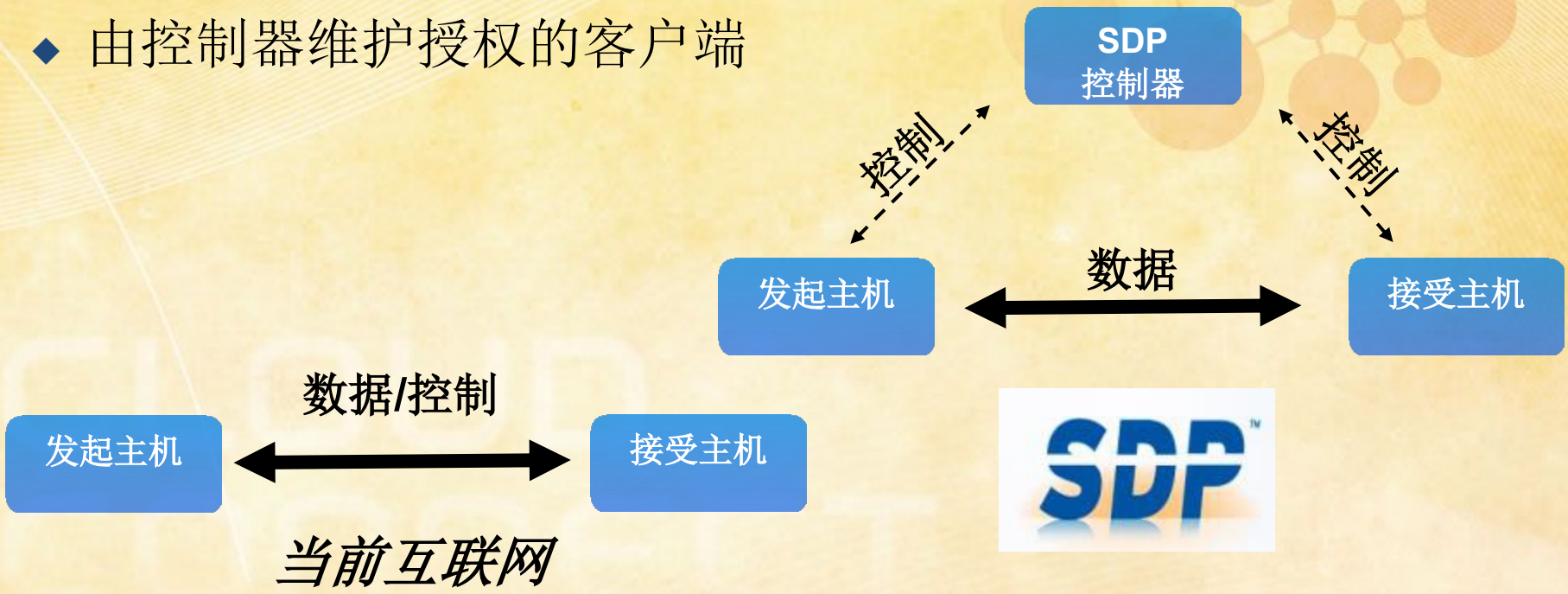
SDP采用的是机密网络模型来保护应用程序，传统边界已经迅速成为设备在网络内部移动以及应用程序从网络边界迁移到云计算的障碍。通常在机密或高度安全网络，每台服务器被隐藏在远程接入网关后面，用户在查看和访问授权服务之前必须进行身份验证。

“SDP保留了‘需要知道’模型的优势，同时消除了对远程访问网关设备的缺点，”根据该CSA报告显示，“SDP要求端点在获取对受保护的服务器的网络访问之前，必须进行身份验证以及获得授权，然后，在请求系统和应用程序基础设施之间会实时创建加密连接。”请求系统可以是移动设备，例如智能手机、计算机或 者甚至是传感器。

SDP有什么特点？

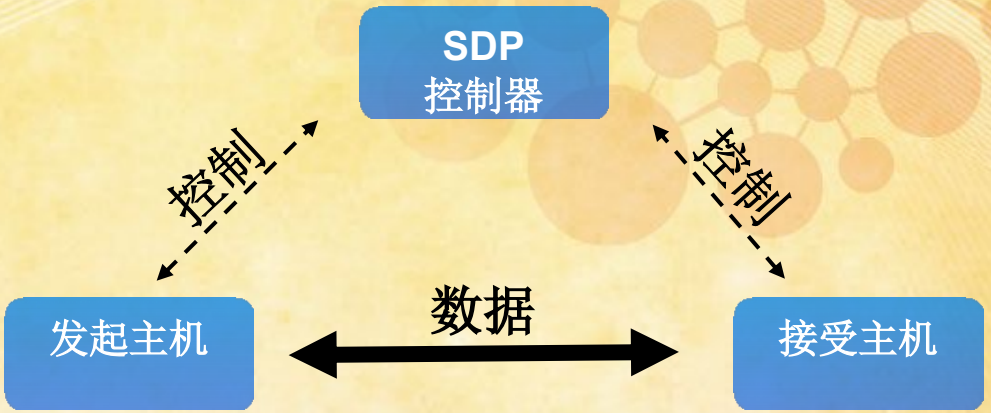
- 控制信道和数据信道分离！
- 所有服务器缺省情况下不接受任何连接请求 – 认证之前资源不可见

- 由控制器维护授权的客户端



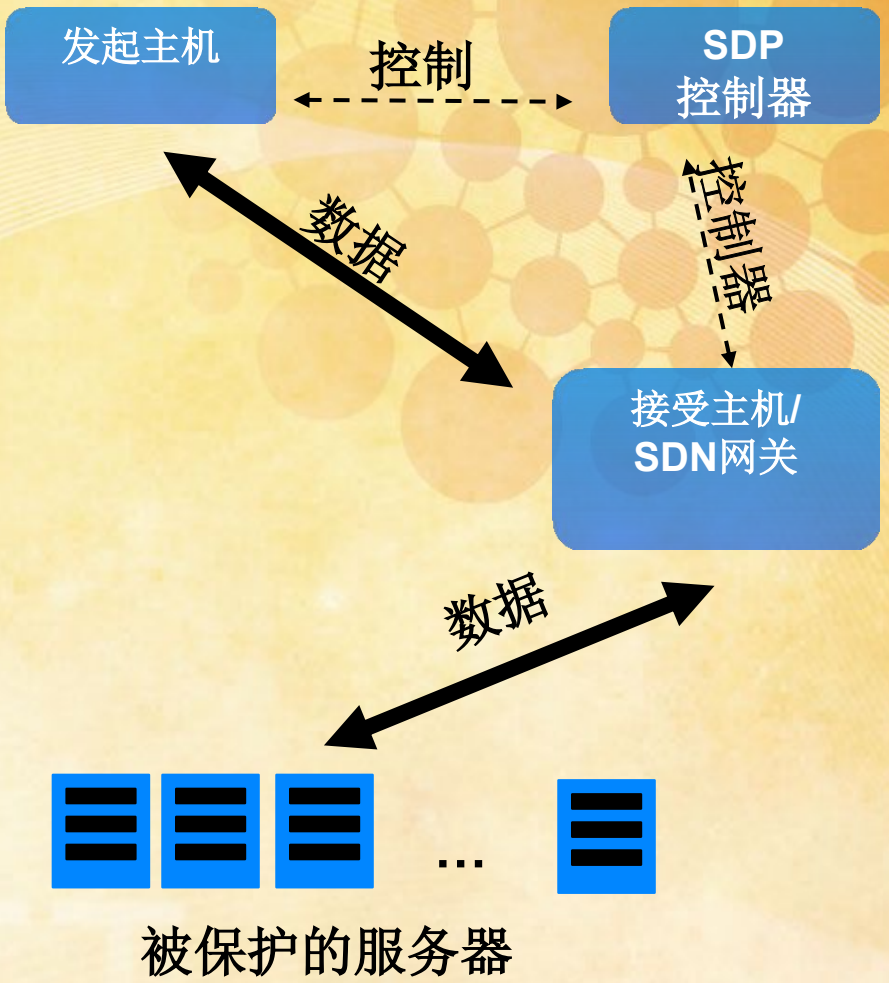
SDP怎么用？

- 企业应用隔离
- IaaS (VPC)
- SaaS
- PaaS
- Cloud-based VDI
- BYOD, 移动
- 物联网



动态防火墙 / SDP 网关

- SDP 网关: 接受主机的特殊版本，用以保护服务器
- 只有一条初始化规则：Deny All
- 在收到SDP控制器的指令后，为发起主机增加一条到被保护主机的“允许通过”的规则



CLOUD CONNECT
全球云计算大会 · 中国站

软件定义安全
SDDC->SDI->SDS

P1: Securing Software-Defined Data Centers
保护软件定义数据中心

- **解码/解密/深度检查相关新协议，e.g. OpenFlow, VXLAN, NVGRE， etc.**
- **保护控制器和可编程通信接口**
- 确保Controller和网元通信安全和完整性
- 保护安全策略的一致性以及SOD
- 提供策略调整的审计、日志和监视
- **将安全管理控制平面和数据运行平面分离**

P2: Integrating With the Software-Defined Infrastructure
集成软件定义基础设施

- 支持SDN awareness and integration via OpenFlow
- 加强Context aware security policies
- 基于逻辑属性的安全策略，而不是物理属性
- 使用RESTful or JSON APIs自动化

- *Security doesn't have to all move to software.*

P3: Evolving Into Software-Defined Security
演化到软件定义安全

- 安全管理平面和安全数据平面分离
- 将出现安全管理器，集中管理安全SLA/策略/属性
- 全局管理，而不是某个安全设备
- P+V混合按需部署优化
- 与其它SDx控制器双向集成
- 关注策略和风险，而不是基础设施的编程

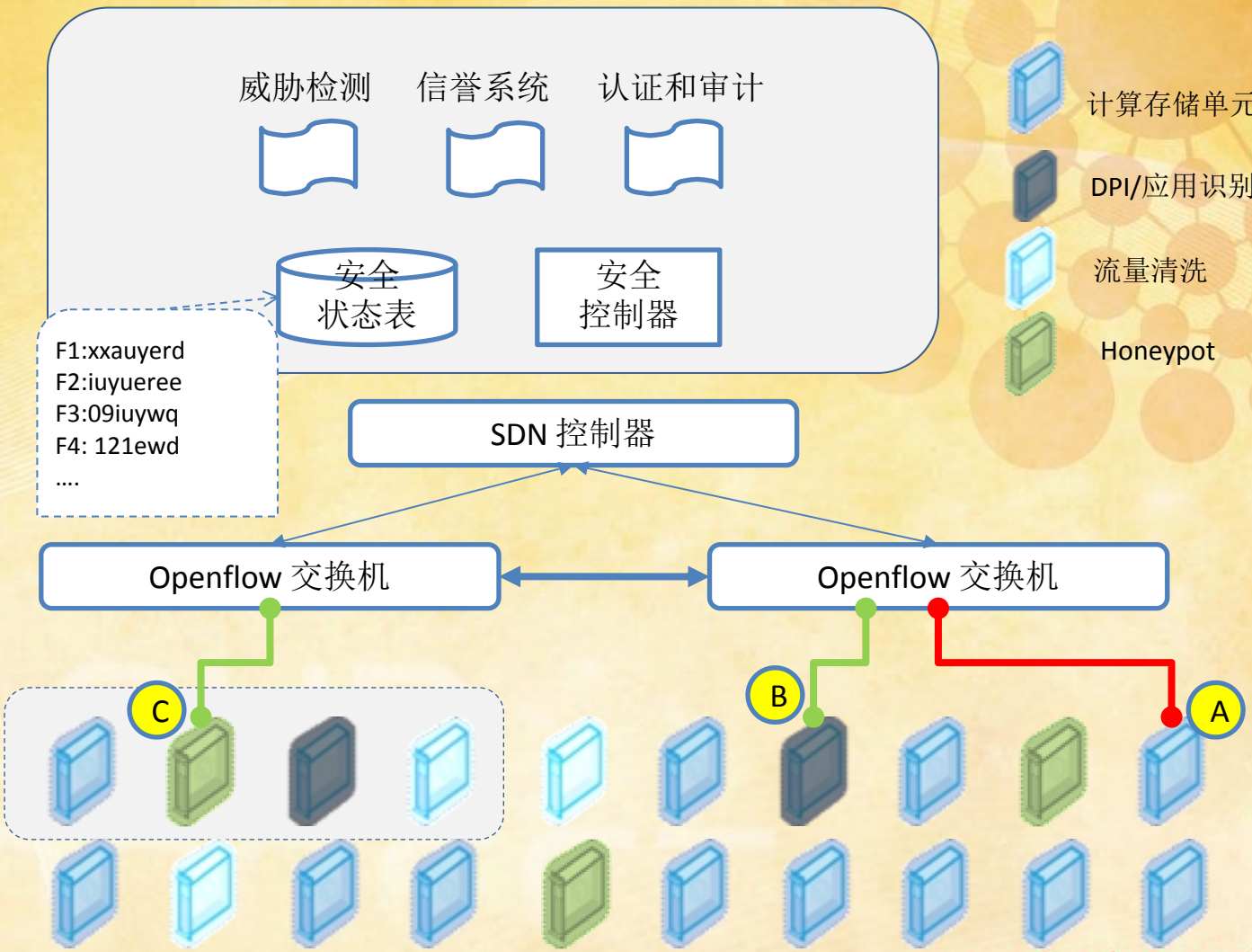
Data Source: Gartner, 2013

SDS的一个架构实例

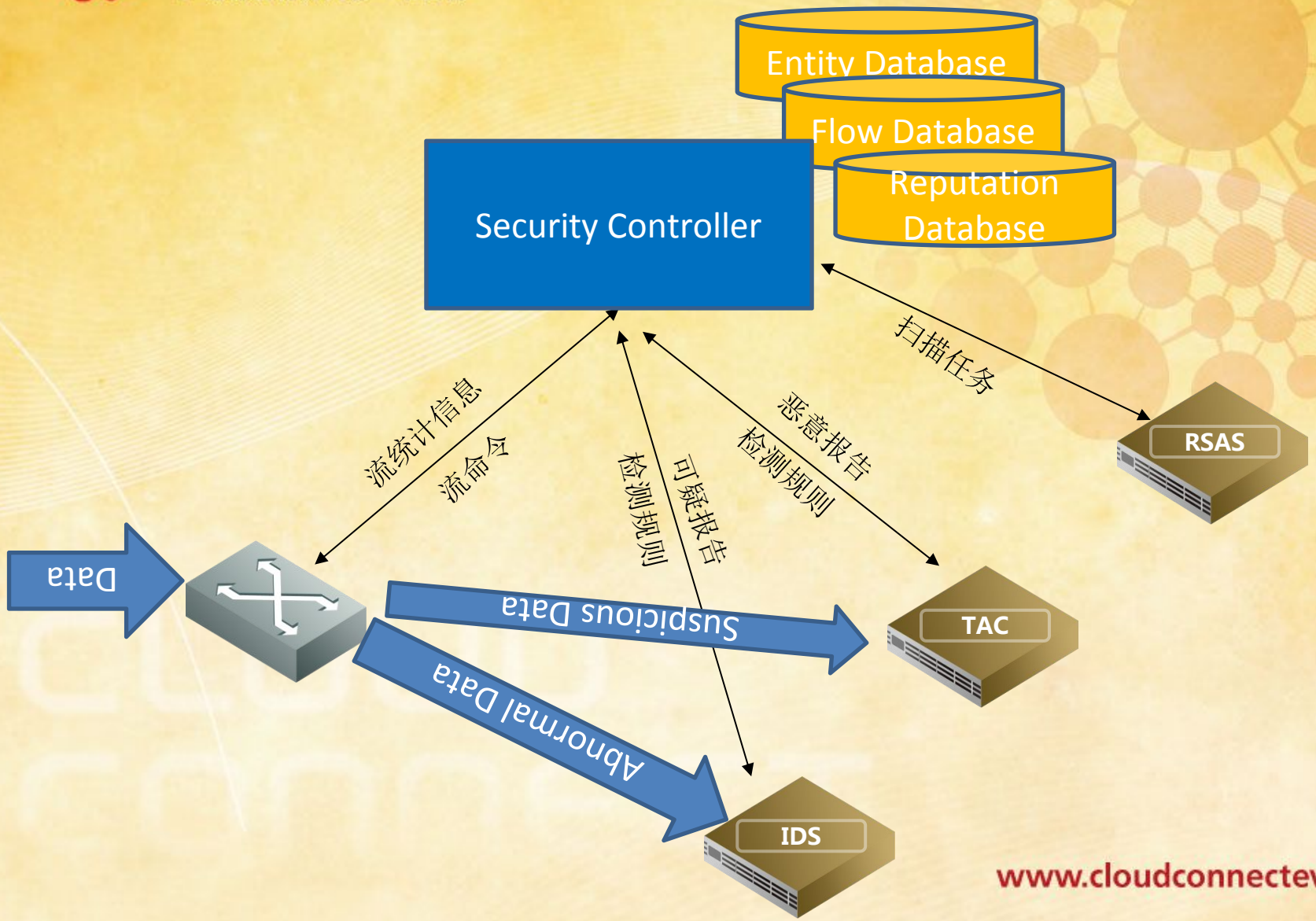
安全服务层

控制层

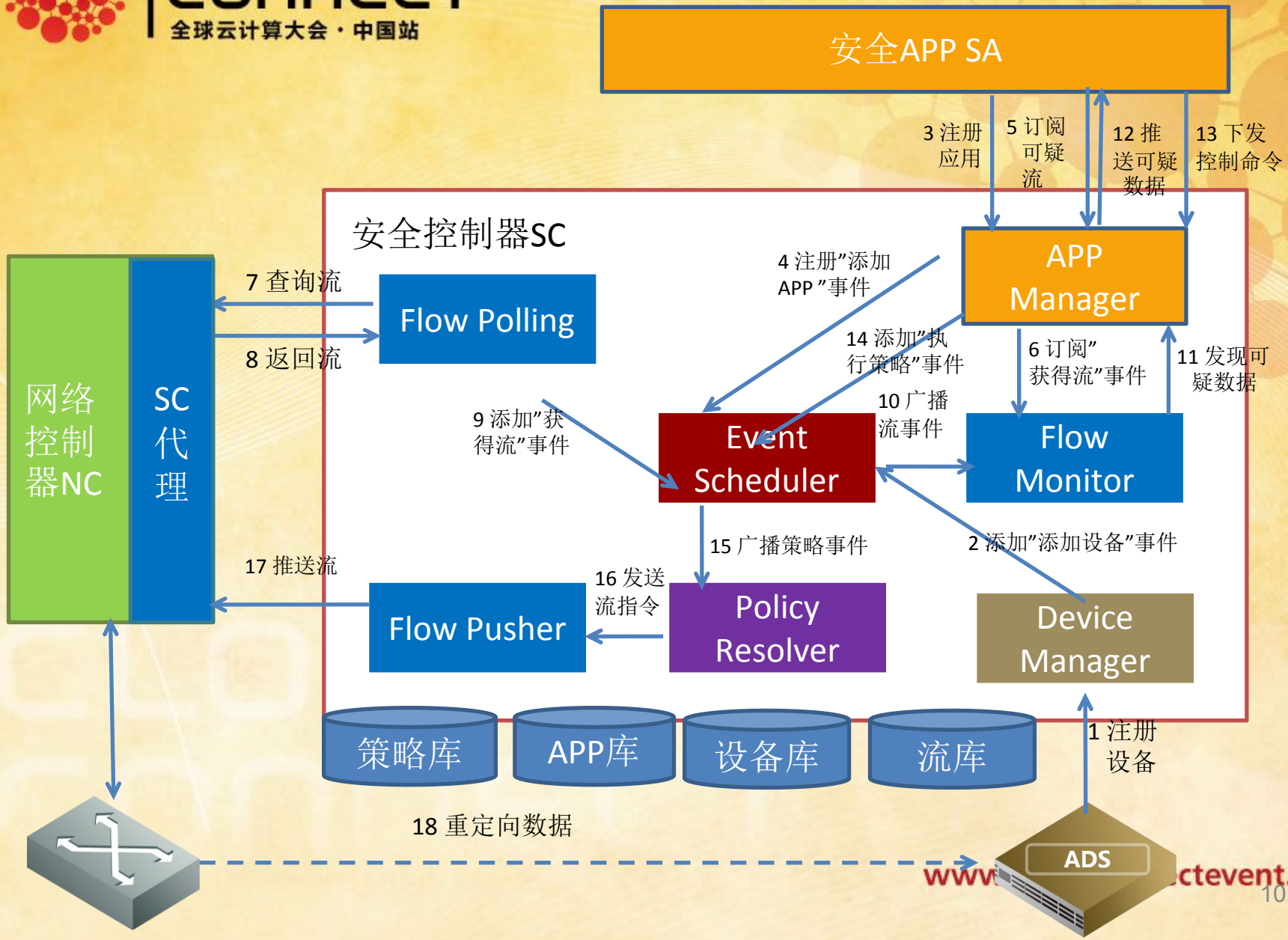
基础设施层



场景示例：软件定义的APT检测



我们的实现- 安全控制器


安全APP SA
3 注册应用
5 订阅可疑流
12 推送可疑数据
13 下发控制命令
安全控制器SC
APP Manager
4 注册"添加APP"事件
7 查询流
8 返回流
Flow Polling
网络控制器NC
SC代理
14 添加"执行策略"事件
6 订阅"获得流"事件
11 发现可疑数据
9 添加"获得流"事件
10 广播流事件
Event Scheduler
Flow Monitor
15 广播策略事件
2 添加"添加设备"事件
17 推送流
16 发送流指令
Flow Pusher
Policy Resolver
Device Manager
策略库
APP库
设备库
流库
1 注册设备
18 重定向数据
ADS

业界趋势

- SDN & NFV
- IaaS、PaaS、SaaS
- Container

Software Defined

Networking
Storage
Security
Infrastructure
Data Centers

- Abstraction
- Instrumentation
- Automation
- Orchestration

Q&A

For more information on the Cloud Security Alliance, please contact:

- 李雨航
  v-yli@cloudsecurityalliance.org
- 沈寓实
  v-yshen@cloudsecurityalliance.org
- 许舟平
  pipin@139.com