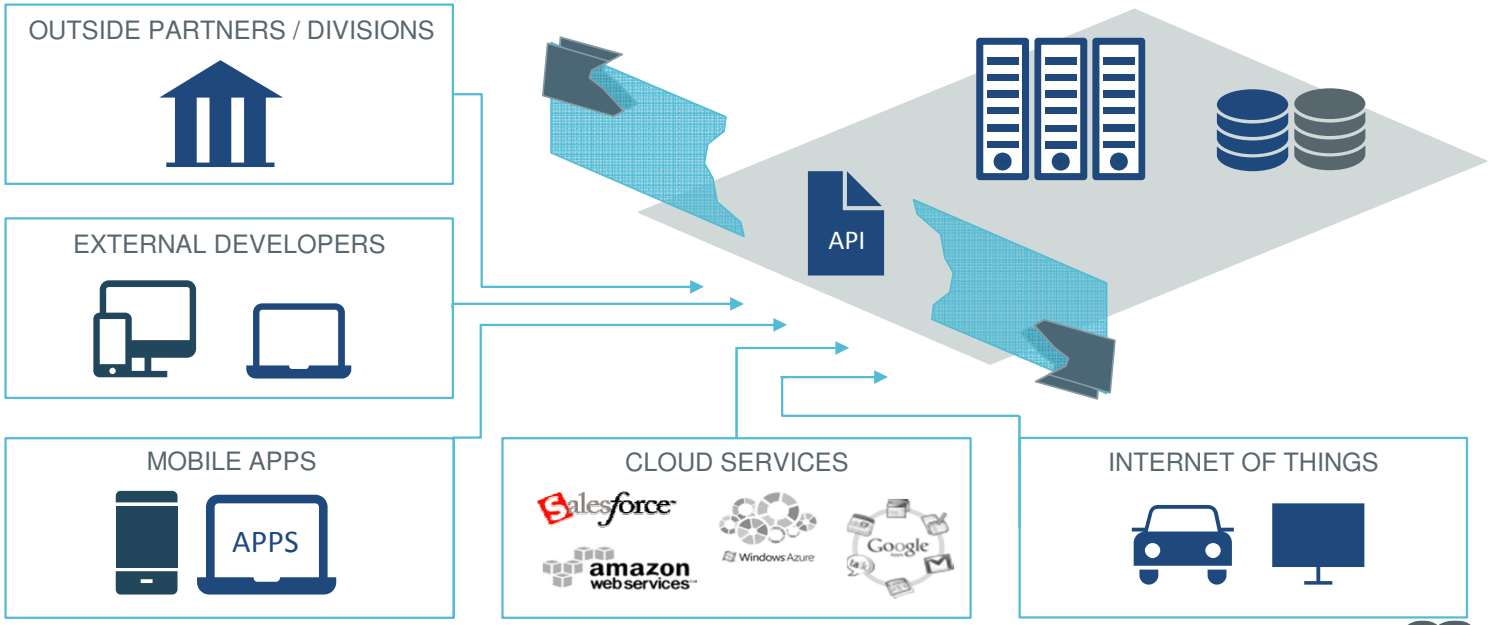
API Security – Key Considerations for Securing APIs

Dinesh Chandrasekhar – Director, Product Marketing
Balaji Radhakrishnan – Sr. Principal Consultant, Pre-Sales

Agenda

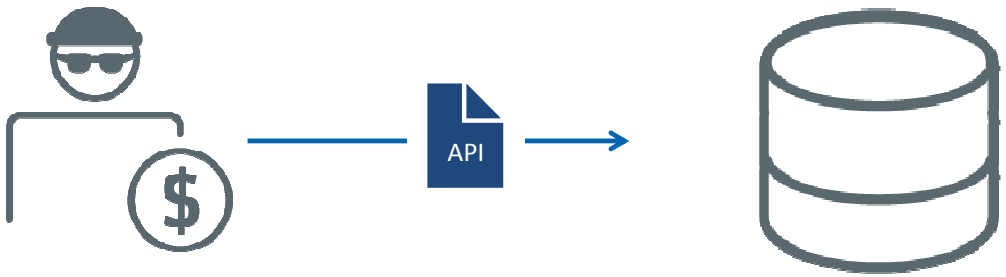
1. API BREACHES
2. RISK MITIGATION STEPS
3. API MANAGEMENT SOLUTIONS
4. DEMO

APIs at the center



APIs expose sensitive data

APIs are also the attack vector of choice for hackers to disrupt your service or gain access to private information



Prominent API Breaches

Confirmed: Snapchat Hack Not A Hoax, 4.6M Usernames And Numbers Published

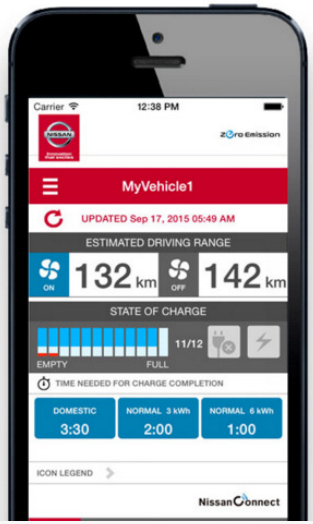
Yahoo Admits It Was Breached but Not Shellshocked

MoonPig's API breach could cost its business

API Vulnerability Exposed Accounts of Delmarva Power Customers

Hacked passwords can enable remote unlocking, tracking of Tesla cars

Nissan Leaf - Hacked



```
GET https://[redacted].com/orchestration_1111/gdc/ACRemoteRequest.
php?RegionCode=NE&lg=no-NO&DCMID=&VIN=SJNFAAZE0U60XXXXX&tz=Europe/
Paris
```

- Communication between the Nissan mobile app, Nissan servers, and Nissan Leaf electric vehicles took place over completely unencrypted, unauthenticated APIs.
- Breach allowed a hacker, using only a web browser, to remotely control the car's climate functions, and read private data including userID, battery status, range, charging information, and driving history

Top API Vulnerabilities and Mitigation Steps

When an API is hacked . . .

- API vulnerabilities surface
  - When exploits are discovered by the API publisher
  - When discovered by 3rd party
  - When an organization is actually hacked
- Exploits are rarely documented
- Public APIs are most scrutinized
- Private/Hidden APIs are also vulnerable

Top-5 vulnerabilities/mitigations

- Most common/current vulnerabilities and mitigations for securing your API
  - Client impersonation
  - Phishing
  - Brute force
  - Injections
  - Unauthorized access/compromised secrets

Client impersonation

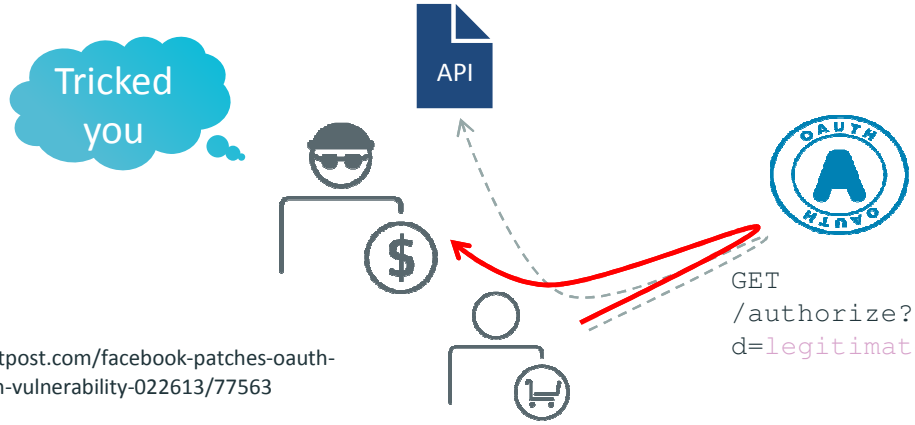
- An attacker reverse-engineers a secret assigned to an app and uses it to call an API pretending to be the legitimate app
- E.g. Twitter OAuth Keys Leaked
  - March 2013
- E.g. Snapchat
  - December 2013

Client impersonation mitigation #1

- It's either confidential, or it isn't
  - Don't 'hide' a secret on a public app store or render it on a web page
- Learn to 'let go' of your app once published
  - Design security mechanisms assuming public clients
  - Don't grant access to resource based solely on the app identity (require user auth)

Phishing attacks

- Risk associated with redirection-based handshakes
  - Malicious ‘application’ pretends to be legitimate
  - Inserts its own endpoint in callback address
  - Gets token
- *E.g. Facebook February 2013



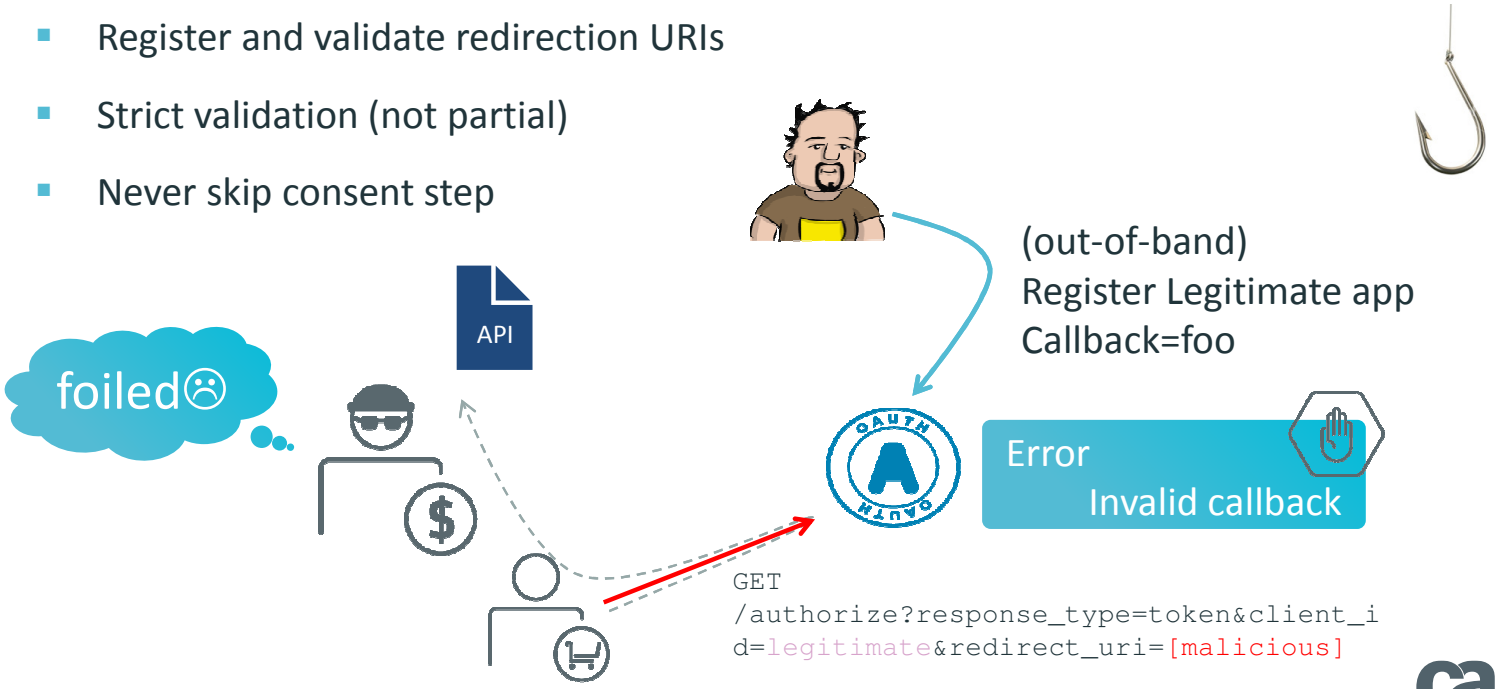
Do you authorize *Legitimate* app to access API on your behalf?

[X] Yes
[ ] No

*http://threatpost.com/facebook-patches-oauth-authentication-vulnerability-022613/77563

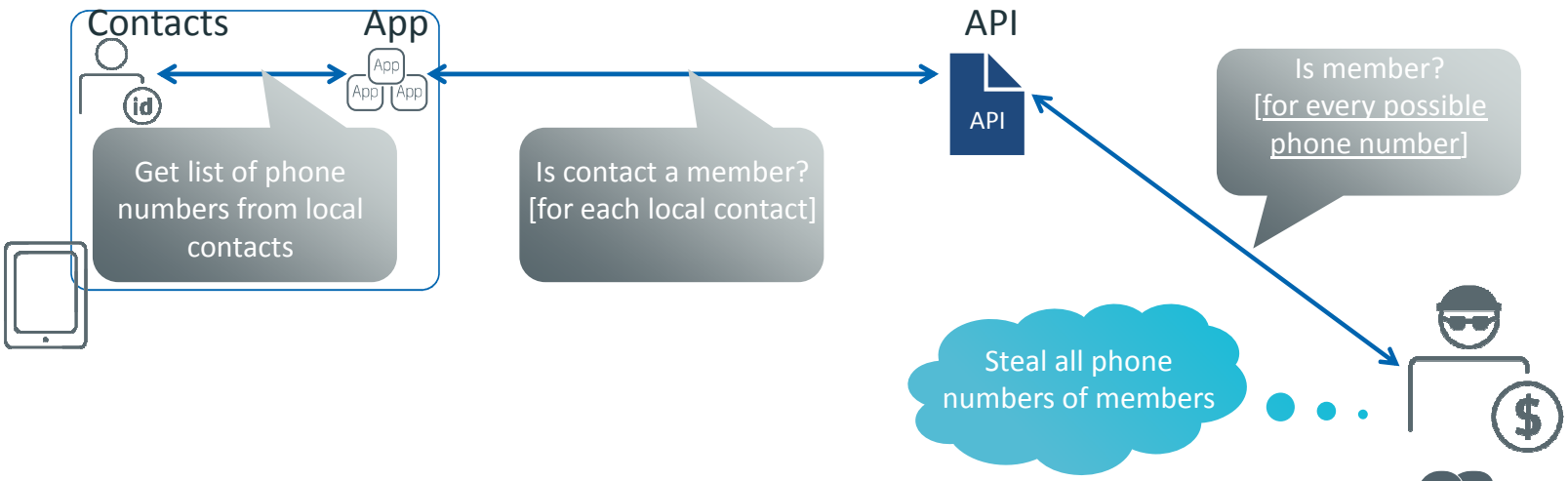
Phishing mitigation 101

- Register and validate redirection URIs
- Strict validation (not partial)
- Never skip consent step



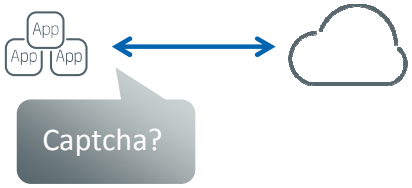
Brute force

- E.g. snapchat find_friend exploit
  - December 2013



Brute force mitigation

Supporting headless clients

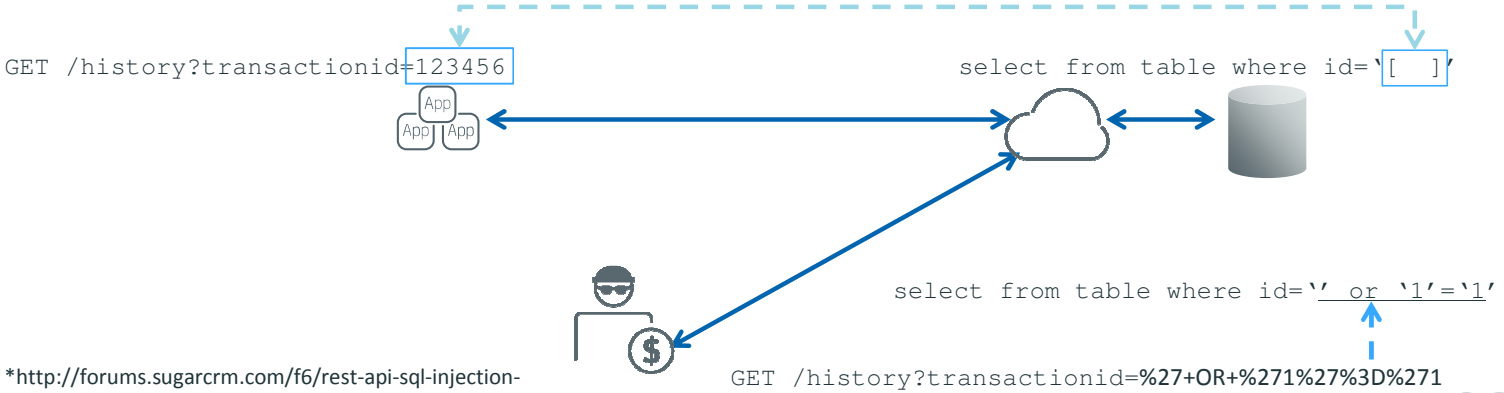


Rate Limiting, Quotas, SLAs

- Targeted rate limiting specific attack vectors
  - Limit access to any resource granted without direct ownership
  - Limit failed authentication, limit password resets
- Detect brute force pattern and block
- Correlate identity, location, concurrency
- Rate limit to protect backend API
  - Global limits to prevent DoS
- Apply rate-limiting with application level awareness
  - Limit for a specific operation for each user/application
  - Limit for a specific input for each user/application

Injection

- Injection attacks, particularly in public clients scenario is at the core of the most common exploits
  - SQL/LDAP/Xpath/Xquery/Code injections
- *E.g. Injection in query parameters



*http://forums.sugarcrm.com/f6/rest-api-sql-injection-exploit-89589/

Injection Mitigation

- Input sanitization
  - Parse input parameters (payload/transport)
  - Apply pattern validation
  - JSON Path, XPath, XSD, JSON Schema, RegEx, …
  - Own and tighten your metadata
  - Code-level sanitization (e.g. Prepared Statements)
- Signature-based threat detection
  - Look for injection patterns in payload and at transport level

Unauthorized access

- E.g. Unsecured API
- E.g. Authenticated client can access resource that should be restricted
- E.g. Session secret compromised

Balancing UX and Security

More Convenience
More Risk

Less Convenience
Less Risk

Unauthorized Access Mitigation

- Authentication
  - Local auth, integration into existing identity providers
  - Social provider integration
  - Federation, SAML
- Token issuing, lifecycle management
  - OAuth, OpenID Connect
  - JWT/JWS
  - Token refresh, revocation
- Assert user/app/device identities
- Scope
  - User-granted permissions
- Resource Server
  - Map token identities and resource ownership
- Identity mapping
  - SAML/OAuth/local/Kerberos/…
  - Runtime mapping internal/external

How API Management can help

CA API Management

Building Blocks of Digital Transformation

Outside the Enterprise

- Internet of Things
- Mobile
- SaaS/Cloud Solutions
  AWS, Google, SFDC …
- Partner Ecosystems
- External Developers

Integrate and **Create**

- Instantly connect SOA, ESB, and legacy applications
- Aggregate data including NoSQL up to 10x faster
- Build scalable connections to cloud solutions like Salesforce
- Easily create live REST APIs with valuable business logic

Secure the Open Enterprise

- Protect against threats and OWASP vulnerabilities
- Control access with SSO and identity management
- Provide end-to-end security for apps, mobile, and IoT

Accelerate Mobile/IoT Development

- Simplify and control developer access to data
- Build a wider partner or public developer ecosystem
- Leverage tools that reduce mobile app delivery time

Unlock the Value of Data

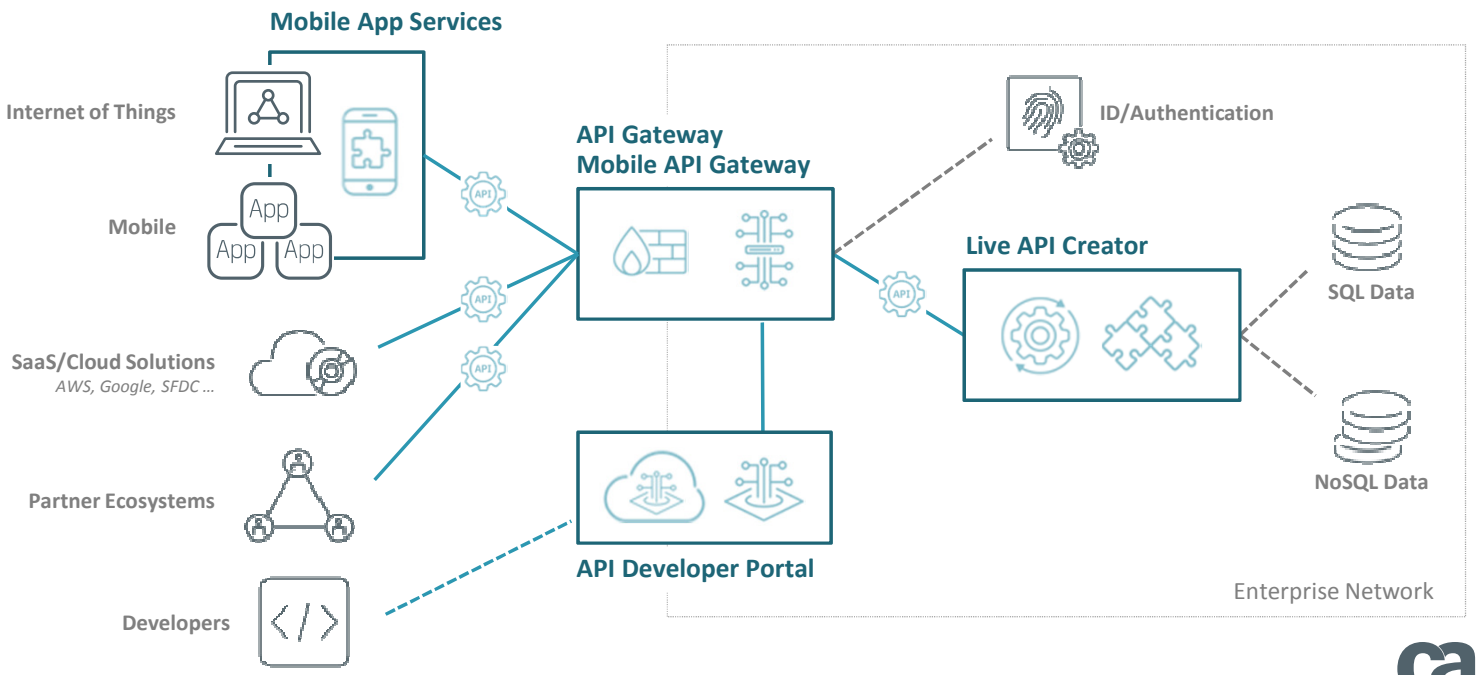
- Monetize APIs to generate revenue
- Build digital ecosystems to enhance business value
- Create efficiencies through analytics and optimization

Within the Enterprise

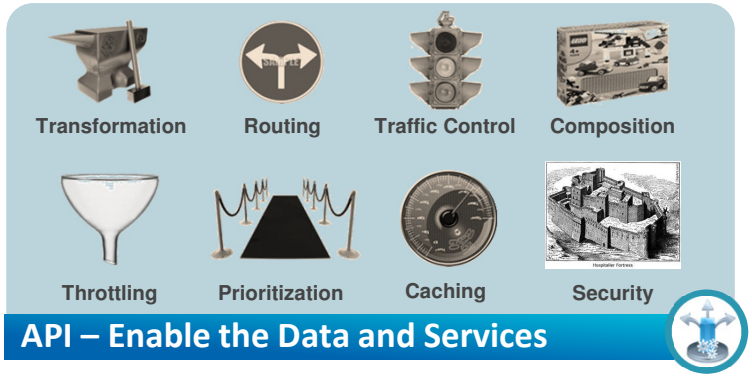
- Secure Data
- Application Portfolio
- ID/Authentication
- Reporting & Analytics
- Internal Teams

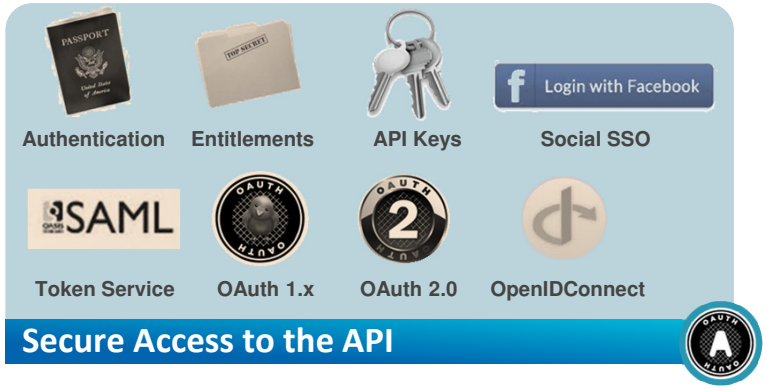
CA API Management

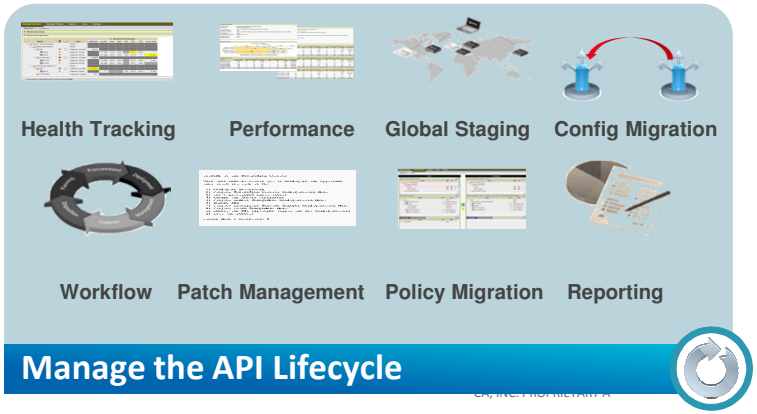
Product Family Architecture



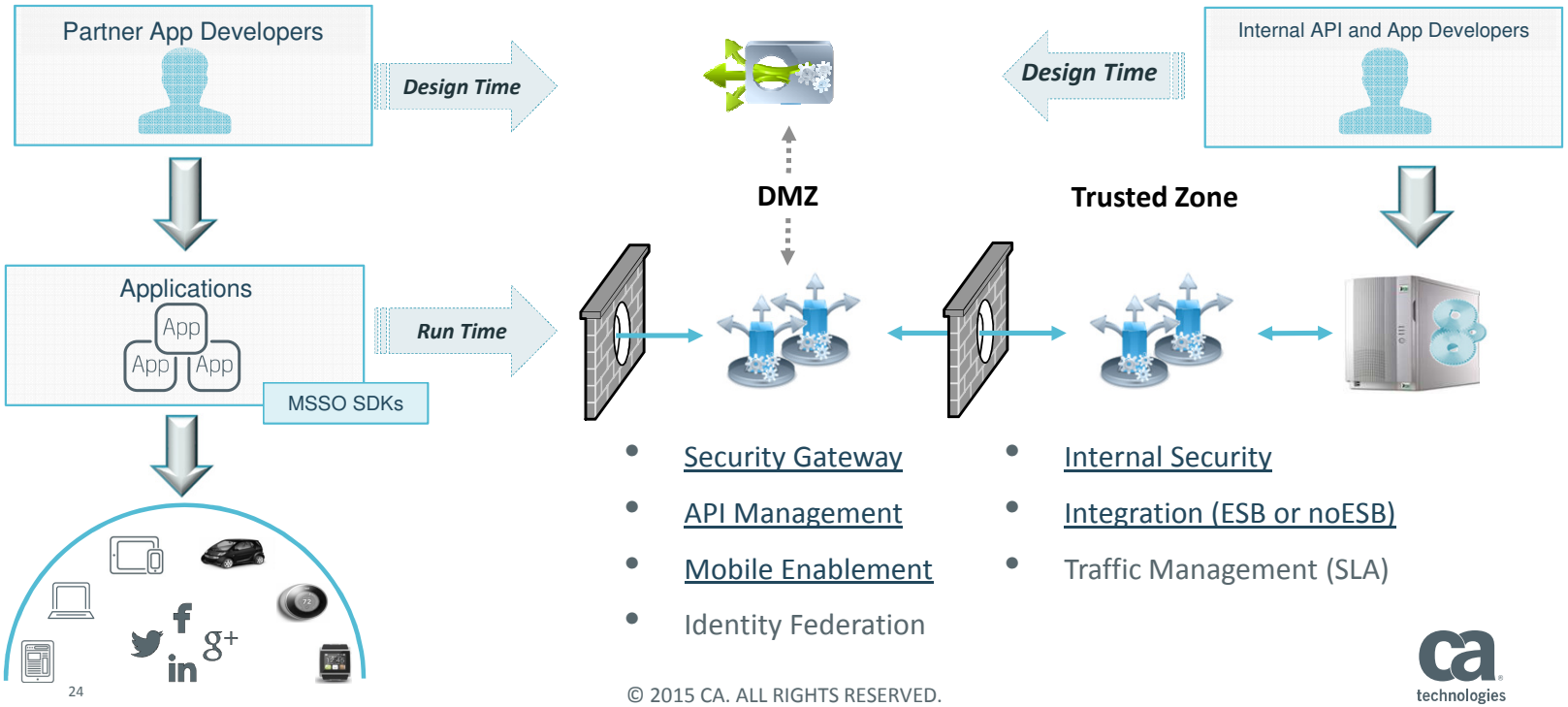
CA API Management Suite







CA API Management Suite Use Cases and Deployment



- Security Gateway
- API Management
- Mobile Enablement
- Identity Federation

- Internal Security
- Integration (ESB or noESB)
- Traffic Management (SLA)

Brief Demonstration

CA Live API Creator

Data Source Integration (SQL & noSQL)

API Developer Portal
(for discovering, exploring, registering to access and monitoring utilization of APIs)

Security:
API Keys, OAuth, SAML, JWT, LDAP, FIPS etc.,

REST & SOAP WS calls

Backend Legacy Services
Service Virtualization

Back end Systems
ESB's

(Mobile) API Gateway
(for runtime policy enforcement)

LDAP Integration for SSO
Oauth, SAML, WS Security & Adv Auth
Two Factor and Multi Factor Authentication

Policy Manager
(for policy authoring and administration)

Dinesh Chandrasekhar

Director API Management Product Marketing

Dinesh.Chandrasekhar@ca.com

@AppInt4All

Legal Notice

THIS PRESENTATION IS FOR YOUR INFORMATIONAL PURPOSES ONLY. CA assumes no responsibility for the accuracy or completeness of the information. TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. In no event will CA be liable for any loss or damage, direct or indirect, in connection with this presentation, including, without limitation, lost profits, lost investment, business interruption, goodwill, or lost data, even if CA is expressly advised of the possibility of such damages.