RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

API – 是下一个黑客攻击目标，还是业务和安全机会？

会议 ID：MAN-T09

Tim Mather

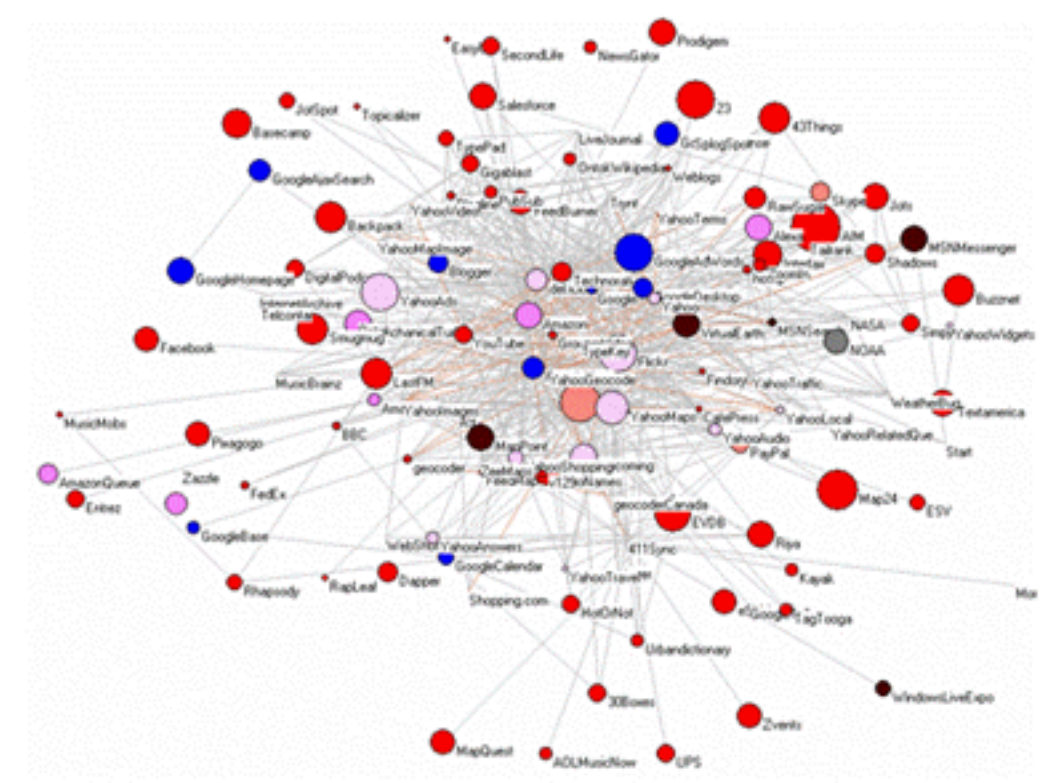
副总裁、首席信息安全官
Cadence Design Systems
@mather_tim

为何应该关注 API？

- 仅 Amazon Web Services EC2 就有 148 个 API

可编程 Web

- 跟踪向开发人员公开提供的 10,500 多个 API



每天的 API 调用数 = 数十亿次

API 业务规模庞大

- Expedia 的联盟网络每年仅通过 API 就处理价值超过 20 亿美元的交易

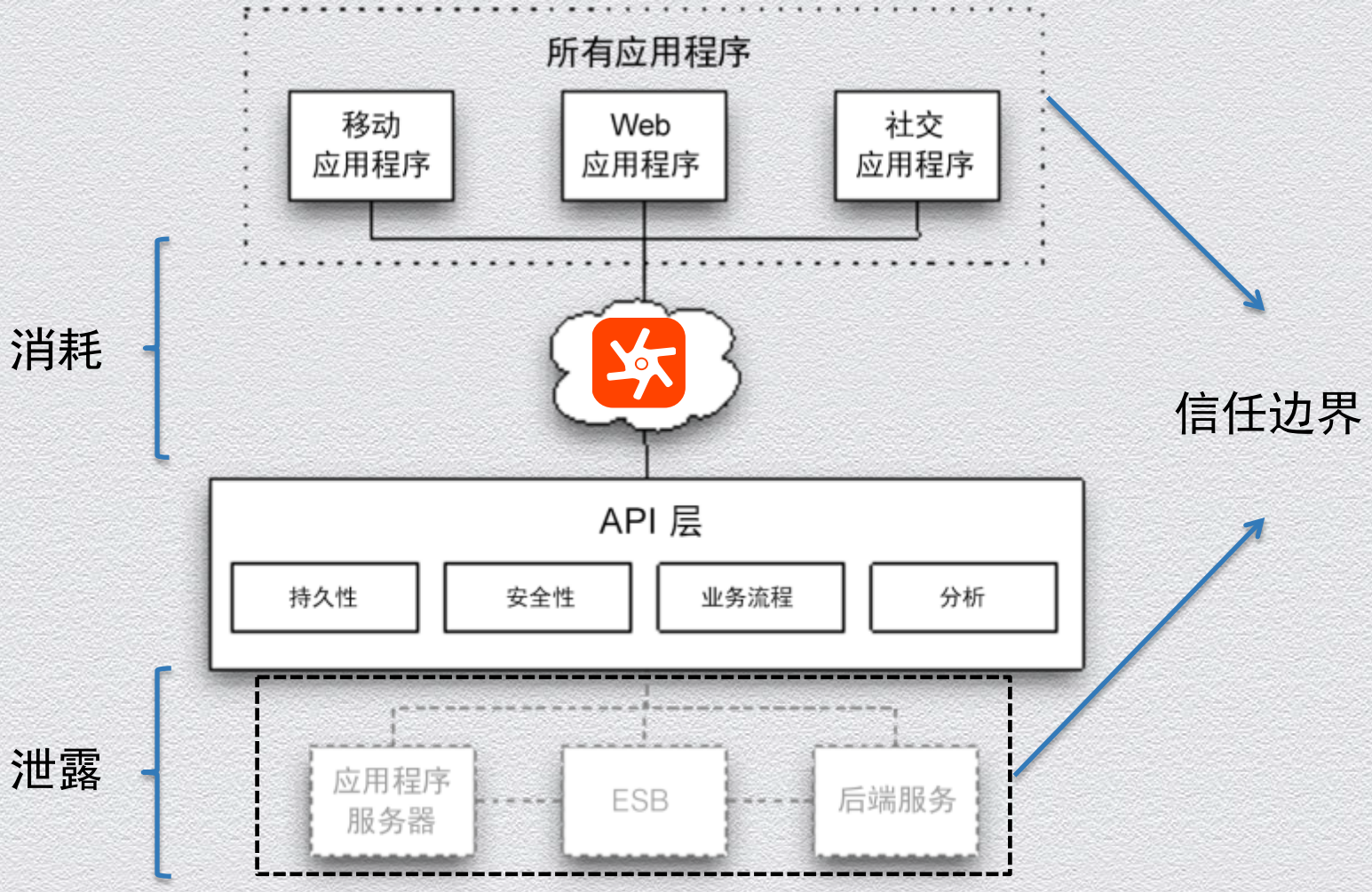
API 安全的现实情况

- 2013 年 12 月 Snapchat API 非法闯入
  - 个人信息泄漏
    - 大量的电话号码盗取
    - 创建虚假帐户
    - 准备成为大规模的垃圾邮件平台

从何处开始？

- 您是否了解您的组织有哪些 API 或者正在使用哪些 API？
- 您是否知道通过 API 正与您的受信任或不受信任客户、合作伙伴和/或供应商共享哪些数据？

消耗与泄露


所有应用程序
移动
应用程序
Web
应用程序
社交
应用程序
消耗
信任边界
API 层
持久性
安全性
业务流程
分析
泄露
应用程序
服务器
ESB
后端服务

需要端到端安全性

消耗

灵活的应用程序级别访问控制

使开发者实现安全自动化

应用程序到 API 的安全

泄露

一致的后端服务保护

使 API 团队可安全访问后端服务

API 到后端的安全

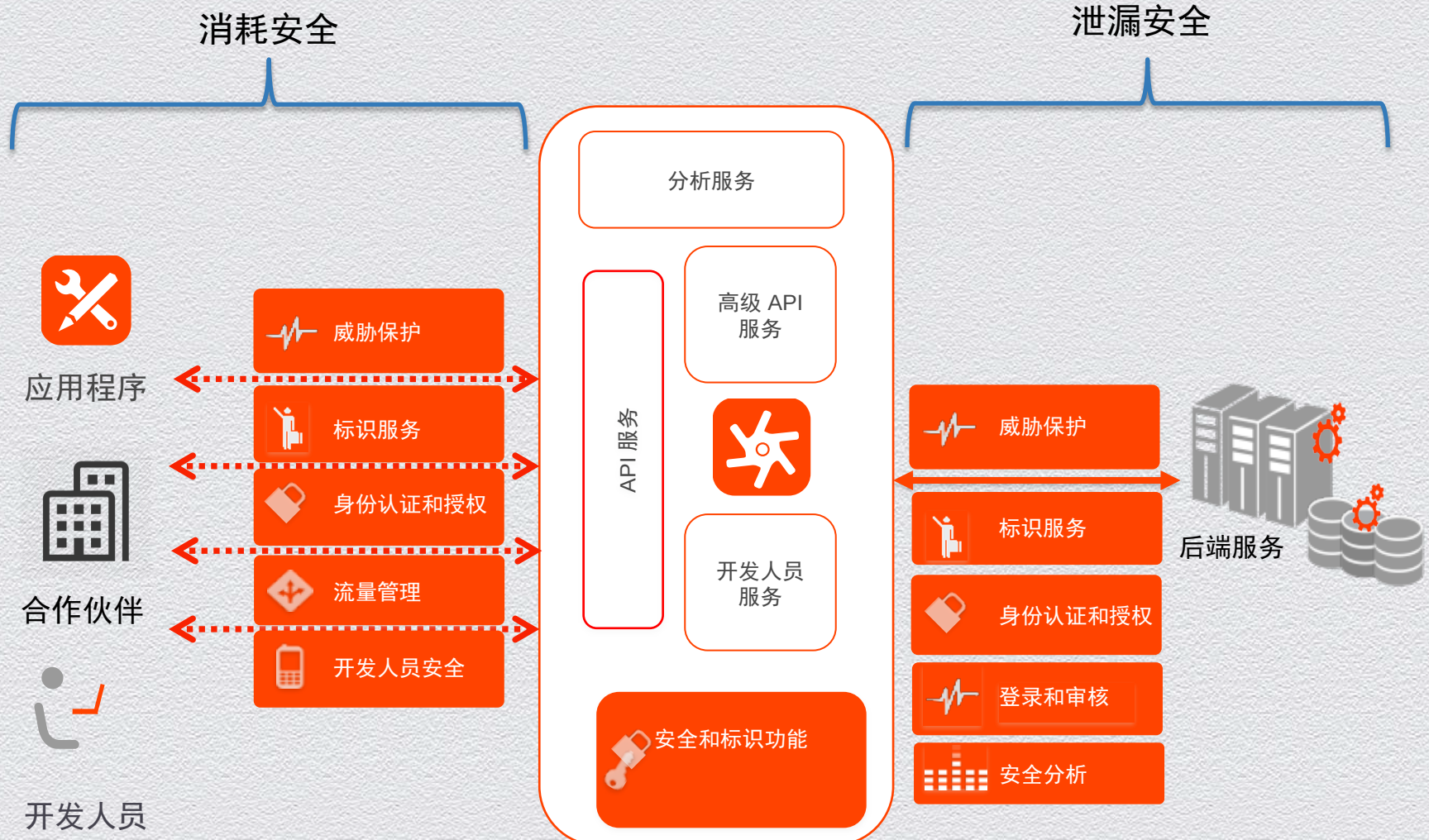
端到端的安全

边缘提供端到端的安全

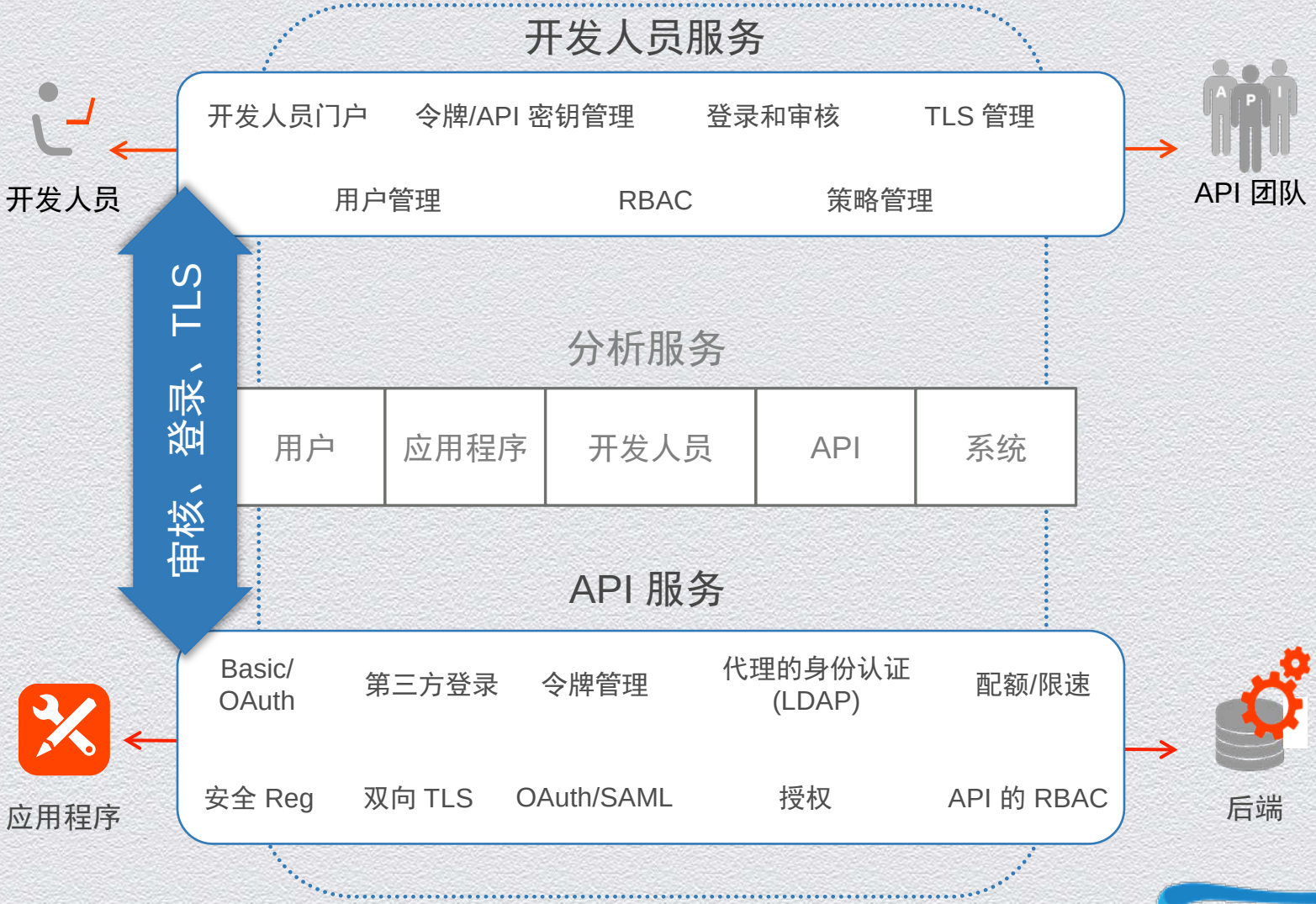
利益相关者	API 泄露安全	API 消耗安全
DevOps	☑	☑
应用程序开发人员		☑
IT 安全	☑	☑
API 架构师	☑	
业务负责人	☑	☑
终端用户		☑

API 管理解决方案必须解决 API 的不同利益相关者和消费者的安全担忧

安全组件



应用程序和 API 开发人员的端到端安全



12

提供安全的应用程序和 API 基础架构

应用程序到 API（消耗）

- 身份认证（TLS、OAuth、API 密钥）
- API 密钥和令牌管理
- 双向 TLS
- 身份认证（权限管理）
- 运行时策略
- SLA 实施
- 登录和审核

API 到后端（泄漏）

- 身份认证（TLS、OAuth、SAML）
- 双向 TLS
- 委派的身份认证（LDAP、AD）
- 与自定义标识供应商集成
- 精细身份认证
- 登录和审核

分析

- 安全报告
- 运行时检测报告（基于卷，流量属性）

威胁保护

- XML/JSON Poisoning/Injection
- SQL 注入
- DDoS/App-DoS 攻击
- Quota/Spike Arrest
- 基于 IP 的访问限制

身份

- 用户调配
- RBAC 管理
- 组
- 身份提供商

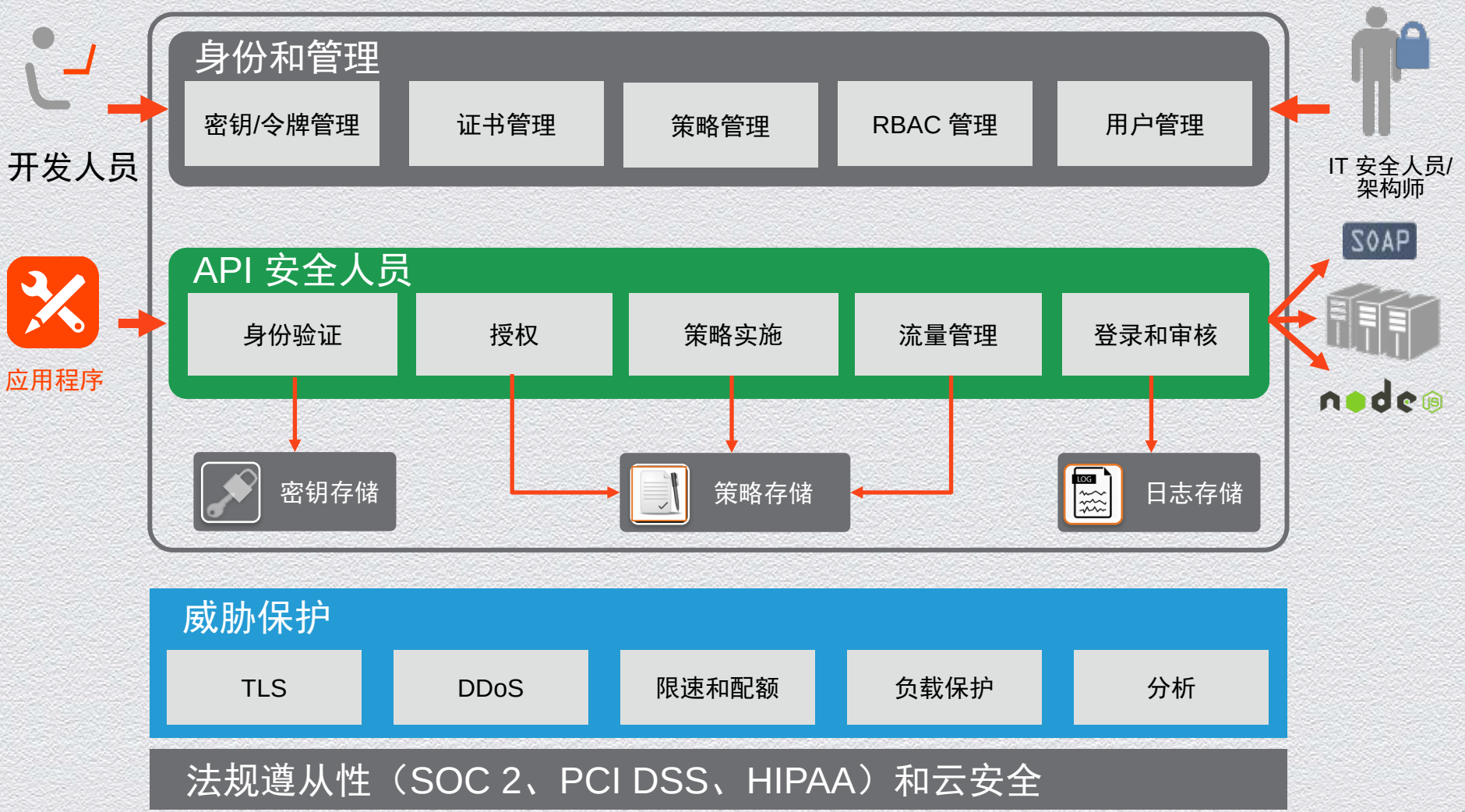
基础架构安全和法规遵从性

- 云或内部部署
- 基于云的安全（AWS + 其他）
- SOC 2、PCI-DSS、HIPAA
- 24 x 7 组织支持

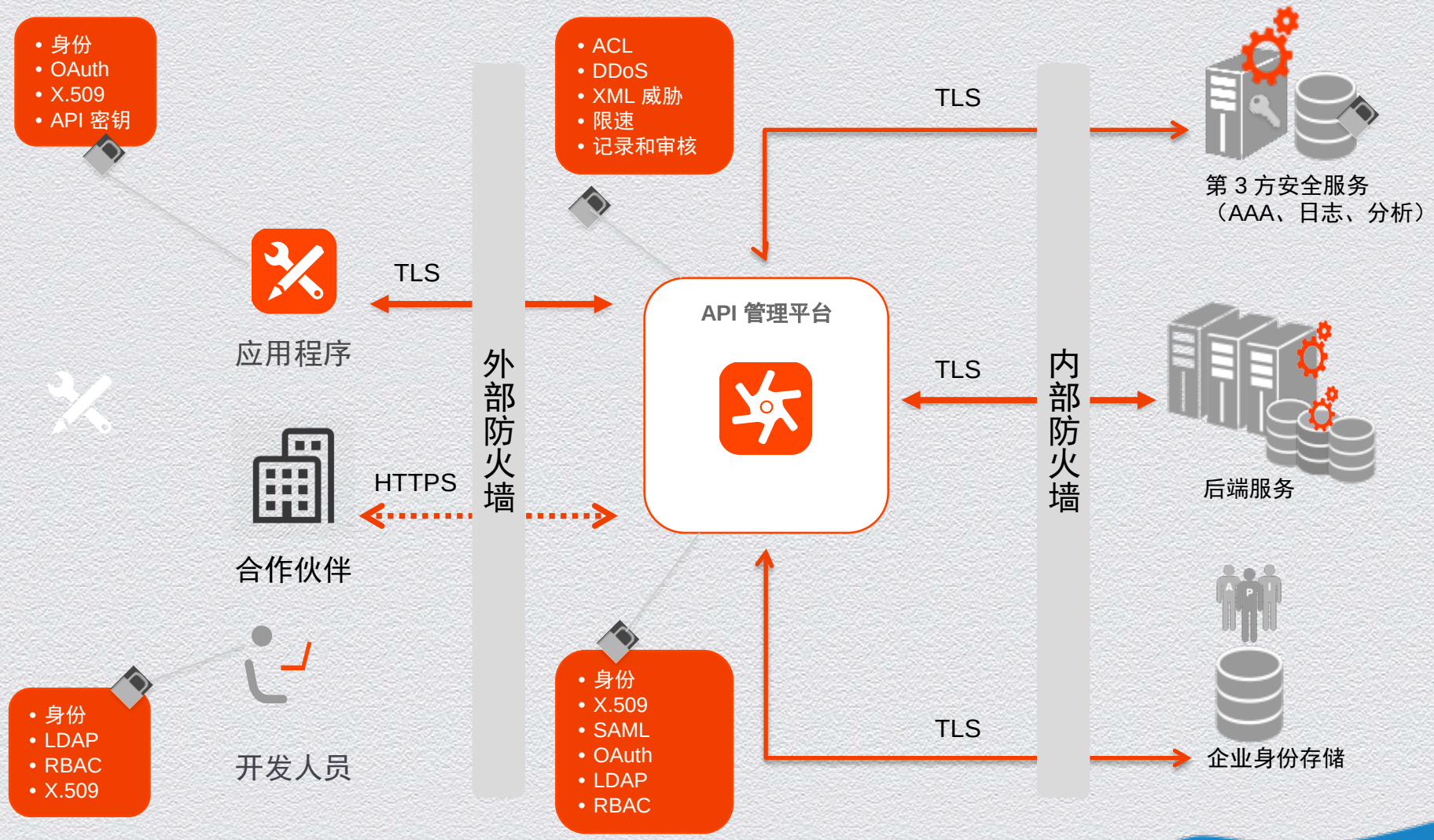
cadence

13

安全体系结构


开发人员
身份和管理
密钥/令牌管理
证书管理
策略管理
RBAC 管理
用户管理
IT 安全人员/
架构师
SOAP
应用程序
API 安全人员
身份验证
授权
策略实施
流量管理
登录和审核
node
密钥存储
策略存储
日志存储
威胁保护
TLS
DDoS
限速和配额
负载保护
分析
法规遵从性（SOC 2、PCI DSS、HIPAA）和云安全

内置安全 + 灵活的安全集成



cadence

身份认证和授权

模拟情景	身份验证	授权
企业对企业	TLS 证书，API 密钥	OAuth 1.0a 和 OAuth 2.0 策略 ◆ 客户端凭据授予（两脚 Oauth）
受信任的开发人员	API 密钥、OAuth 令牌、IP 地址 SAML 身份控制策略 ◆ 生成 SAML 声明 ◆ 验证 SAML 声明	OAuth 1.0a 和 OAuth 2.0 策略 ◆ 资源所有者密码授予
不受信任的开发人员	API 密钥、OAuth 令牌 SAML 身份控制策略	OAuth 1.0a 和 OAuth 2.0 策略 ◆ 授权码授予（三脚 OAuth） ◆ 隐式授予
HTML5 应用程序	双向 TLS	
身份跟踪	基于身份的访问跟踪策略 ◆ 验证 API 密钥	

API 面临的威胁

cadence

API 面临的威胁 — 新增内容。

- 假冒身份
- 由于不良参与者、意外错误和僵尸网络的原因而拒绝服务
- 存在于应用程序和企业后端服务之间的通信链中的网络窃听
- 重播攻击
- 对管理系统和配置数据进行未经授权的访问
- 中间人攻击
- 使用合法 API 调用的速度攻击
- 通过应用程序和开发人员提升权限
- 数据篡改和注入攻击导致信息泄露
- 泄露在移动、API 和后端服务中存储和处理的机密数据
- 凭据、API 密钥、令牌或加密密钥失窃

威胁保护

模拟情景	威胁保护
拒绝服务攻击	Spike Arrest 策略 ◆ 防止流量即时性突发 访问控制策略 ◆ 对可访问您的 API 的人员进行限制
注入和脚本攻击	正则表达式保护策略 ◆ 使您可扫描 SQL、JavaScript 等有效负载
XML/JSON 威胁	XML 和 JSON 威胁保护策略 ◆ 让格式错误的有效负载远离您的系统

身份

模拟情景	身份
用户调配	配置对用户访问数据特征和功能的精细控制。灵活的用户调配和管理。
RBAC 管理	通过现成的角色提高了系统安全性。利用每一层的 RBAC 保护敏感信息。 ◆ API 密钥 ◆ TLS 证书 ◆ OAuth 令牌 ◆ 审核日志
管理组	基于包括位置和兴趣的任意数量标准的方便实用的用户分组。
身份提供商	与任何具有以下特征的身份提供商集成： ◆ 具有 API ◆ 支持 SAML ◆ 支持 LDAP v3（仅针对内部部署）

基础架构和法规遵从性

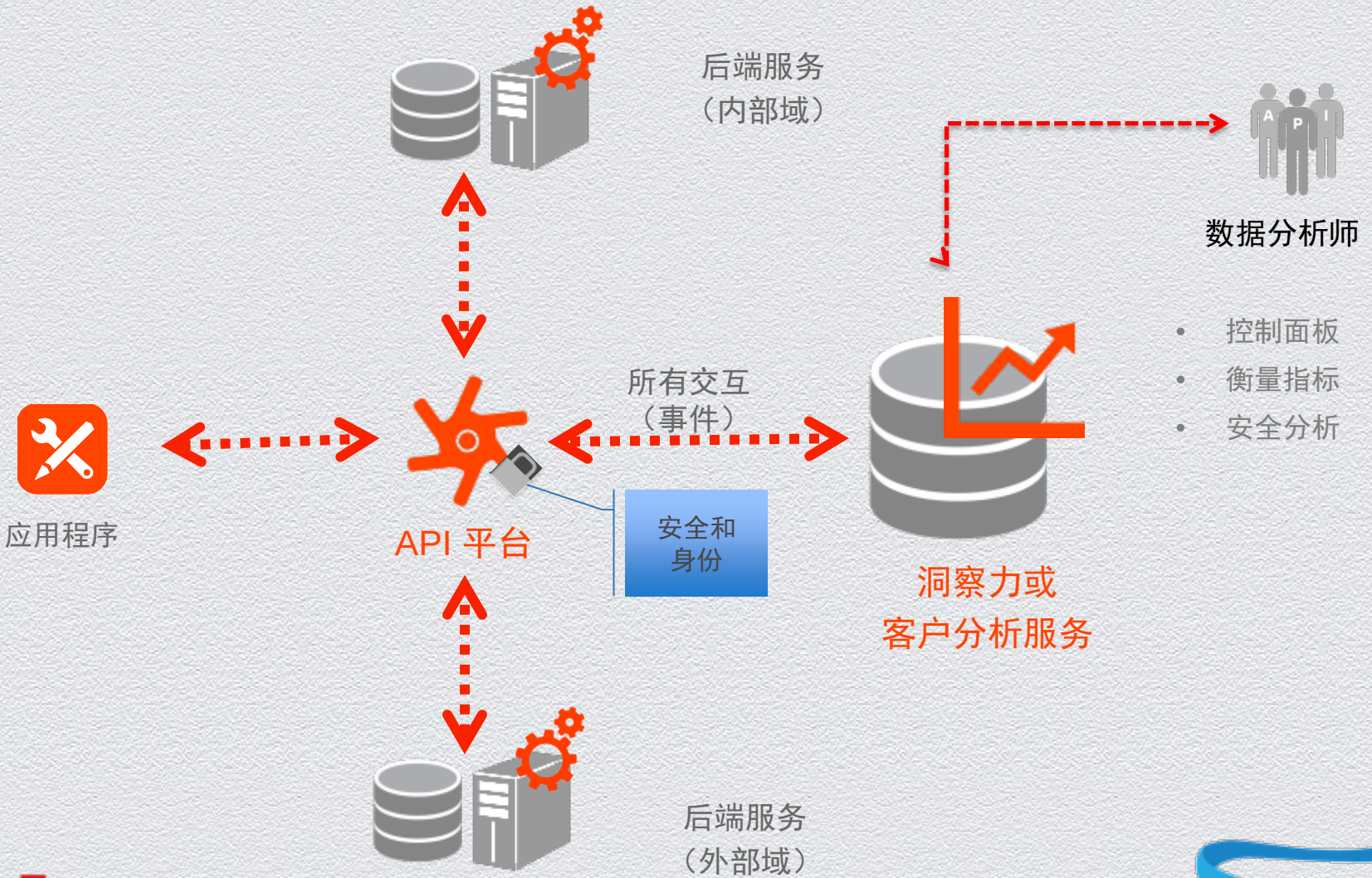
模拟情景	基础架构安全和法规遵从性
SOC 2	您或您的提供商几乎必定需要
PCI-DSS、HIPAA	您或您的提供商可能需要
欧洲数据指令	如果您的提供商在欧洲有业务，则这一项是必须的
API 运行状况监控	全天候监控 ◆ 实时和历史 API 运行状况监控 ◆ API 安全和法规遵从性跟踪 ◆ 组件和进程监控

安全性：不仅仅保护新的渠道

API 正使在渠道范围内集成客户体验变得更容易。

- 与开发人员和企业合作将安全构建到 API 体系结构中
- 仪表安全遥测与您现有的安全信息事件管理系统 (SIEM) 无缝集成
- 通过 API 渠道保护客户 PII 数据并防止数据泄露
- 不仅保护 API 通信层，而且保护有效负载
- 构建能够实际提供价值以及有助于减少新的威胁并管理您的企业所面临的风险的安全分析计划

使用案例 – 保护合作伙伴协作



cadence

23

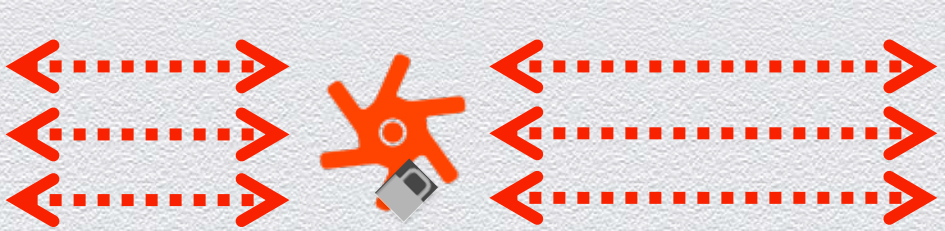
使用案例 – API 启用的数据联合

工具

合作伙伴

分析师

API 管理平台



可实施的多个访问级别

数据存储集成 API

多元化的数据存储

精细的访问控制

cadence

24

下面的内容对应用程序和 API 安全重要吗？

- 用于身份认证的 Kerberos
  - Kerberos 不适合 Web 服务身份认证，可使用 OAuth、OpenID connect for AuthN 和 AuthZ 代替。
- 基于策略管理的 XACML (AuthZ)
  - 由于 XACML 的复杂程度、有效负载大小和对开发人员不够友好（开发人员更喜欢灵活的轻量级机制），其不适合云和移动应用程序。
- WS-* 安全服务
  - 以 SOA 为中心并且对于以 REST 为中心的 API 体系结构来说过于重量级了。

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

谢谢大家！