



QCon 全球软件开发大会
INTERNATIONAL SOFTWARE
DEVELOPMENT CONFERENCE

BEIJING 2017

API 平台的安全实践

张 梁



促进软件开发领域知识与创新的传播



关注InfoQ官方信息
及时获取QCon软件开发者
大会演讲视频信息



扫码，获取限时优惠



全球架构师峰会 2017 [深圳站]

2017年7月7-8日 深圳·华侨城洲际酒店

咨询热线: 010-89880682



全球软件开发大会 [上海站]

2017年10月19-21日

咨询热线: 010-64738142



很高兴，与您分享 ...

- ▶ API与数字化转型
- ▶ API平台的安全需求与解决之道
- ▶ API网关的安全实践
- ▶ 案例分享
- ▶ API云服务与身份云服务

什么是API?

An APIs is an **interface** to a **service** at an **endpoint**.

(API就是一个用于访问某个端点上服务的接口。)



入口

访问您的 API 的入口在哪里?

执行安全策略 的关键位置

不能随意访问您的API。



认证

如何标识“来访者”、“客户”的身份？



授权

有访问您的API的权限吗？



抵禦安全威脅

如何防盜？如何防破壞？



监控

谁在使用、在如何使用您的API？
实时掌握API的使用情况。

A man in a dark suit and purple tie stands in an airport security line. He is holding a white folder and looking to his left. In front of him are several blue automated security screening machines with monitors and card readers. Above the machines are signs with numbers 43, 44, 45, and 46. The background shows a busy airport terminal with other people and structural elements.

如何上手

如何才能快速上手、开始访问您的API?



有序

您的API是否足够直观？

用户体验

您的API是否易于使用？





可寻址能力

用户如何能够方便地找到您的API?

开放性

您的API是否可以公开?



EMPLOYEES ONLY

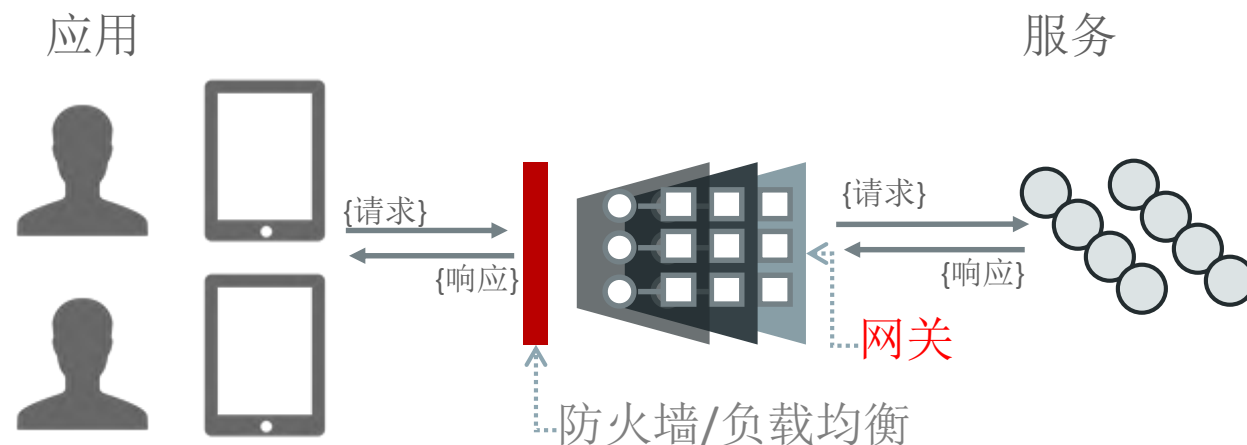
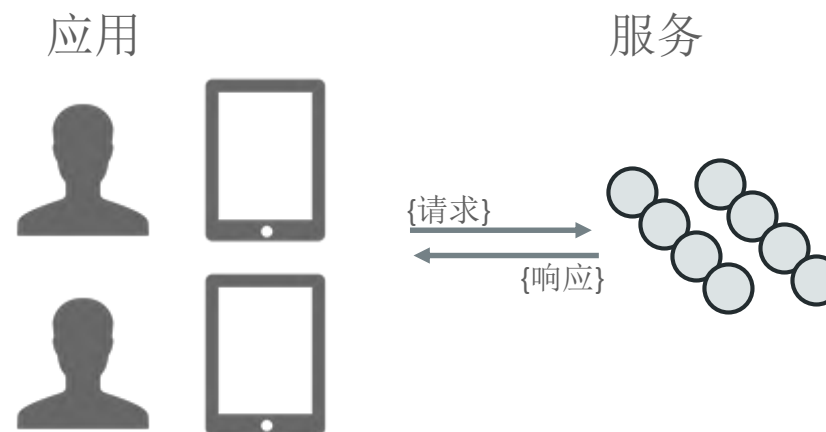
DO NOT OPEN
DOOR
SNAKE PIT

受限区域

只为“您”服务的特定能力。

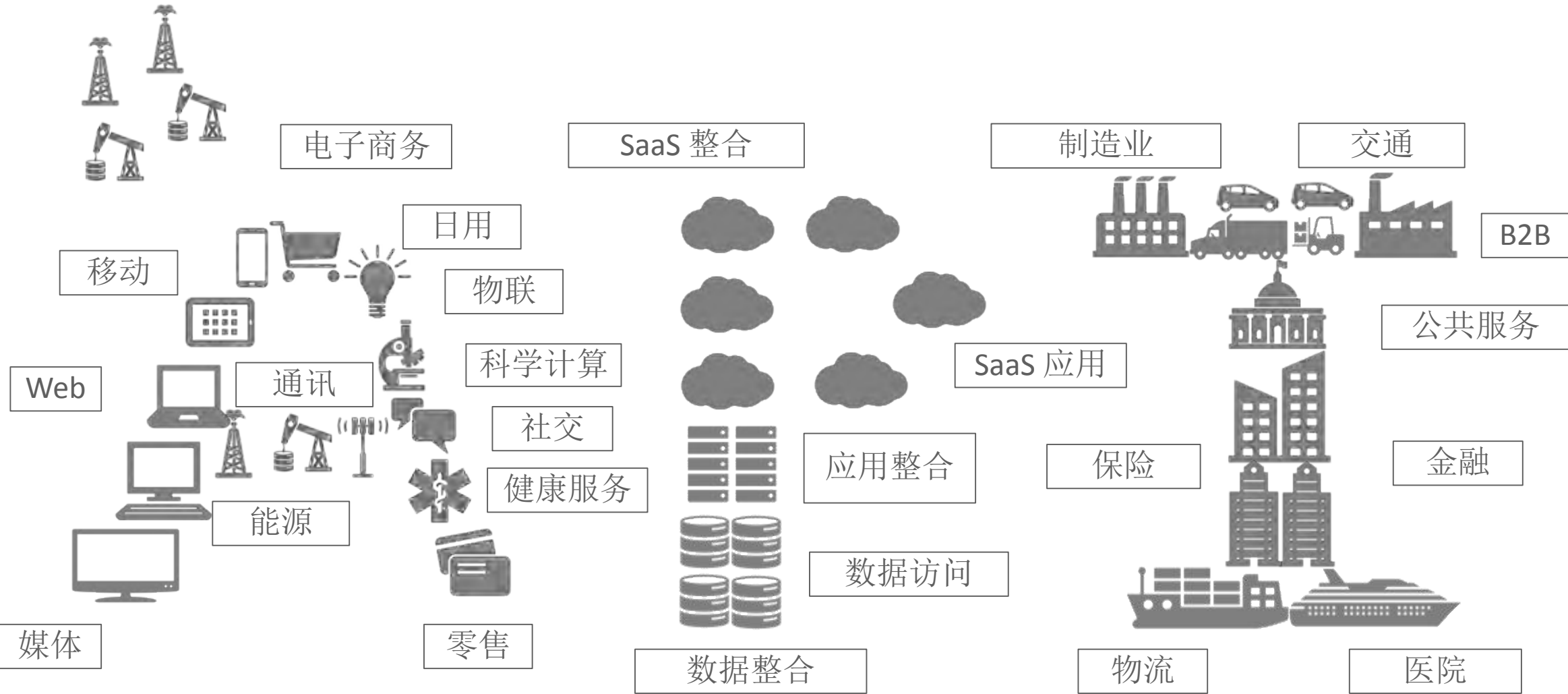
一个API需要:

- 被保证安全
 - 对服务进行保护
- 易于被发现
 - 把功能向开发者和业务伙伴进行宣讲和推广
- 能够被监控
 - 随时掌握您的服务的使用情况
- 需要被管理
 - 对API进行全生命周期的管理

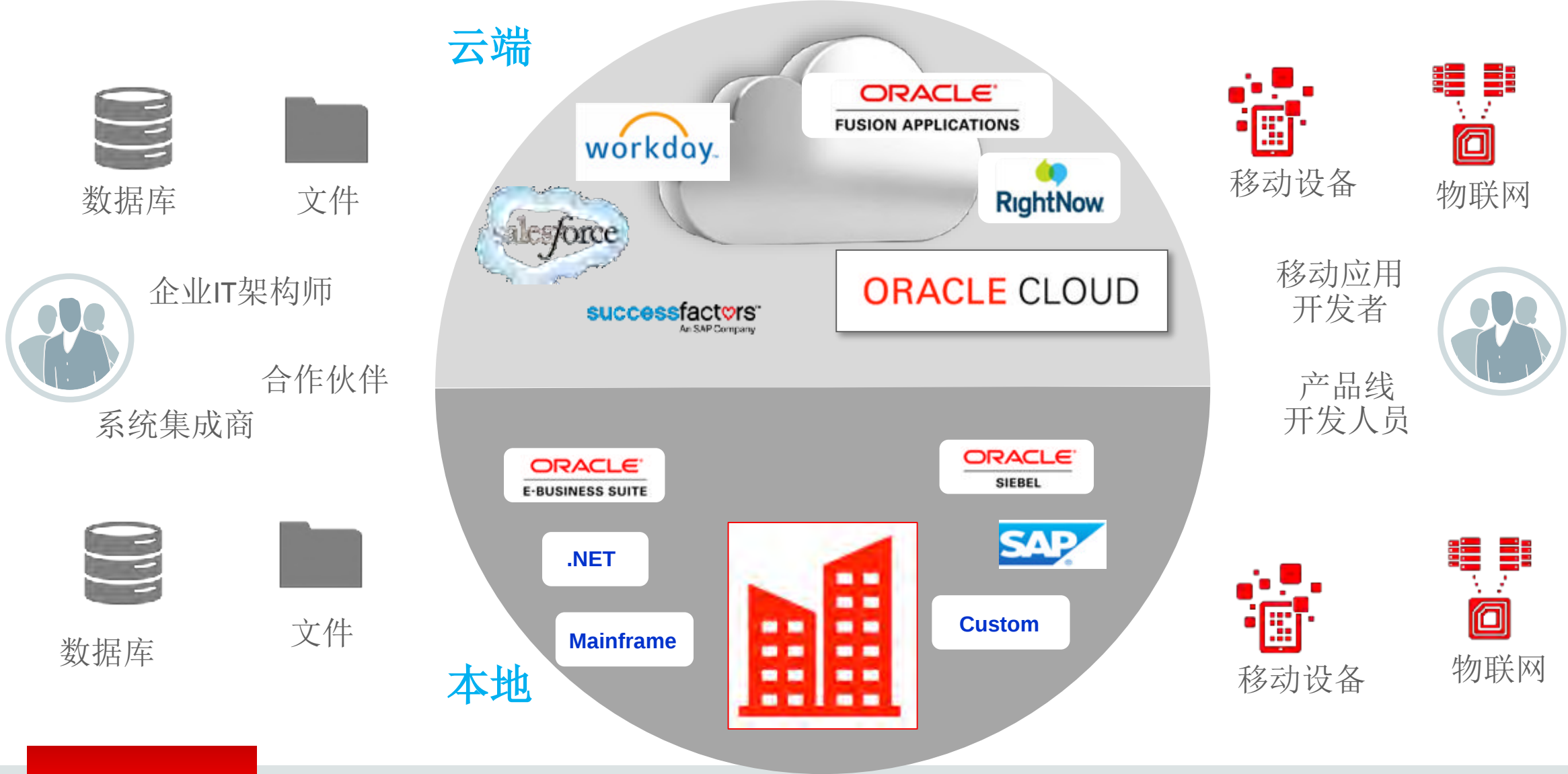


API是通往数字化经济的**大门**，
同时也是安全需求最高的门。

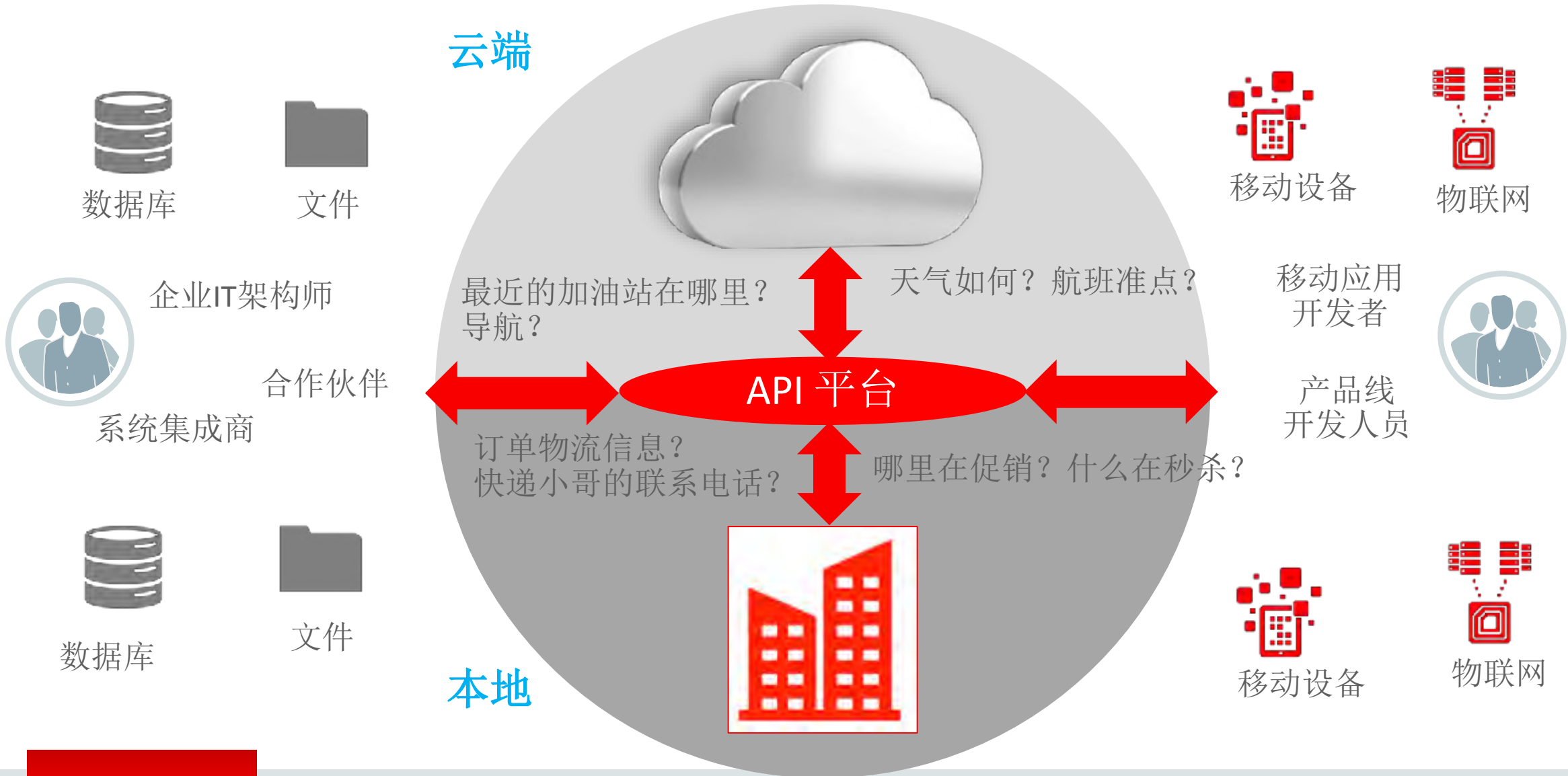
数字经济 – 跨界的整合与挑战



数字经济 – 复杂的业务挑战，复杂的IT，复杂的开发者



数字经济 – API平台是通往数字化经济的大门



API平台需要考虑的问题

我需要开放多少服务和API?

API的演进路标及版本控制?

如何设计我的API?

API的权限管理?

发布移动应用?

与智能设备互联的API?

如何对服务及API
进行分类管理?

我的API在哪里?

如何克服分类实现的障碍?

能否以及如何对API进行收费?

网络安全防护?

谁在使用我的API?

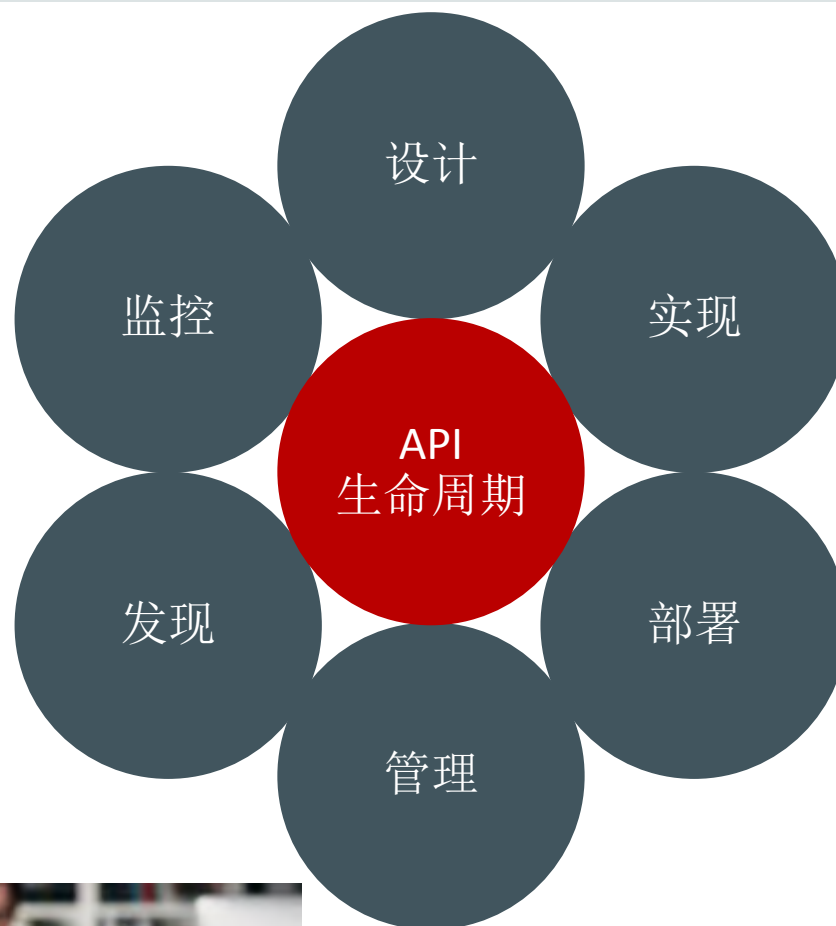
如何评价我的API?

数据安全保障?

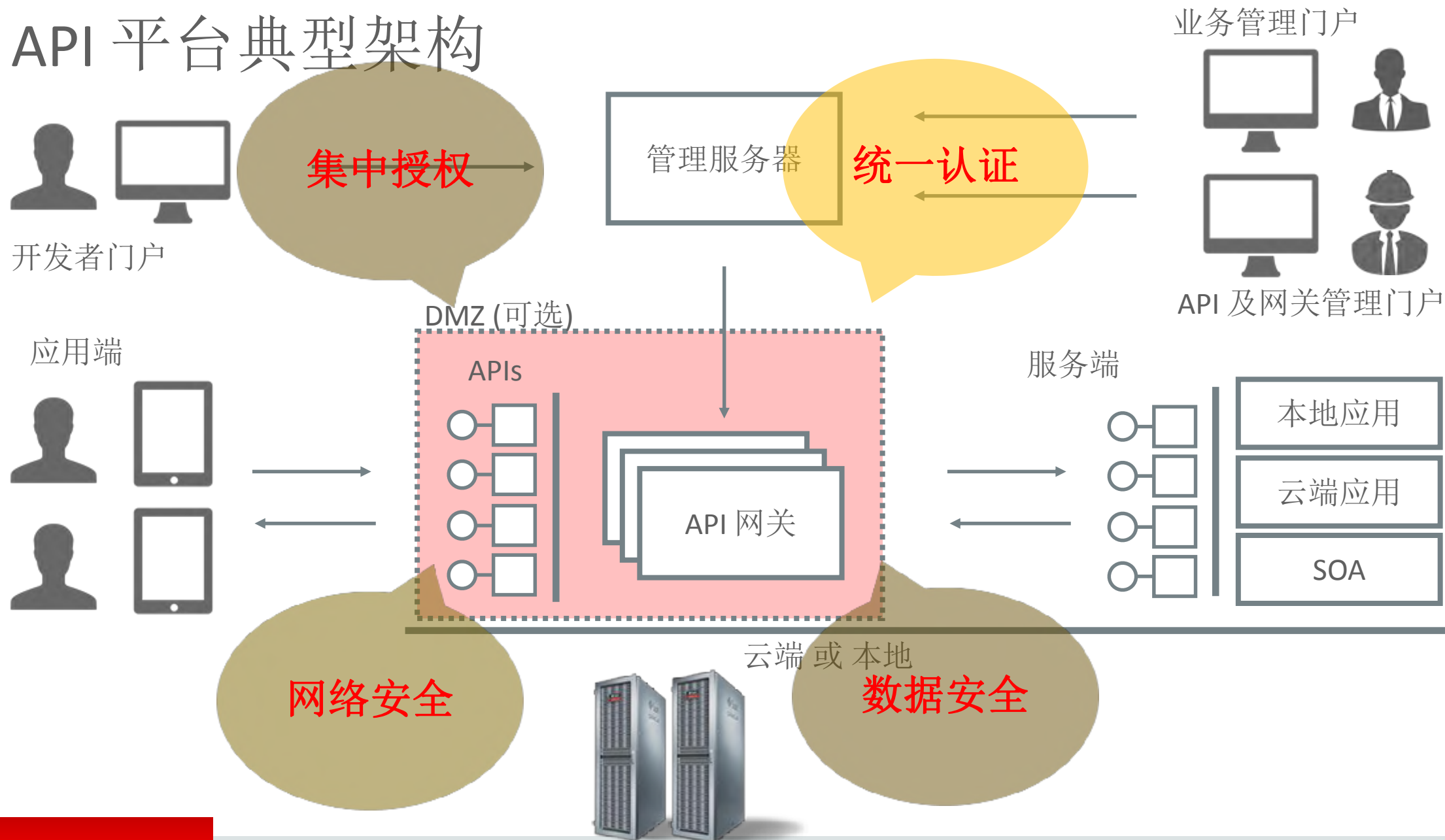
API 生命周期管理

- 参与者

- API 生产者
- API 管理者
- 网关管理者
- API 消费者



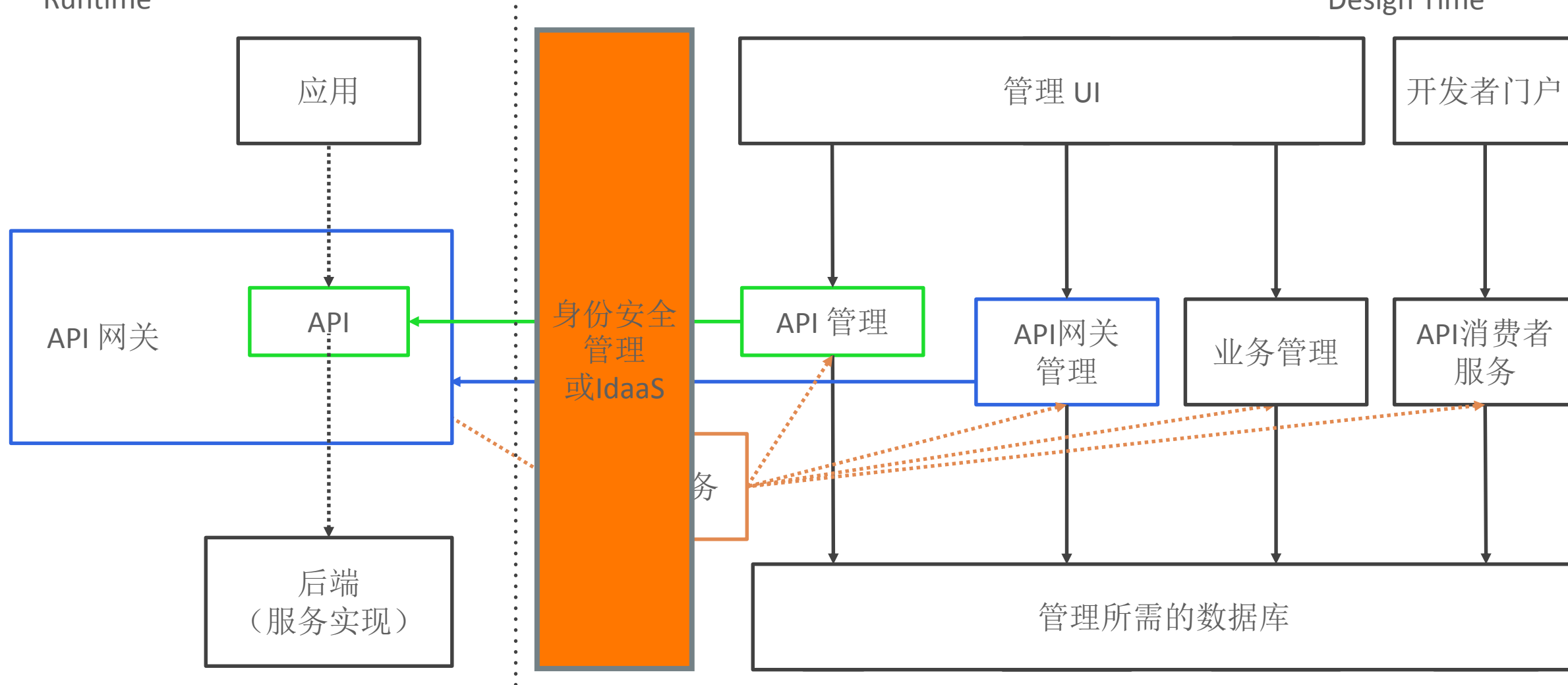
API 平台典型架构



API 平台的高阶架构图

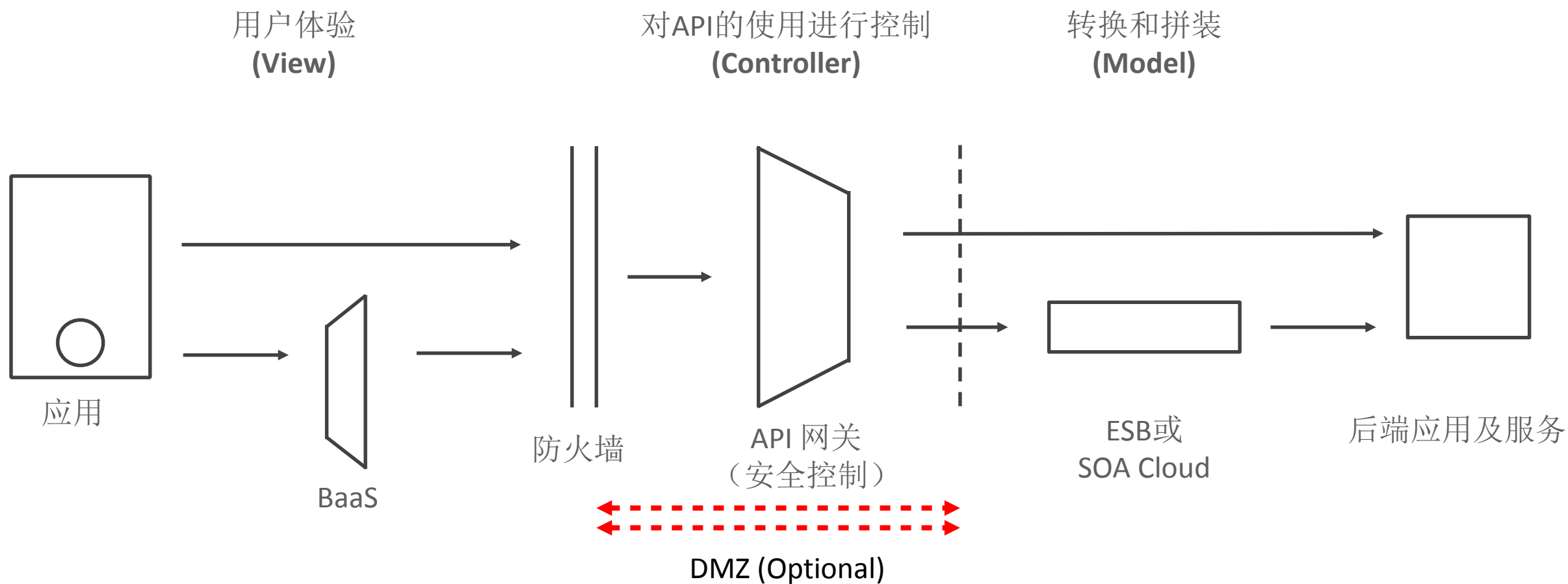
Runtime

Design Time

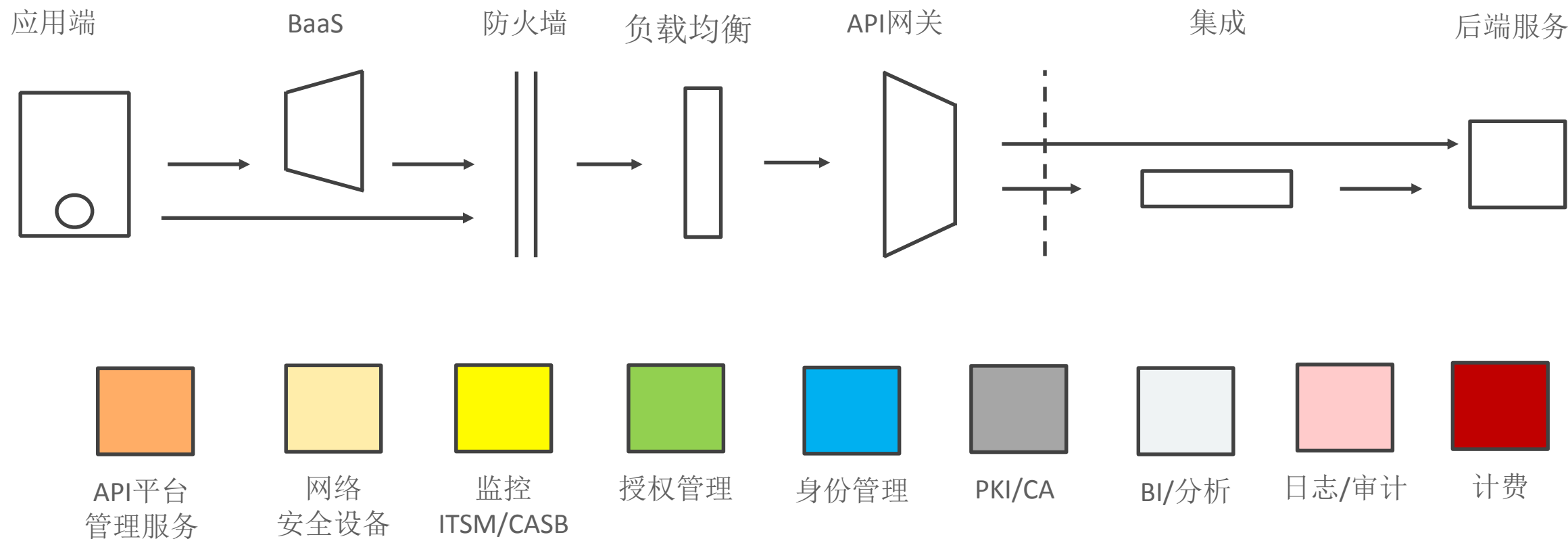


API网关的安全实践

API 网关的位置



API网关与其他组件



API网关的安全整合

- 安全协议

- OAuth 2
- Basic Auth
- API Key校验
- IP Filtering
- Service Auth
- WS-Security
- SAML
- 令牌管理

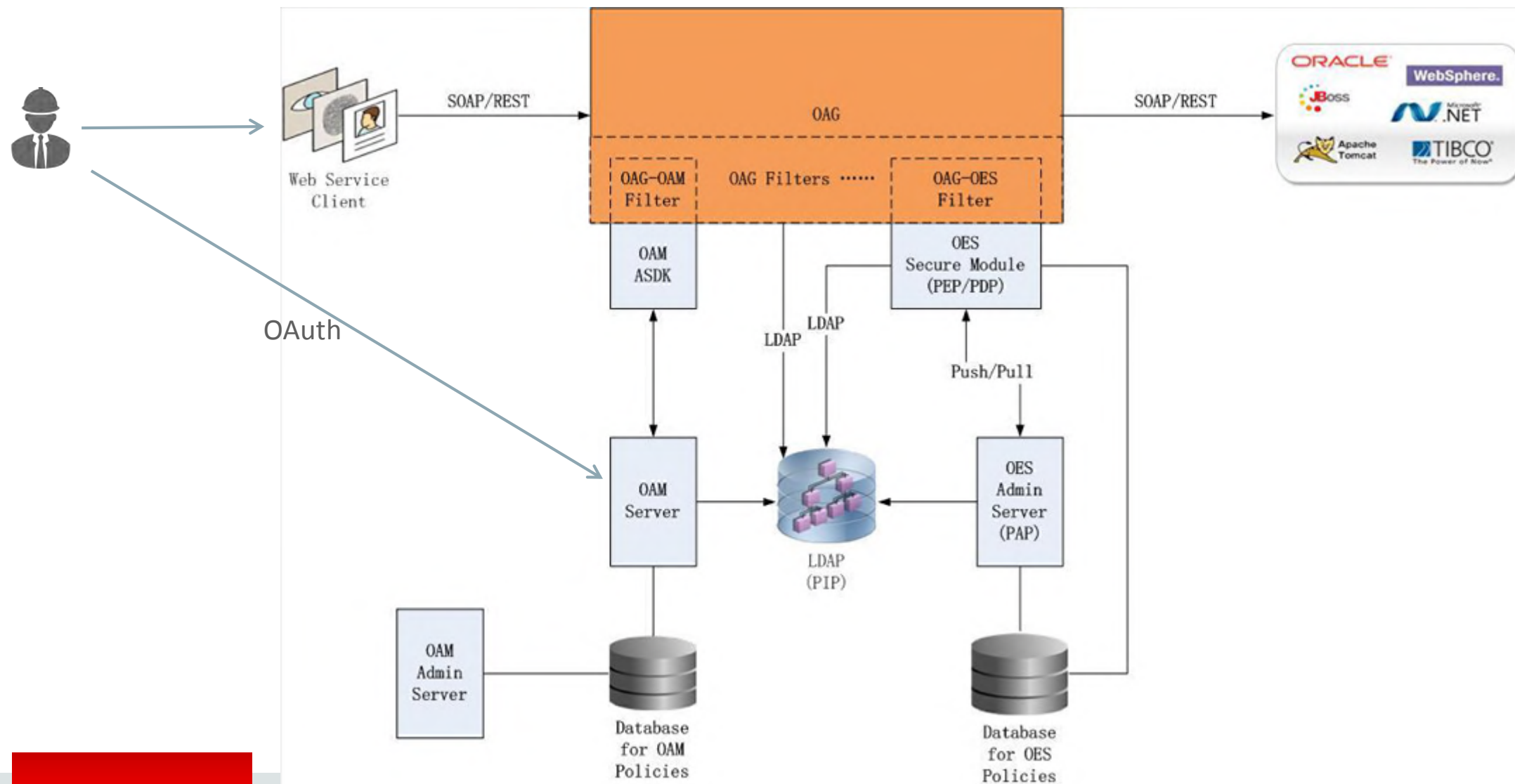
- 统一认证与外置授权整合

- 统一认证的接口
- 细颗粒度、动态外置授权检查
 - RBAC
 - ABAC
 - 附加条件（位置、时间、认证级别、身份信息、属性值。）
- 行为检查与监控
- LDAP及数据库的查询接口
- PKI/CA集成
- 分布式缓存集成

- 监控整合

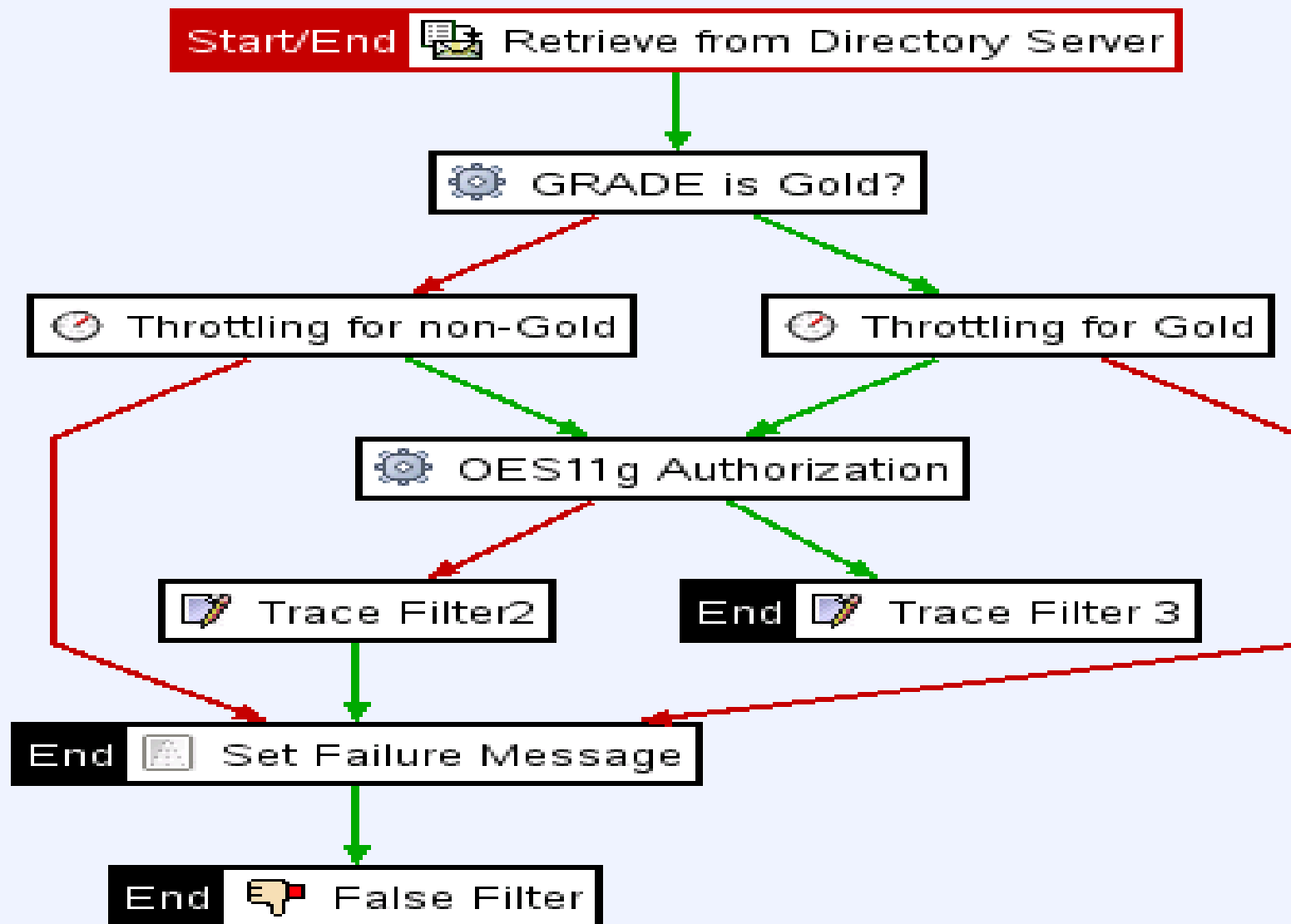
- 集中化的日志管理
- 安全策略跟踪与统计
- 响应时间、拒绝率、性能的跟踪与统计
- 安全事件报警
- 服务报警
- 版本及配置监控
- 审计服务
- ITSM集成
- BI集成与分析

API网关的身份安全整合视图



API网关：限流与细颗粒度、动态外置授权检查

1. 用户属性提取
2. 根据用户身份级别做限流控制（是否金卡）
3. 根据用户角色进行授权
4. 根据用户属性进行授权
5. 根据其他条件进行授权



细颗粒度动态授权管理：定义授权策略

针对哪些角色，对哪些资源类型与哪些资源和哪些操作进行授权；
以及哪些条件下才允许授权，授权成功后返回哪些Obligations提示信息

The screenshot displays the 'Authorization Management' console, specifically the 'System Configuration' tab. The left-hand navigation pane shows a tree structure with 'Authorization Policies' highlighted under the 'Default Policy Domain'. A red box labeled '1' is around this item. The main configuration area shows the 'TodoTaskListAuthzPolicy' configuration. A red box labeled '2' is around the 'Effect' dropdown, which is set to 'Permit'. Below this, the 'Name & Description' section shows the policy name and description. The 'Principals' section shows a table with one entry: 'authenticated-role'. A red box labeled '3' is around this entry. The 'Targets' section shows a table with one entry: 'TodoTaskListResource'. A red box labeled '4' is around this entry. The 'Enabled Actions' column for this entry lists 'POST,PATCH,GET,DELETE,PUT'. A red box labeled '5' is around this list. The bottom section shows the 'Condition' and 'Obligations' fields. A red box labeled '6' is around the 'Condition' field, which contains a complex logical expression. A red box labeled '7' is around the 'Obligations' field, which is currently empty. Red arrows point from the Chinese text labels to these specific fields.

1. Authorization Policies

2. Effect: Permit

3. Principals

4. Targets

5. Enabled Actions

6. Condition

7. Obligations

定义授权策略是允许还是拒绝

关联的用户角色，可运行多个角色or或and关系

所要授权的资源

所要授权的操作Actions

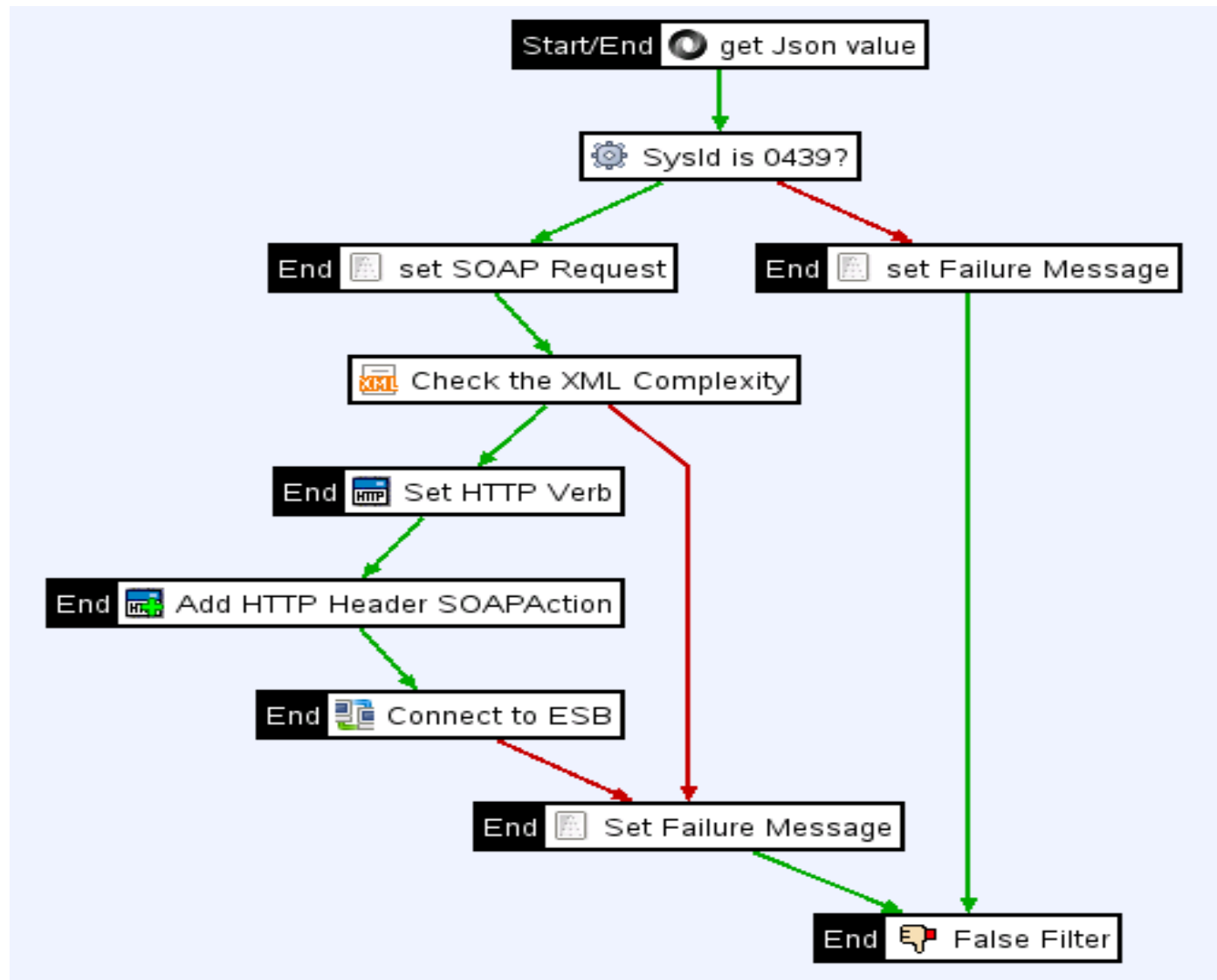
额外处理条件

提示返回信息，包括属性值或指定信息等

API网关的服务及内容安全管理

- 内容扫描与过滤

- SQL注入
- 跨站脚本
- XML 逻辑炸弹、XML深度检查
- Schema及DTD校验
- 报文大小检查
- 安全标签检查与敏感内容扫描
- 内容混淆、打码与改写
- RESTful 信息攻击保护机制
 - 超大结构消息
 - 超大JSON或元素值、超大JSON数组元素
 - 具有异常的大量嵌套元素的信息
- 外部实体引用防护
- RESTful消息模式验证



API网关的内容安全管理



拒绝服务攻击

强力攻击
超大有效负载
内存泄漏

注入攻击和恶意代码攻击

SQL注入
XPath 注入
跨站脚本攻击
逻辑炸弹

保密性及完整性

探测
参数篡改
Schema中毒
外部实体
规范化

侦查攻击

代码模板
强制浏览
注册表披露
WSDL扫描
字典转换

权限提升攻击

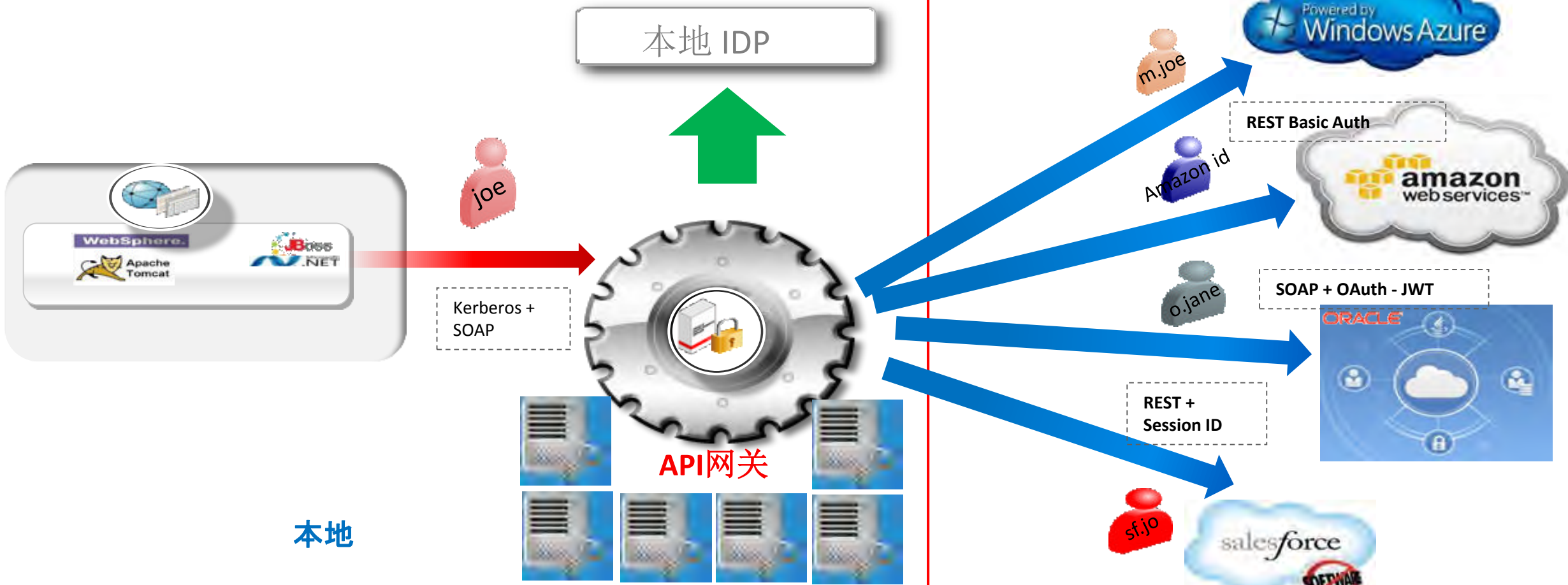
字典攻击
格式化字符串
缓存溢出
竞赛条件
符号链接
未受保护的接口

API网关的服务及内容安全管理

- 网络传输安全
 - 加密与解密
 - 签名与验签
 - SSL卸载
 - 与防火墙配合，防DDoS攻击
- 接口管理
 - 接口过滤
 - 方法映射
 - 领域编辑
 - 头校验
- 流量及配额的安全管理
 - 缓存
 - 基于应用的限流
 - 基于API的限流
 - 基于Client的限流
 - 基于API、Client及应用的组合限流与配额管理
 - 集群与分布式缓存集成
 - SLA管理
- 协议转换与传输协议
 - REST $\leftrightarrow$ SOAP
 - XML $\leftrightarrow$ JSON
 - HTTP(S)
 - SFTP
 - JMS
 - Websockets
 - Pop & SMTP

另一种用法：助力本地应用到云端的安全访问

- 统一管理云端为本地所分配的**Client Key**：简化应用开发和维护
- 统一出口，集中化安全策略：满足企业安全规范
- 访问云端的统一接口：满足云端应用的业务接口要求与安全要求

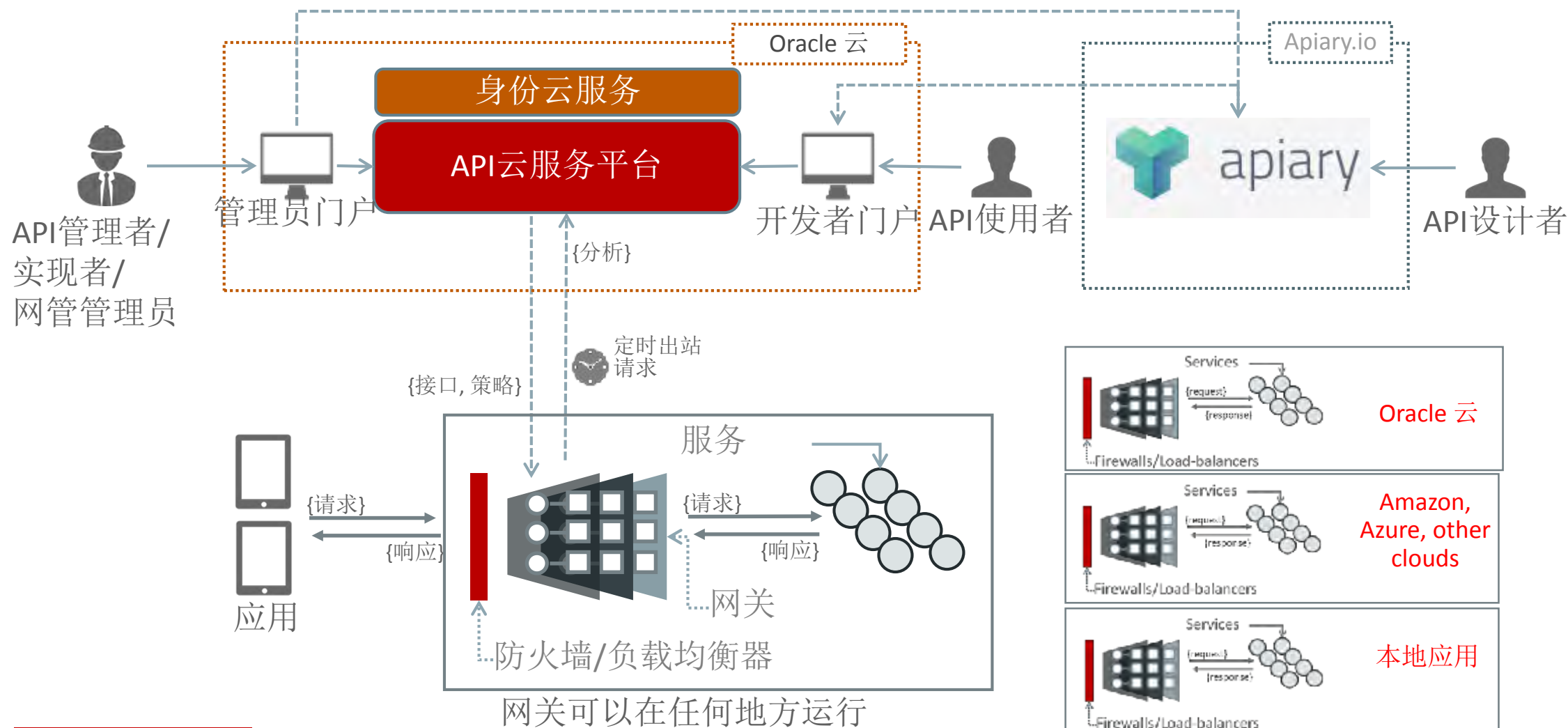


A woman with long brown hair and glasses is sitting at a wooden desk in a modern office. She is wearing a brown leather jacket over a blue patterned scarf. She is holding a black smartphone to her ear with her left hand and looking down at a document on the desk with her right hand. The background is a blurred office space with other people working.

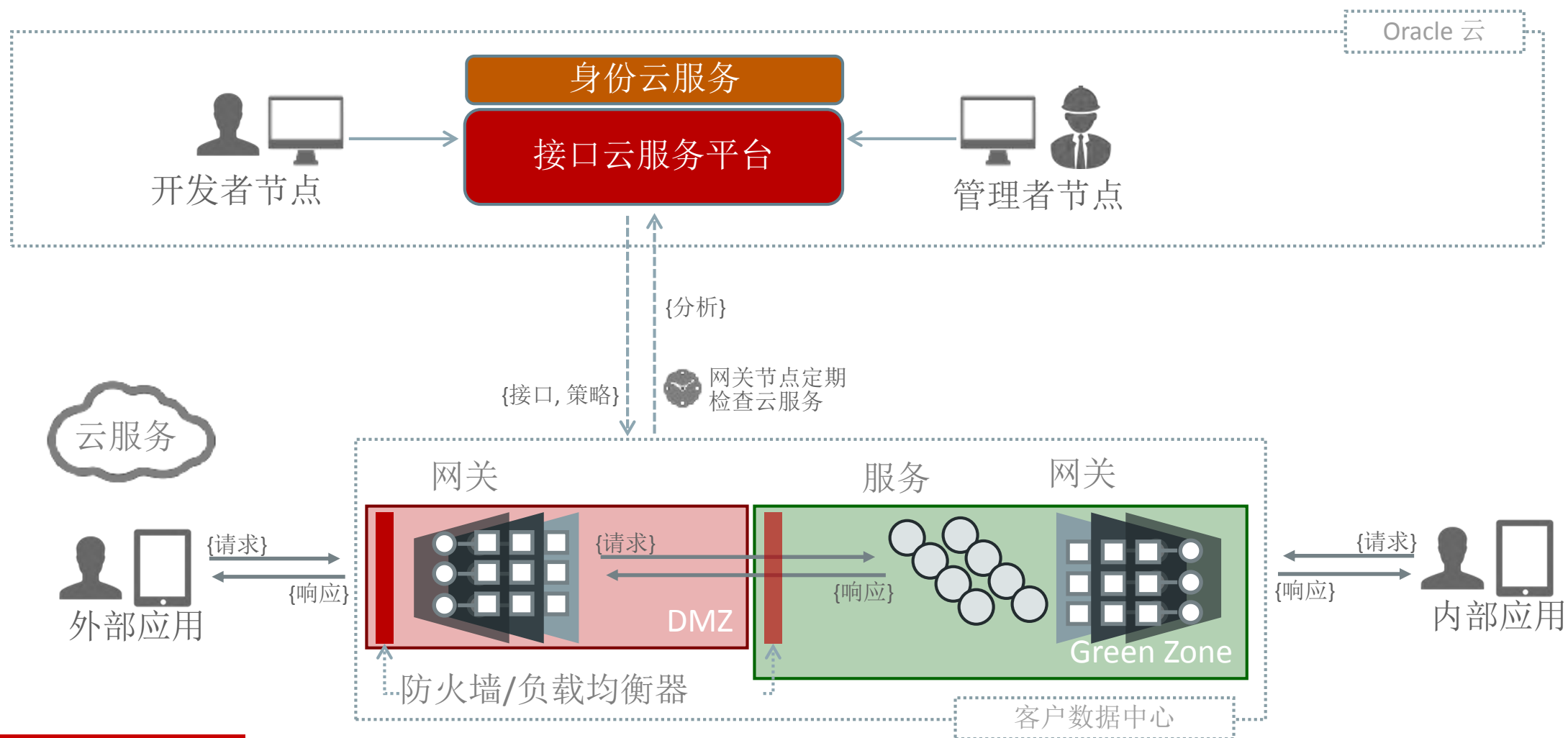
案例分享：能力开放平台的安全实践

API云服务与身份云服务

API云服务平台架构: 集中式API设计, 分布式运行



在本地环境中建立本地API接口供内外应用使用



API是通往数字化经济的大门，
同时也是安全需求最高的门。

ORACLE®

Oracle愿与您共同走向成功！



关注QCon微信公众号，
获得更多干货！

Thanks!



INTERNATIONAL SOFTWARE DEVELOPMENT CONFERENCE

主办方 **Geekbang** > **InfoQ**
极客邦科技