RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

# APIs – The Next Hacker Target
# Or a Business and Security Opportunity?

SESSION ID: SEC-T07


Tim Mather

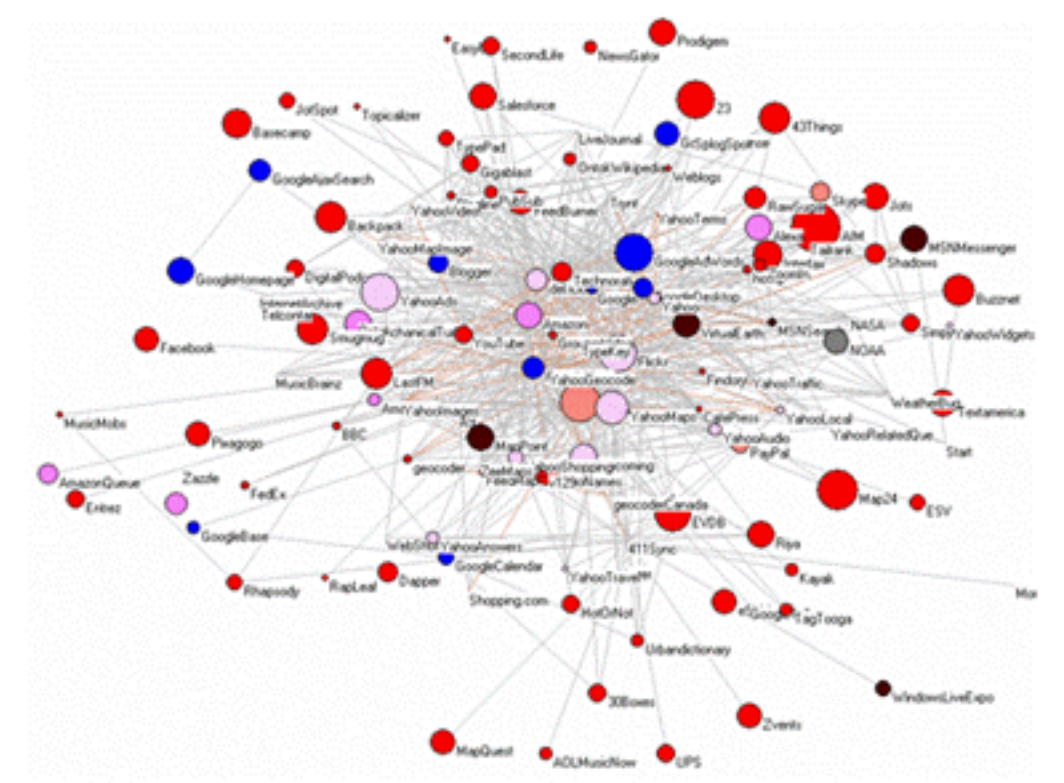
VP, CISO
Cadence Design Systems
@mather_tim


# Why Should You Care About APIs?

- Amazon Web Services EC2 alone has 148 APIs

# Programmable Web

- Tracks over 10,500 APIs publicly available to developers



# API Calls Per Day = Billions Served




# APIs Are Big Business

- Expedia's affiliate network conducts > USD $2 billion worth of transactions per year via APIs alone

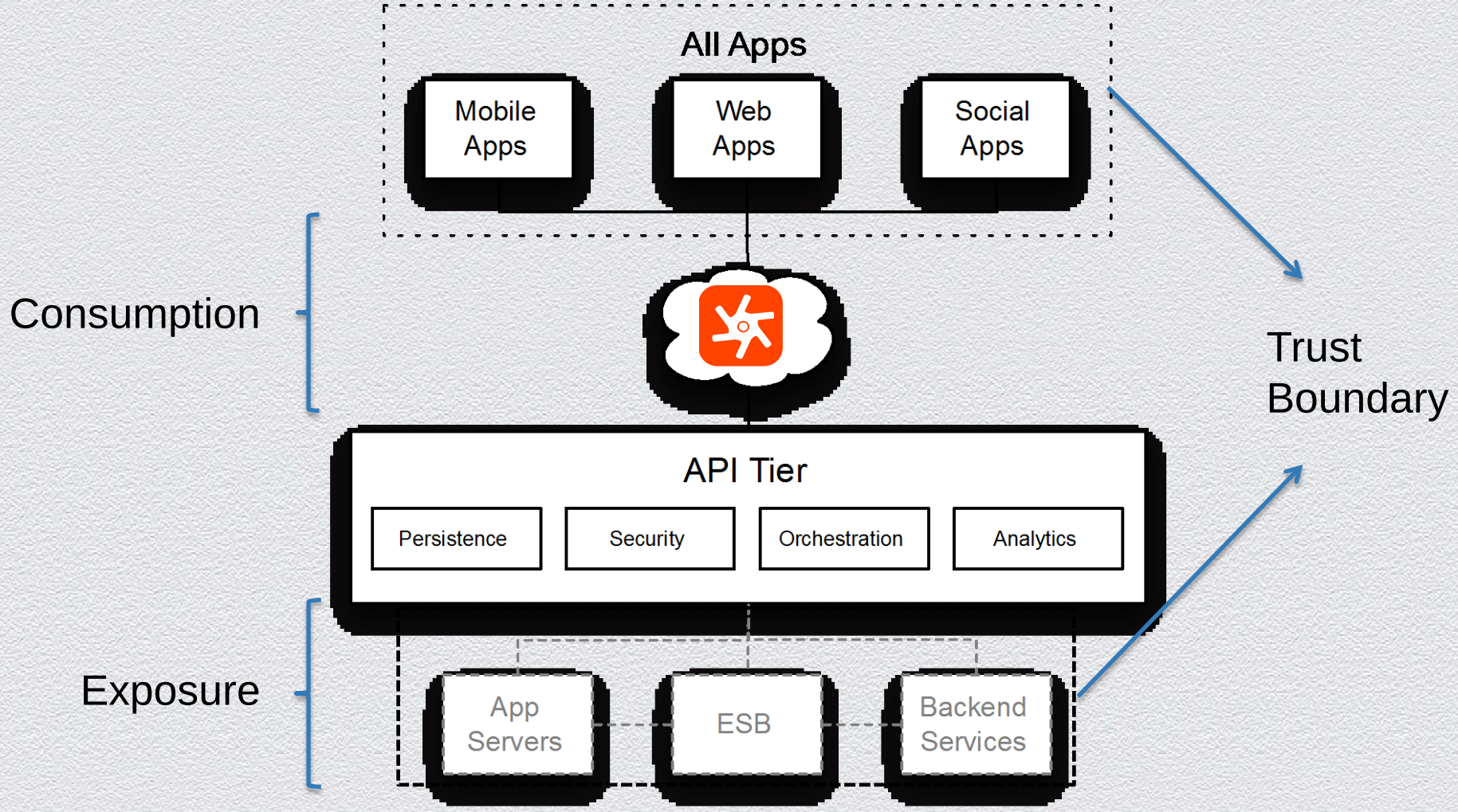
# Reality of API Security

- Snapchat API hack December 2013
  - Personal information breach
    - Mass phone number harvesting
    - Creation of bogus accounts
    - Poised to become a mass spamming platform

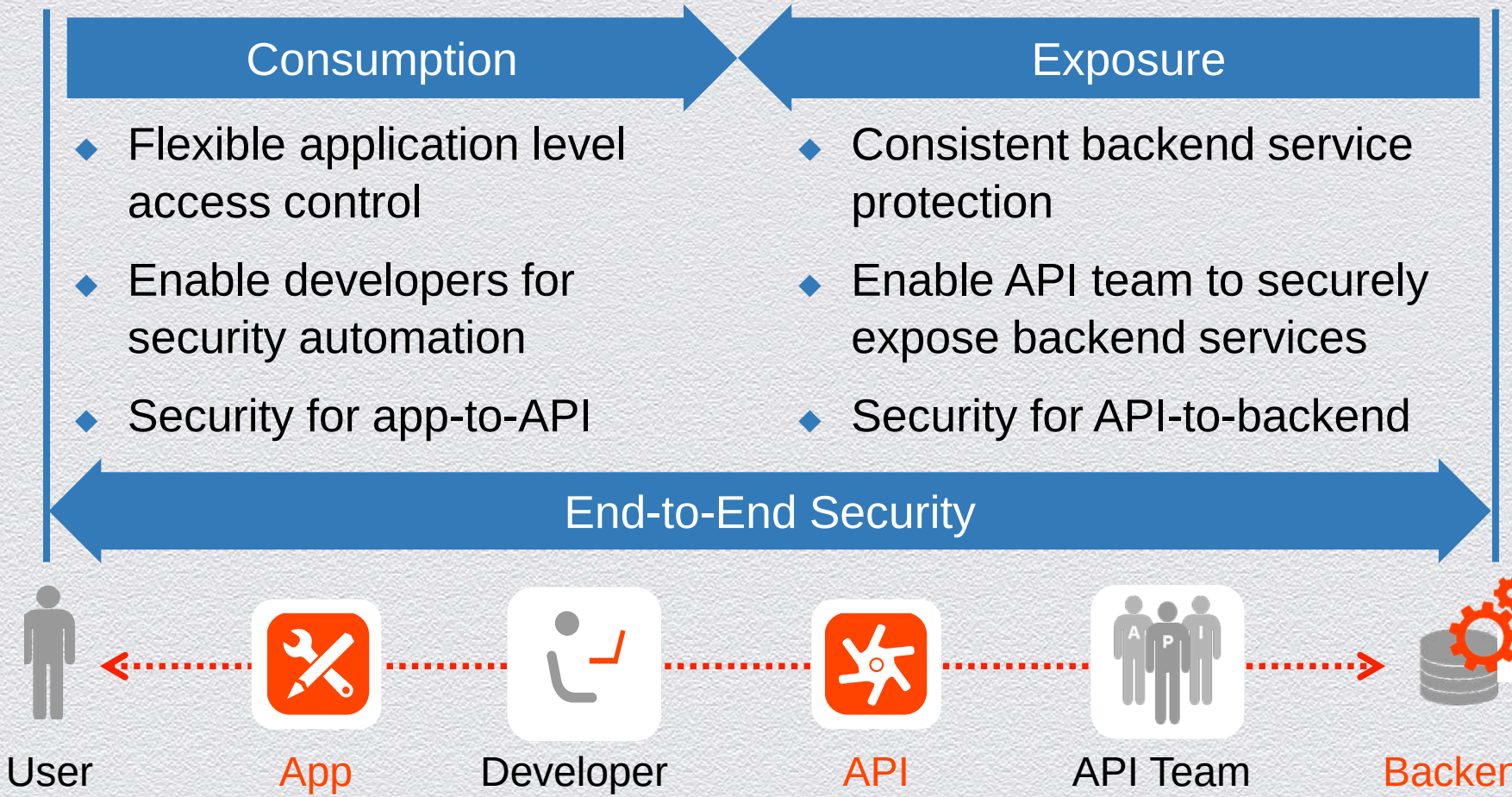
# Where to Begin?

- Do you even know what APIs your organization has or is using?
- Do you even know what data is being shared via APIs with your trusted and untrusted customers, partners, and / or vendors?

# Consumption versus Exposure



# End-to-End Security is Needed



# Edge Delivers End-to-End Security

| Stakeholders | API Exposure Security | API Consumption Security |
|---|---|---|
| DevOps | ☑ | ☑ |
| App Developers | | ☑ |
| IT security | ☑ | ☑ |
| API architects | ☑ | |
| Business owner | ☑ | ☑ |
| End users | | ☑ |

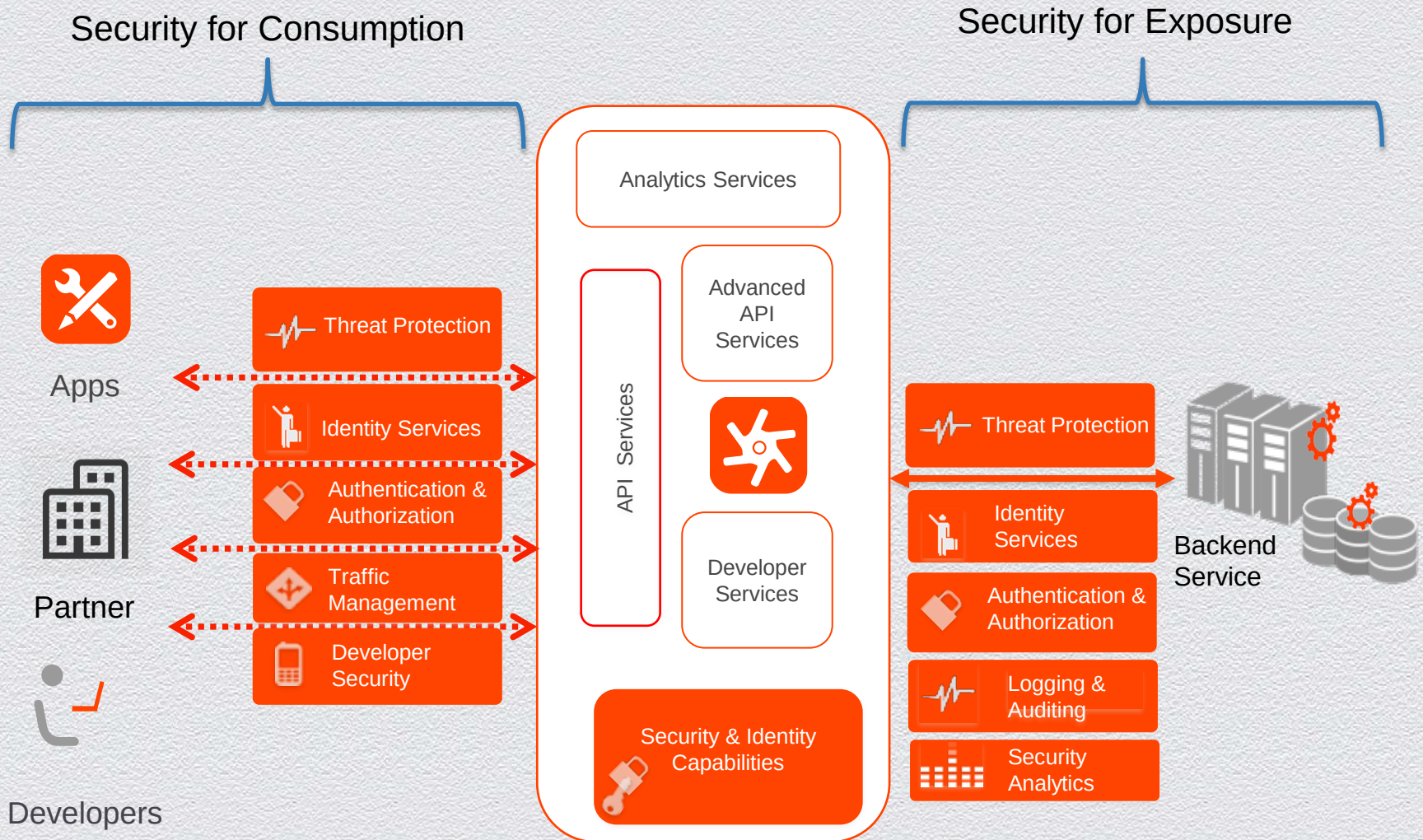
API management solutions must address the security considerations of various stakeholders and consumers of APIs

cadence

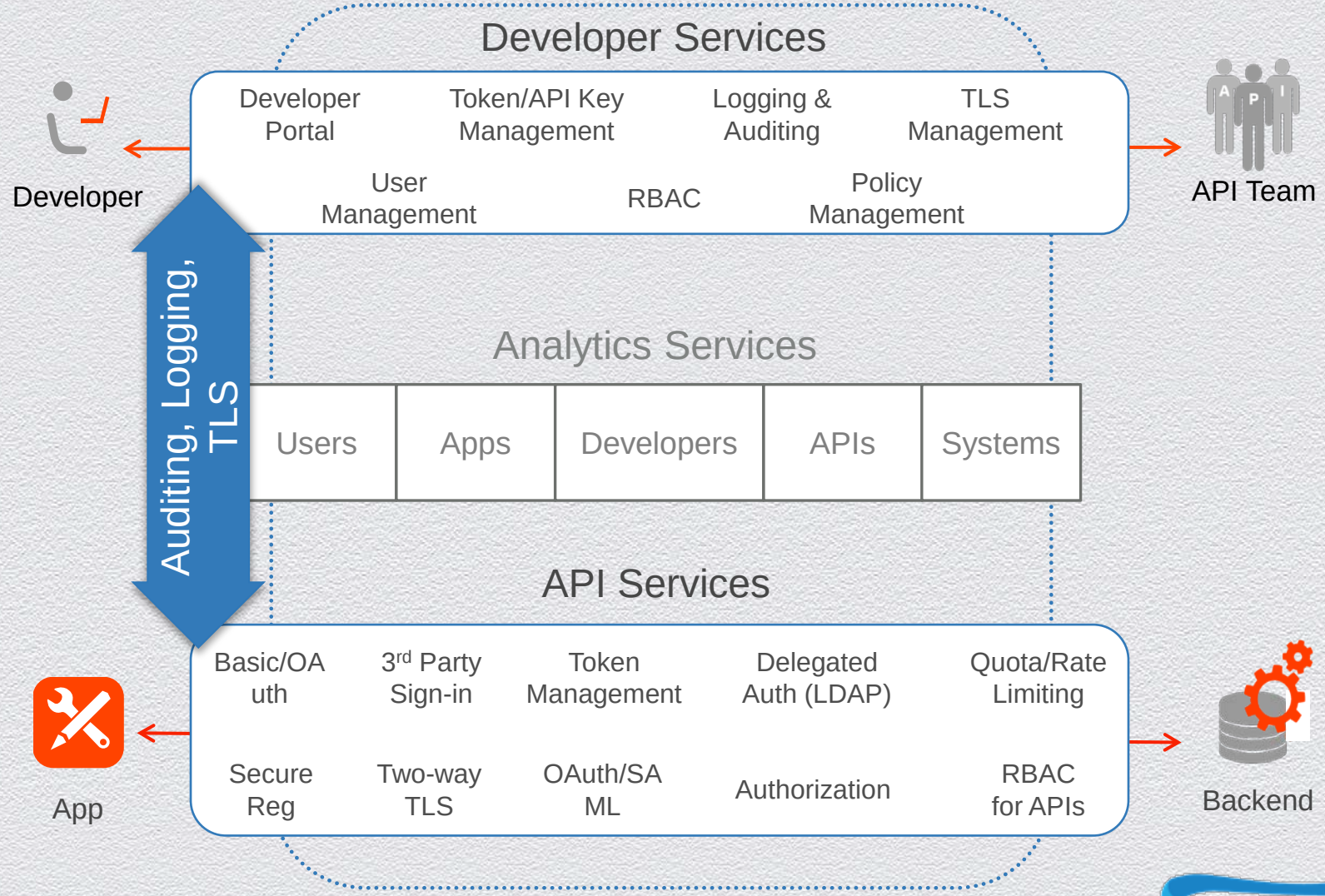


10

# Security Components



# End-to-End Security for App & API Developers



# Delivering a Secure App and API Infrastructure

## App to API (Consumption)

- Authentication (TLS, OAuth, API key)
- API key and token management
- Two-way TLS
- Authorization (permission management)
- Runtime policy
- SLA enforcement
- Logging and auditing

## API to Backend (Exposure)

- Authentication (TLS, OAuth, SAML)
- Two-way TLS
- Delegated authentication (LDAP, AD)
- Integration with custom identity providers
- Fine grain authorization
- Logging and auditing

## Analytics

- Security reports
- Run time detection reports (volume based, traffic properties)

## Threat Protection

- XML/JSON Poisoning/Injection
- SQL Injection
- DDoS/App-DoS Attacks
- Quota/Spike Arrest
- IP based access restrictions

## Identity

- User provisioning
- RBAC management
- Groups
- Identity provider

## Infrastructure Security and Compliance

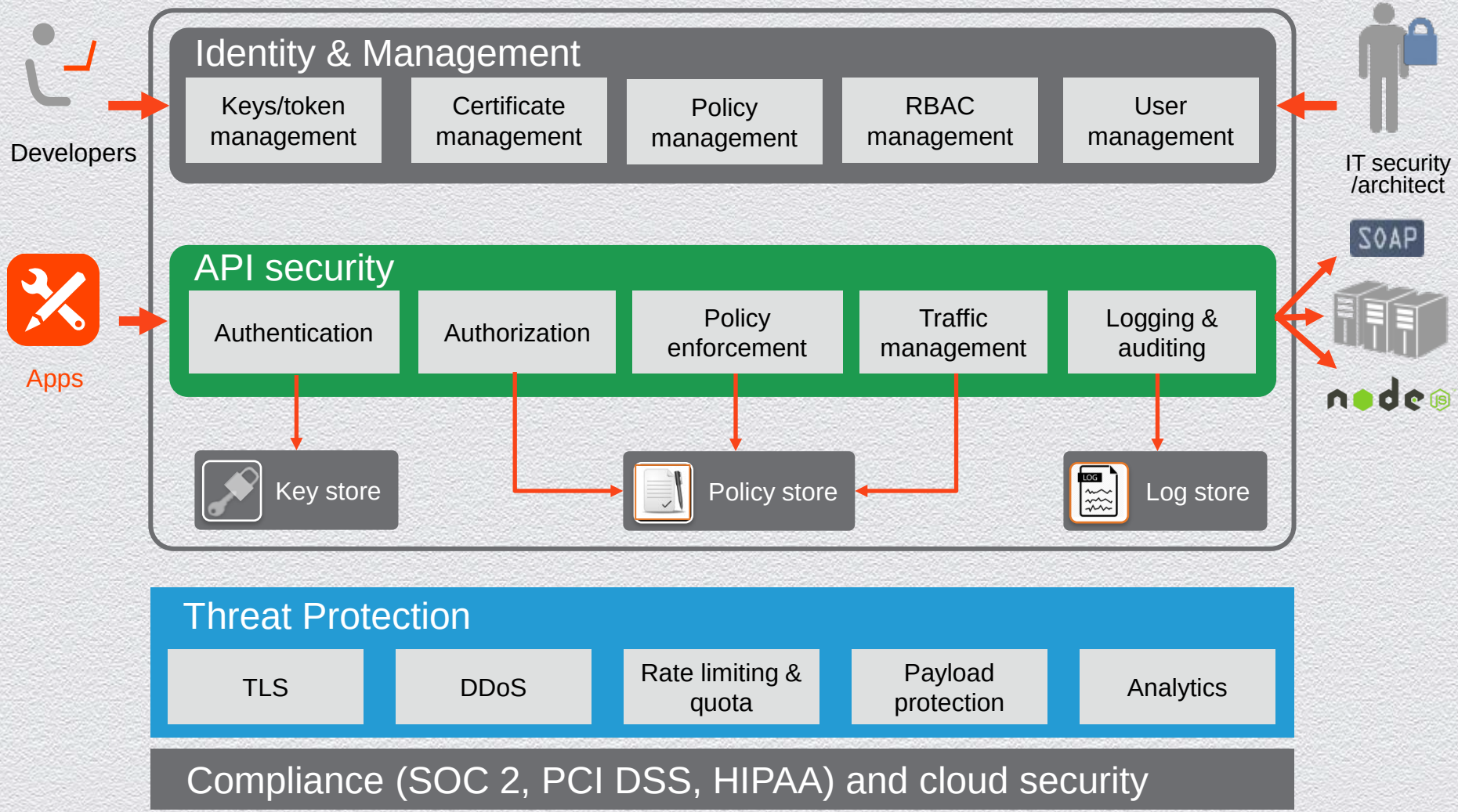
- Cloud or on-premise
- Cloud-based security (AWS + other)
- SOC 2, PCI-DSS, HIPAA
- 24 x 7 organizational support

cadence

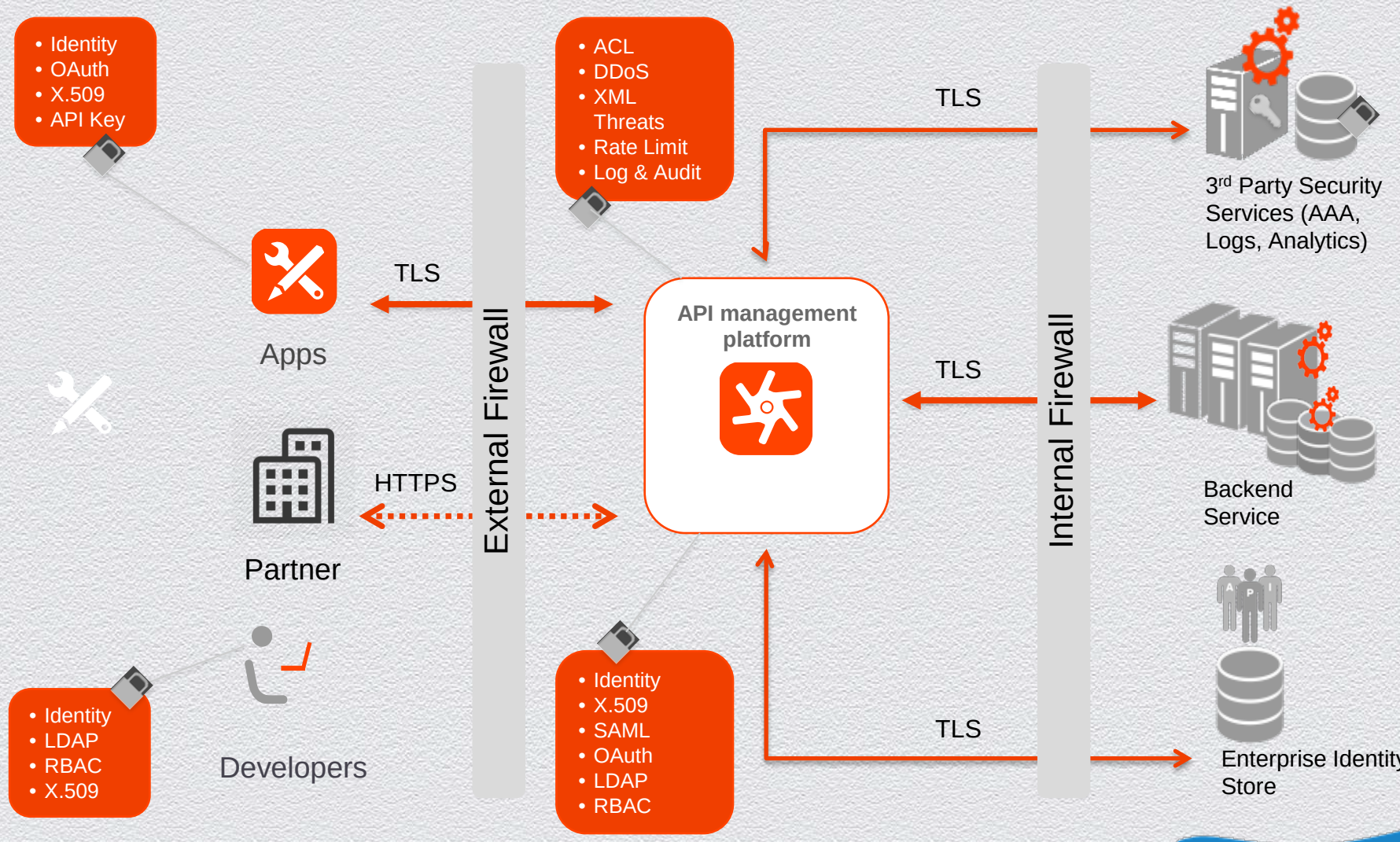


13

# Security Architecture



# Built-in Security + Flexible Security Integration




cadence

# Authentication & Authorization

| Scenario | Authentication | Authorization |
|---|---|---|
| Business to Business | TLS Cert, API Key | OAuth 1.0a & OAuth 2.0 policies<br>◆ Client credentials grant (two-legged Oauth) |
| Trusted developers | API Key, OAuth Token, IP Address<br>SAML identity control policies<br>◆ Generate SAML Assertion<br>◆ Validate SAML Assertion | OAuth 1.0a & OAuth 2.0 policies<br>◆ Resource owner password grant |
| Untrusted developers | API Key, OAuth Token<br>SAML identity control policies | OAuth 1.0a & OAuth 2.0 policies<br>◆ Authorization code grant (three-legged OAuth)<br>◆ Implicit grant |
| HTML5 applications | Two-way TLS | |
| Identity tracking | Identity-based access tracking policy<br>◆ Verify API Key | |

cadence

# Threats to APIs

cadence

# API Threats – What Is New?

- Spoofing of identity
- Denial of service by bad actors, inadvertent errors, and botnets
- Network eavesdropping in the communication chain between app and enterprise backend services
- Replay attacks
- Unauthorized access to management system and configuration data
- Man-in-the-middle attacks
- Velocity attack using legitimate API calls
- Elevation of privilege by applications and developers
- Data tampering and injection attacks that lead to information disclosure
- Disclosure of confidential data stored and processed in mobile, API, and backend services
- Theft of credentials, API keys, tokens, or encryption keys

# Threat Protection

| Scenario | Threat Protection |
|---|---|
| Denial of Service attack | Spike Arrest policy<br>◆ Protection against instantaneous bursts of traffic<br><br>Access Control policy<br>◆ Imposing limits on who can access your API |
| Injection and Scripting attacks | Regular Expression Protection policy<br>◆ Allow you to scan payloads for SQL, JavaScript, etc. |
| XML/JSON threats | XML and JSON Threat Protection policies<br>◆ Keep malformed payloads out of your system |

# Identity

| Scenario | Identity |
|---|---|
| User Provisioning | Configure fine-grain control of user access to data features and functionality. Flexible provisioning and management of users. |
| RBAC Management | Enhanced system security with out-of-the-box roles. Employ RBAC at every layer to protect sensitive information<br>◆ API keys<br>◆ TLS certificates<br>◆ OAuth tokens<br>◆ audit logs |
| Manage Groups | Convenient and practical grouping of users based on any number of criteria including location and interests. |
| Identity Provider | Integrate with any identity provider that:<br>◆ has an API<br>◆ supports SAML<br>◆ supports LDAP v3 (for on-premise only) |

# Infrastructure & Compliance

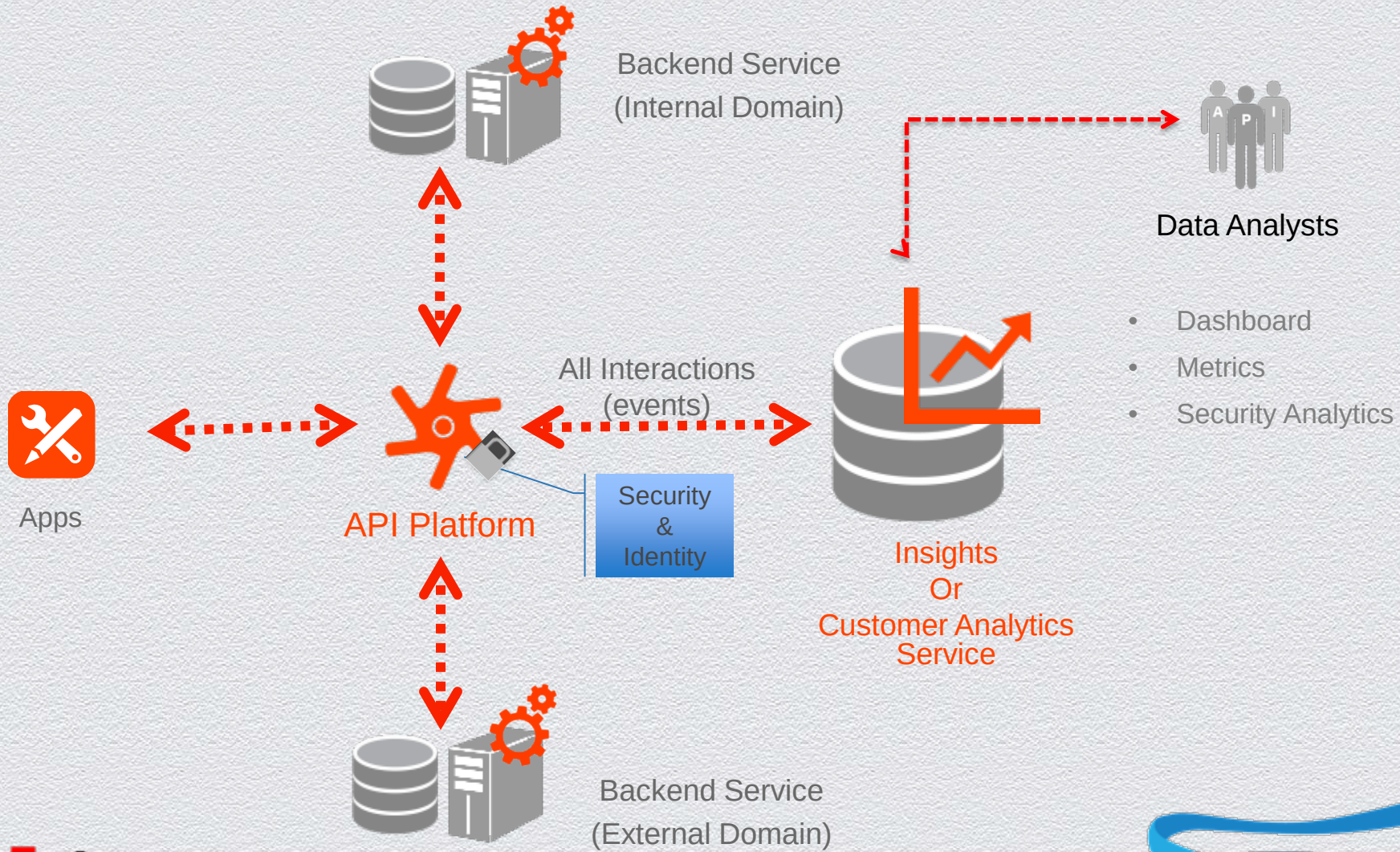
| Scenario | Infrastructure Security & Compliance |
|---|---|
| SOC 2 | You or your provider will almost certainly need this |
| PCI-DSS, HIPAA | You or your provider might need this |
| European Data Directive | If you or your provider are doing business in Europe, then this will be required |
| API ‘health’ visibility | Round-the-clock monitoring<br>◆ Real-time and historic API health visibility<br>◆ API security and compliance tracking<br>◆ Component and process monitoring |

# Security: More Than Securing a New Channel

*APIs are making it easier to integrate the customer experience across channels.*

- Partner with developers and the business to build security into the API architecture
- Instrument security telemetry to seamlessly integrate with your existing Security Information Event Management System (SIEM)
- Protect customer PII data and prevent data breaches via API channels
- Secure not just the API communications layer but also the payload
- Build a security analytics program that will actually provide value and help mitigate new threats and manage risk to your enterprise

# Use Case – Secure Partner Collaboration



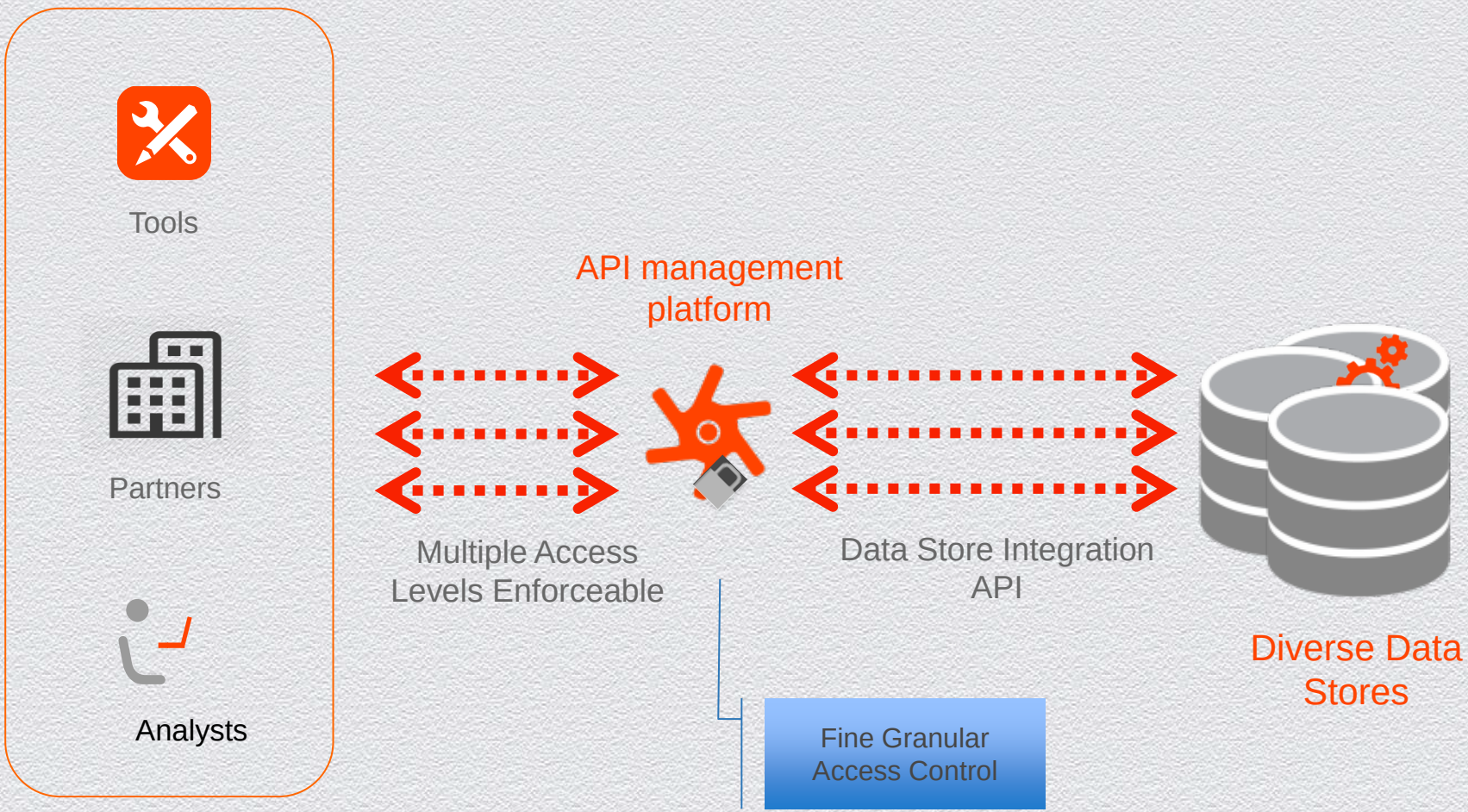

cadence





23

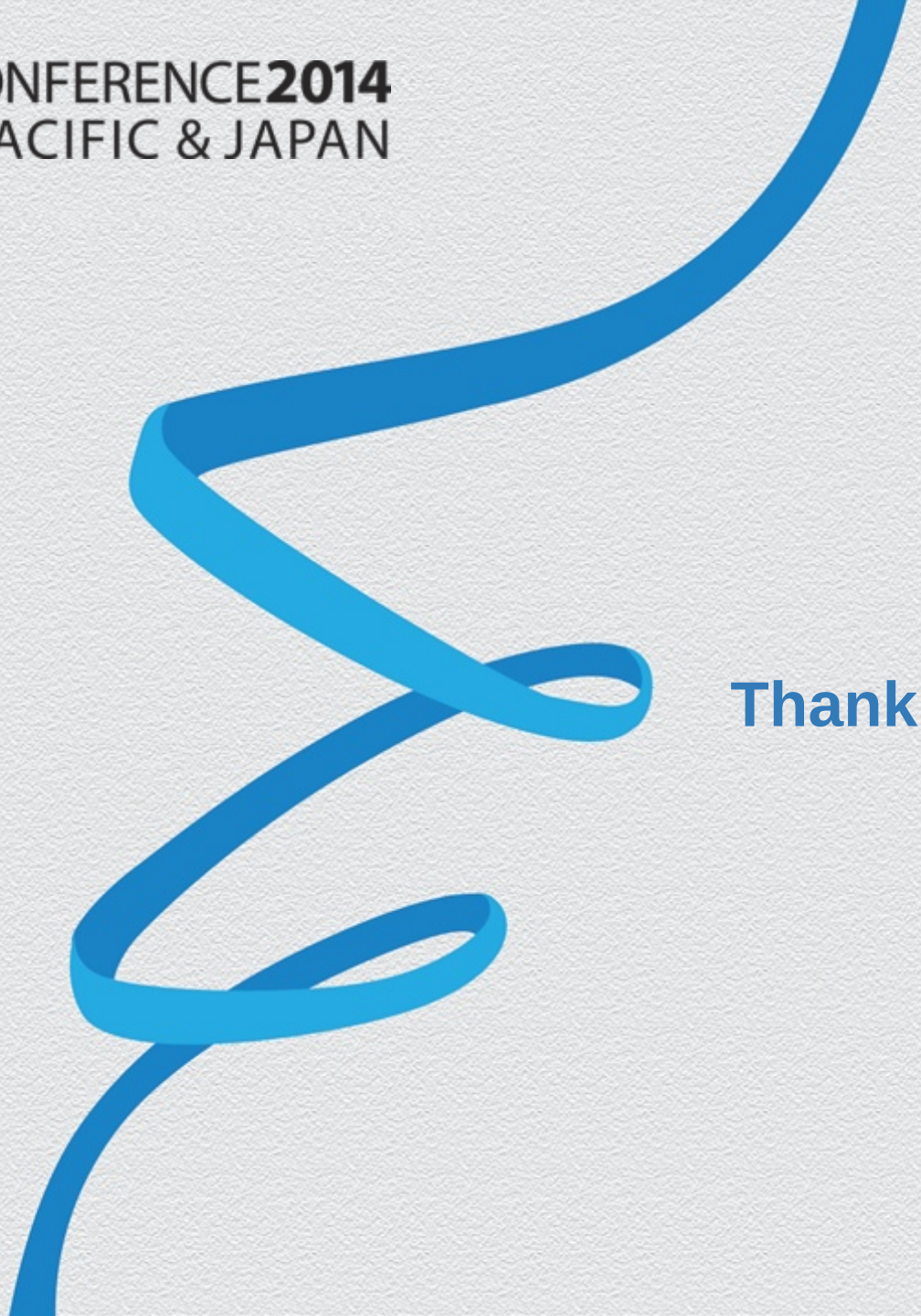
# Use Case – API Enabled Data Federation



# Do The Following Matter in App & API Security?

- Kerberos for authentication
  - Kerberos is not suitable for Web services authentication and can be replaced with OAuth, OpenID connect for AuthN and AuthZ.
- XACML based policy management (AuthZ)
  - XACML not suitable for cloud and mobile apps given the complexity, payload size and not friendly to developers who prefer lightweight mechanisms that promote agility.
- WS-* security services
  - SOA centric and heavy weight for REST centric API architecture.

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN



# Thank You