Enterprise API Security Choices:

One API, Total Security

Blake Dournaee

Senior Product Manager

Intel Data Center Software Division

Securing All Channels to the Enterprise

Mobile/HTML5

Mobile/Native

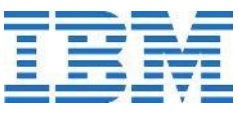
Web Browser

Internal Devs

External Devs/3rd Party Apps

Kiosk/Thick client

One API set, any channel, with Enterprise Security



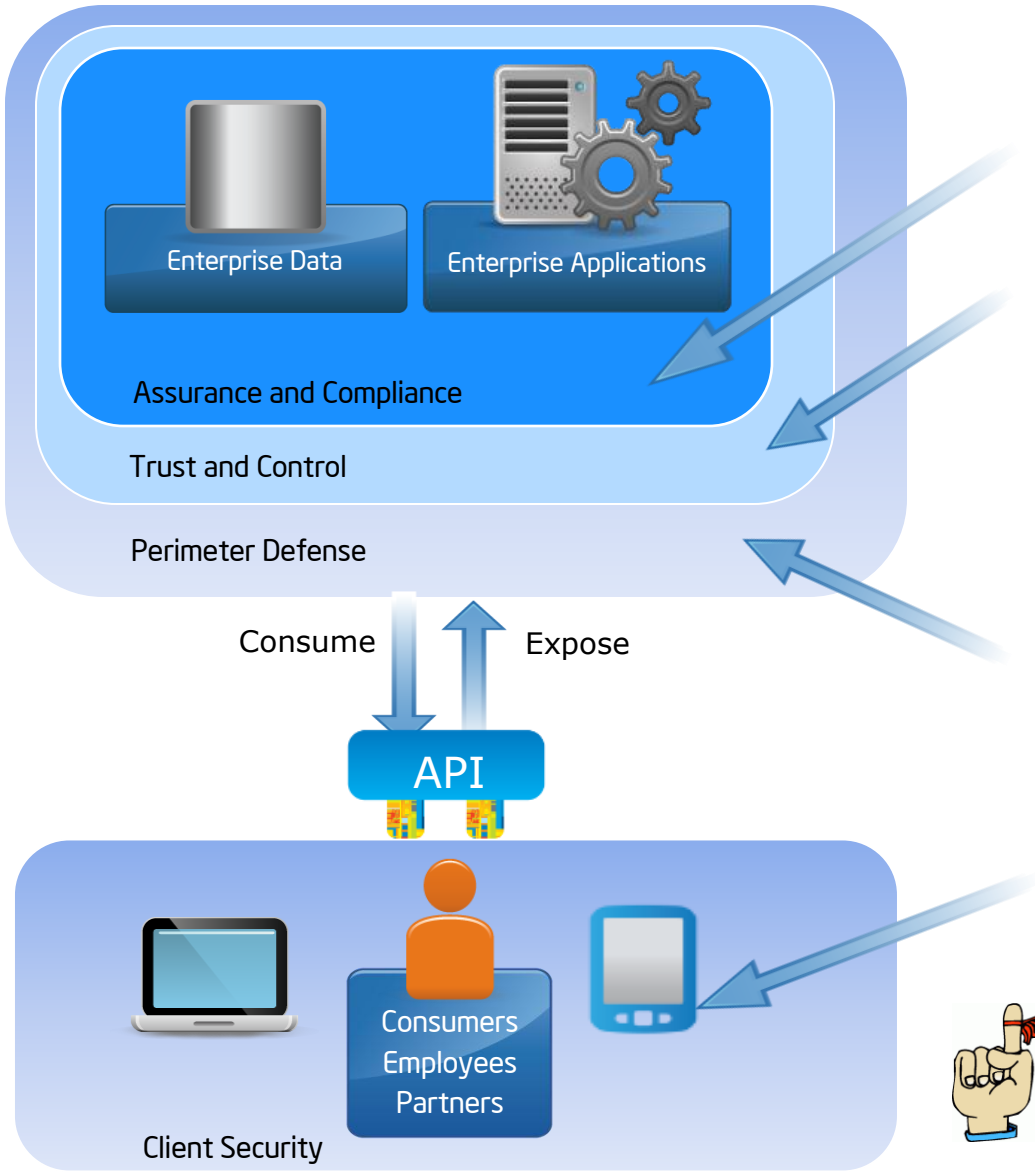
"Hodgepodge" of legacy infrastructure and programming languages...

PII Data

Difficult to apply consistent security, auditability, risk and compliance for API calls...

.. worse API data spans deployment models

Enterprise API Security Layers



- ✓ How to handle sensitive data in API requests & responses?
- ✓ How to audit API calls?

- ✓ Which partner applications can access APIs?
- ✓ Which employee applications can access APIs?
- ✓ How do I trust incoming API calls?
- ✓ How do I handle SSO for API calls?

- ✓ How do I keep API threats out?
- ✓ How do I scan incoming API calls for malware and virus payloads?
- ✓ How do I protect against app-level distributed Denial of Service (DoS)

- ✓ How do I protect clients from malware and content threats?

Remember! Security should be a declarative policy, not "coded in"

API Threats are Real and Now…

[ACTION REQUIRED] Ruby Security Vulnerability; CVE-2013-4164

Hello,

You are receiving this email because you run at least one Ruby (MR… …tion on Heroku.

Early this morning, the Ruby project announced a se… 1.8.7, 1.9.2, 1.9.3, 2.0.0. The CVE identifier is C… JRuby are unaffected.

We believe this is limited to a den… application that parses JSON… crash with little difficult… serious vulnerabili… there are no… …ot be ruled o… …3p484 and …pgrade as soon as …edar stack. If your …the note below.

…iously announced support for the 1.8.7 …nd has de-facto discontinued support for 1.9.2. …2p321 are not official release numbers from them, but …icate the presence of the patch. We strongly urge all …o begin migration plans to 1.9.3 or 2.0.0 at their earliest …s, as we can not guarantee our ability to backport security patches …itely.

Detecting if you're vulnerable

```
$ heroku run "ruby -v" -a APPNAME
```

If your patch version is less than what's listed above (e.g., 1.9.2p320), you're vulnerable.

Denial of Service & Code Execution Vulnerability in Ruby

November 22nd, 2013

ABUSING WEB APIS THROU… SCRIPT… AN… A… 2013

Demonstration of API key retrieval through disassembly and de-compilation

November 18th, 2013

CAPEC-111: JSON Hijacking (aka JavaScript Hi… …ki

JSON Hijack…

Attack Pattern ID: 111 *(Detailed Attack Pattern Completeness: Complete)*

Description

Summary

An attacker targets a system that uses… systems using AJAX) to steal poss… the loophole in the browser's … website.

An attacker gets th… requests a res… capture th… new o…

…object …

Att…

Expl…

1. **Un…** **…Target System:**

An a… …rstand what URLs need to be prov… interes…

Attack …

ID	Att… …cription
1	An att… …count with the target system and observes requests and … Unders… …o properly elicit responses from the server is crucial to the atta…

Indicators

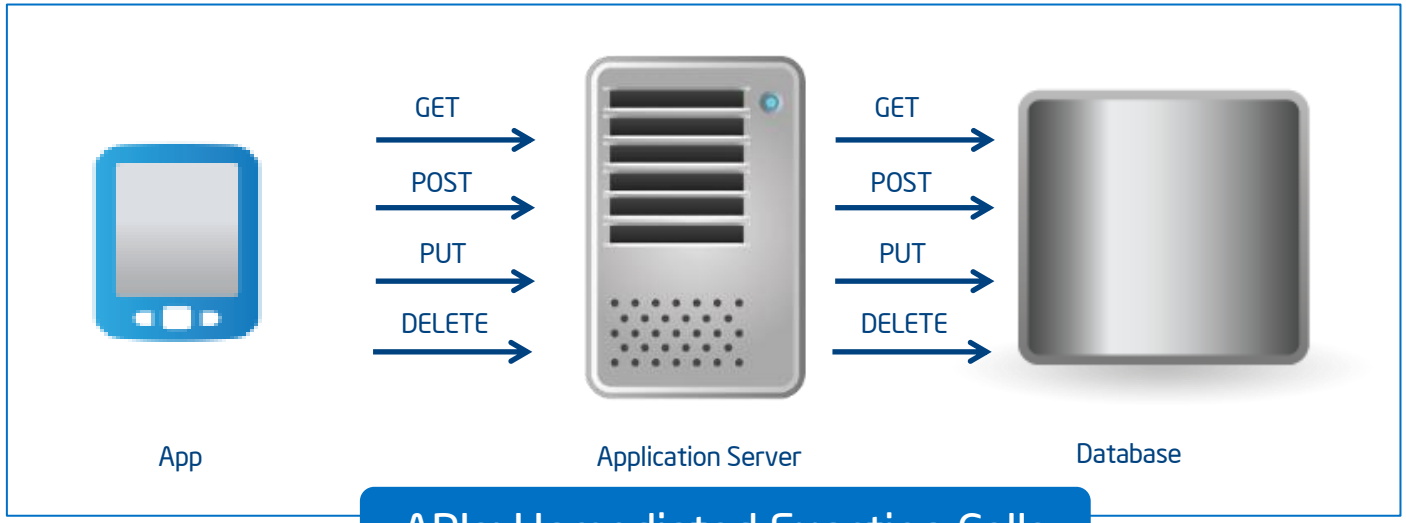
ID	Type	Indicator Description
1	Positive	Targeted application leverages JSON in its architecture.

JSON Hijacking to steal confidential information

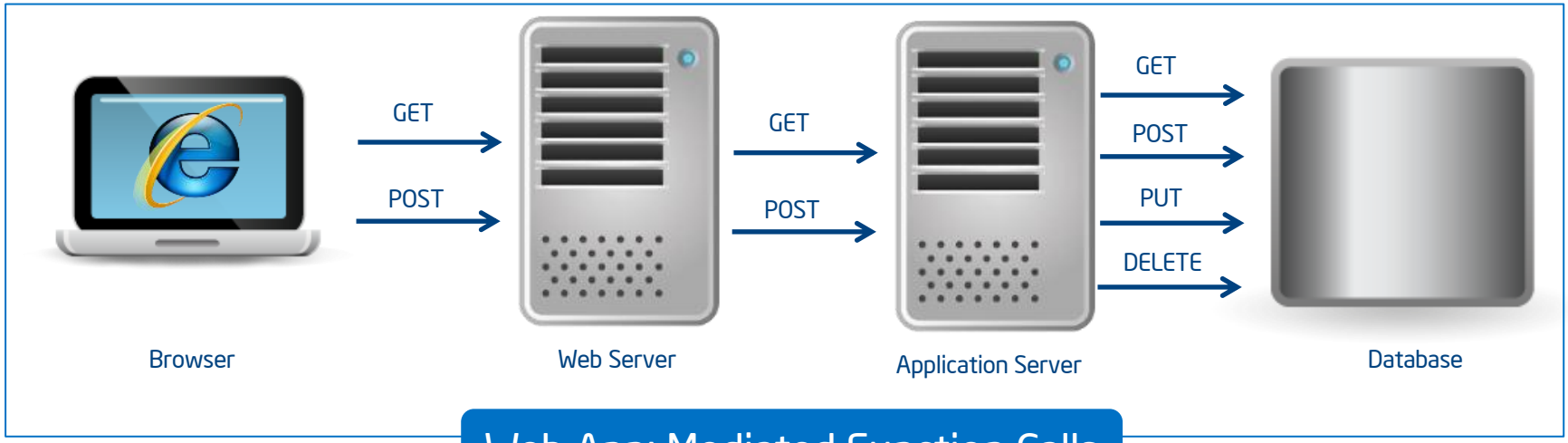
June 2013

But… are these any different than what we saw in the web world?

APIs are a Semantic Tunnel

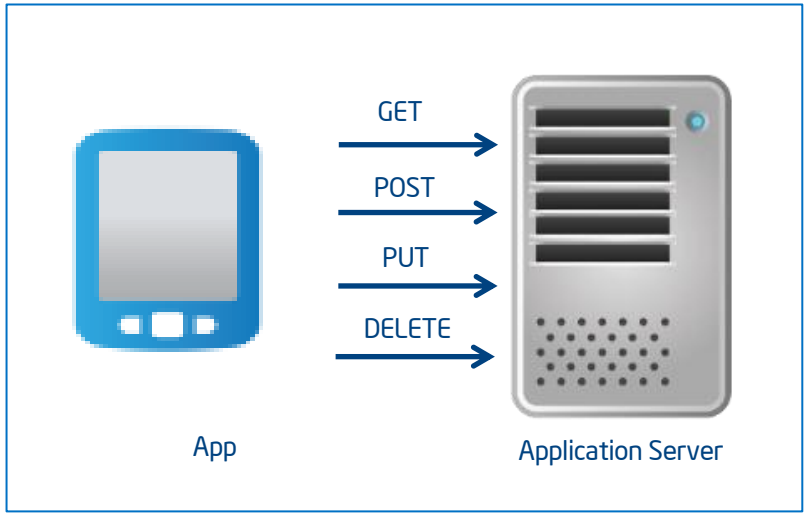


APIs: Unmediated Function Calls



Web App: Mediated Function Calls

Semantic Tunnel: Countermeasures

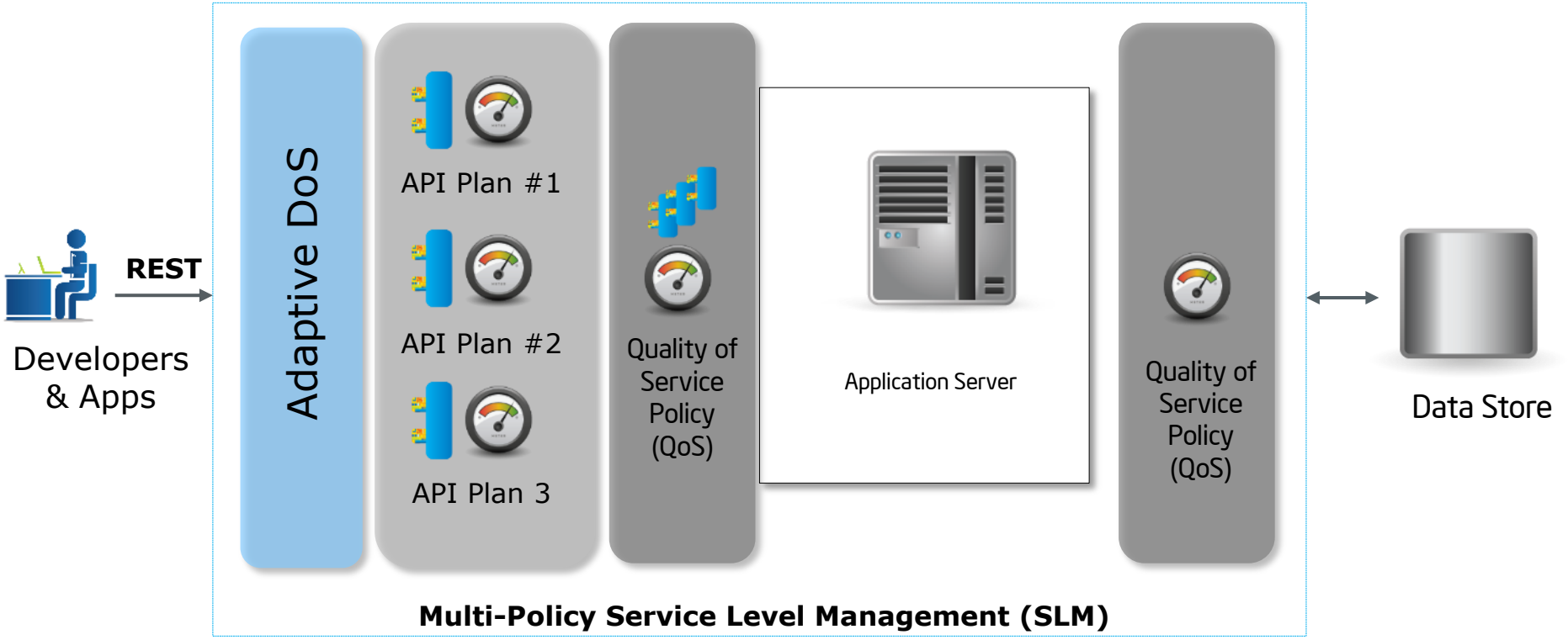


Countermeasures:

- ✓ Obfuscate, hide, or "turn off" certain methods
- ✓ Input validation
- ✓ Data-type checking*
- ✓ Data range checking
- ✓ Word scanning
- ✓ Pattern Scanning
- ✓ Avoid defaulting all data-types to 'string'
- ✓ Schema validation (JSON/XML)
- ✓ Validation/Rejection by regex match
- ✓ Message size limitations
- ✓ Message structure limitations (XML)
- ✓ Attachment scanning/limitations

Remember! Security should be a declarative policy, not "coded in"

Service Level Management (Throttling ! = Security)



	Purpose	Control Scope	Enforcement
API Plans	Coarse Grained Business Enablement	Single API	Messages per day, quota – enforced per calling application
Quality of Service	Fine Grained Infrastructure Tuning	Single API, set of APIs, set of services	Transaction rate, data rate, latency, utilization (plus more) –enforced per API, service, or IP
Adaptive DoS	Fine Grained Infrastructure Protection	Connection & IP Address	Rate shaping, alerting and blocking – Enforced per connection & IP

New Developer AuthN Requirements

API & Mobile Authentication Mechanisms

Authenticating Credential	Secret
API Key	API Key
API Key	Shared Secret
OAuth Consumer Key	OAuth Consumer Secret
Username	Password
Username	One-time Password

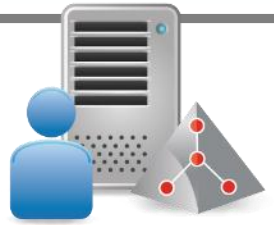
?

Enterprise Authentication Mechanisms

Authenticating Credential	Secret
Username	Password
Certificate	Private Key
Kerberos Ticket	Password
SAML Assertion	Password or Private Key
Username	One-time Password

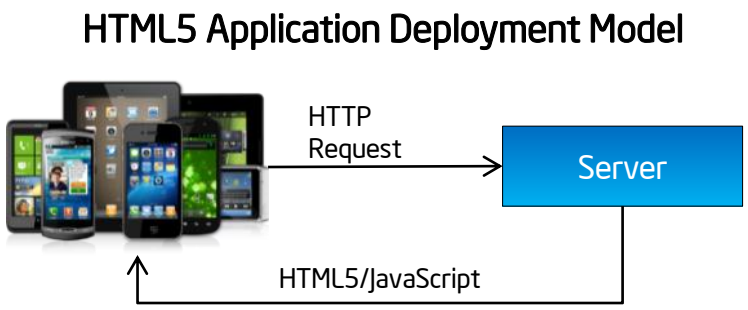
Consumer & BYOD

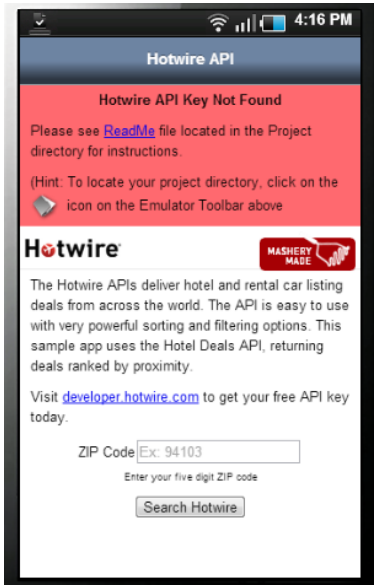
Enterprises can't afford another identity silo



Existing Enterprise IDM systems

API Key Security





API Key Security Concern

- HTML5 apps are pushed to the client *keys distributed to all clients*
- Clients can view source to obtain API keys
- **Solution #1:** Obfuscation
- **Solution #2:** Step-Up Authentication

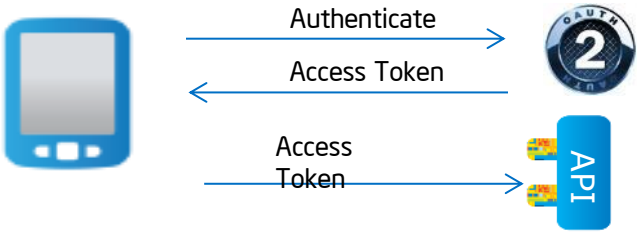
```
// ******************SET YOUR API KEY HERE******************
// ************************************************************

// Insert your Hotwire API Key here. ReadMe for more info.
var api_key = 'your-API-key-here';

// ************************************************************
// ************************************************************

// Check if valid API Key
function check_keys() {
    var url = 'http://api.hotwire.com/v1/deal/hotel?limit=1&dest
    AppMobi.device.getRemoteData(url, "GET", "", "displayFlashMe
}
```

Common Enterprise OAuth 2 Flows

2-Legged OAuth

- Client Credentials
- Resource Owner Password Credentials

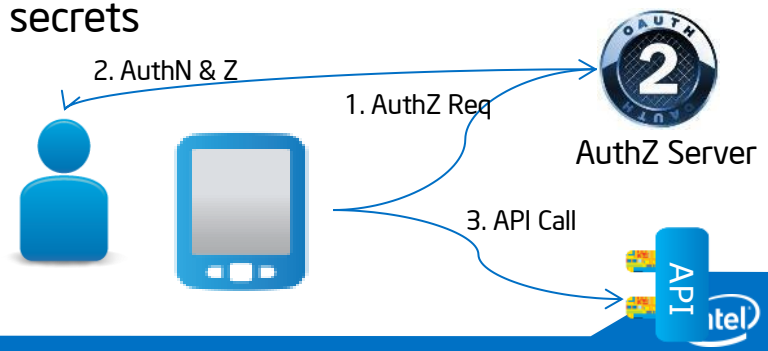
- ✓ Requires out-of-band shared secret
- ✓ Client apps must be completely trusted
- ✓ No refresh tokens
- ✓ No *user* concept
- ✓ Mitigates exposure of shared secrets



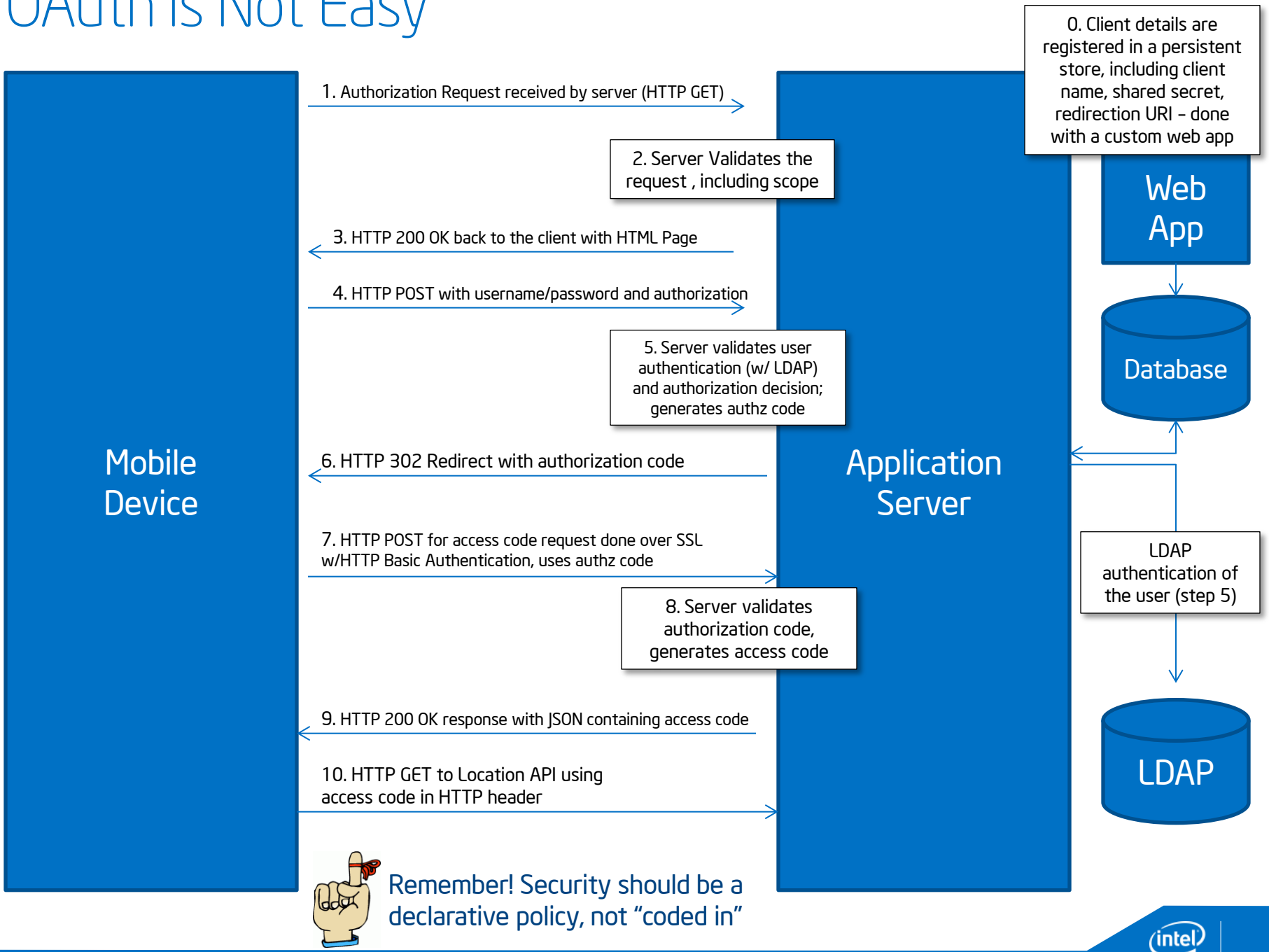
3-Legged OAuth

- Authorization Code
- Implicit Grant

- ✓ Requires out-of-band shared secret
- ✓ Solves impersonation anti-pattern
- ✓ Client apps can be untrusted
- ✓ Supports refresh tokens
- ✓ Requires *user* concept
- ✓ Mitigates exposure of shared secrets



OAuth is Not Easy



API Compliance

Regulatory Drivers

- Credit card data (PCI)
- Personally identifiable information (PII)
- Medical records (HIPAA)
- Financial data (SOX, GLBA)

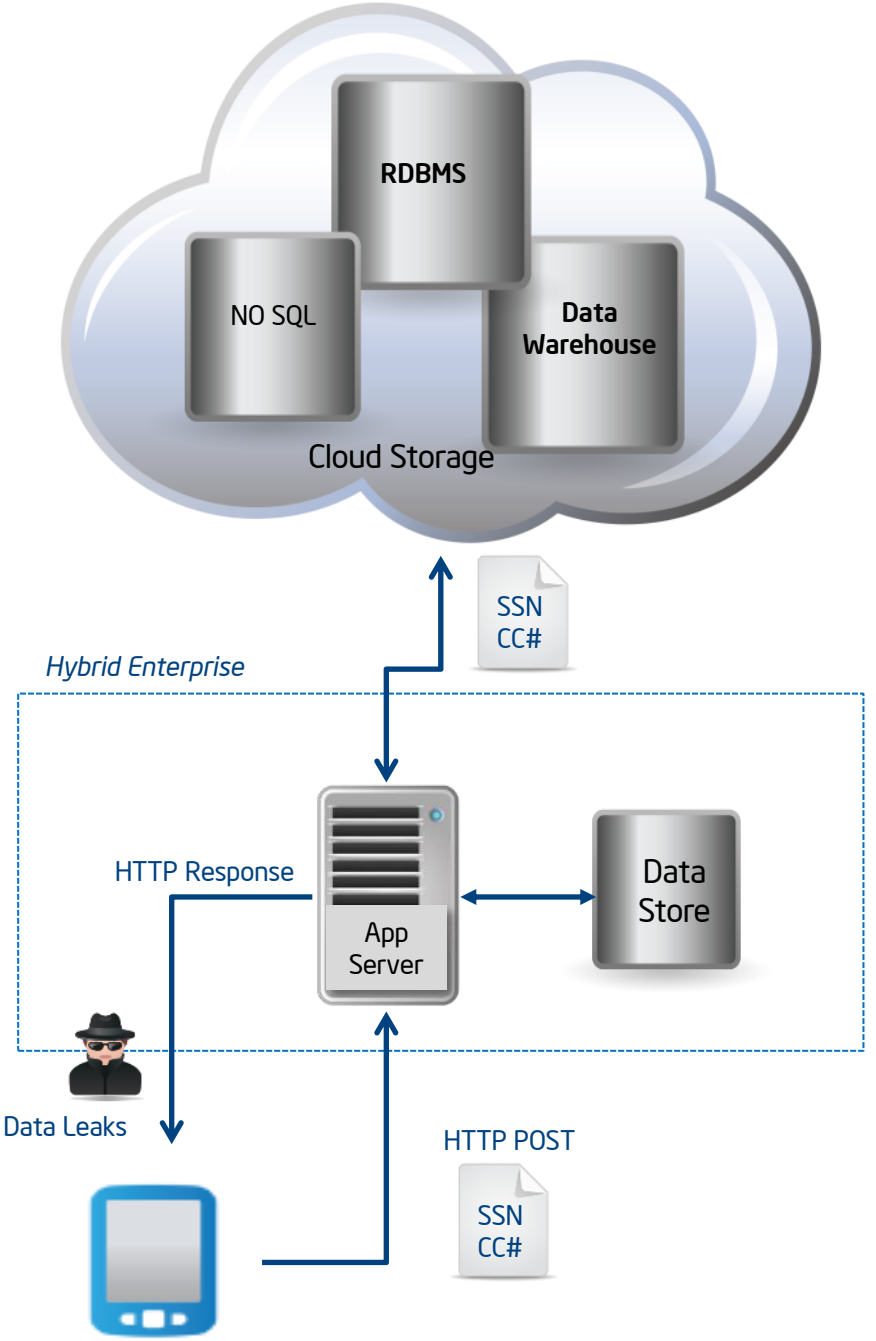
Reduce assessment costs, avoid fines, protect customers & shareholders

Intellectual Property

- Source code, blue prints
- Roadmap data
- Business plans & models
- Data from M&A, marketing

Protect organization IP, assets, resources and improve competitive posture

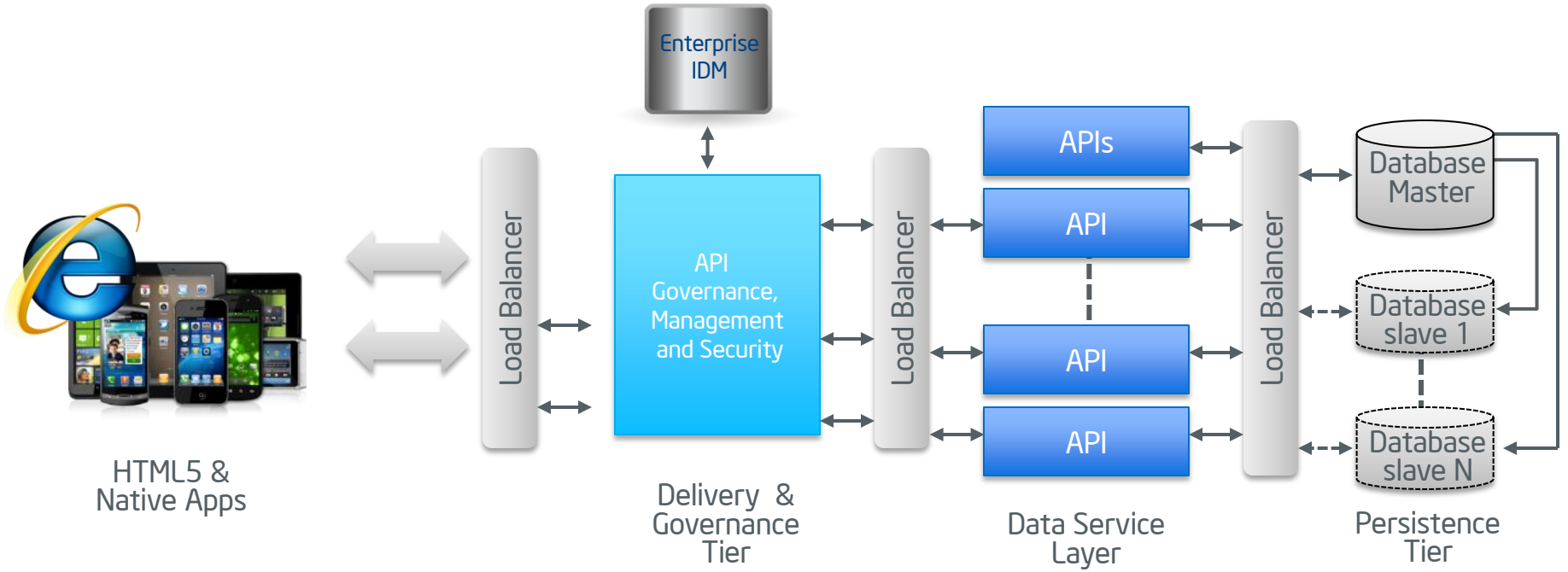
Remember! Security should be a declarative policy, not "coded in"



API Security Choices

	Trust	Threats
 3rd Party Apps	✓ RESTful Service ✓ OAuth 2.0 – Auth Code Flow ✓ API Keys ✓ Server side SSL	✓ DDoS Protection ✓ Content Attack Protection ✓ API Plans ✓ API Resource Protection
 Enterprise Mobile Apps	✓ RESTful Service ✓ 2-Way SSL ✓ API Keys with Step-Up Auth ✓ 2-Legged OAuth – Client Credentials Flow ✓ SSO – Use SAML 2.0 or OpenID Connect ✓ JSON Web Tokens	✓ DDoS Protection ✓ Content Attack Protection ✓ API Plans ✓ API Resource Protection
 Internal Client / Server	✓ SOAP or REST ✓ SSL w/ Enterprise authentication ✓ SSO – Use SAML 2.0 or OpenID Connect	✓ API Plans ✓ API Resource Protection
 Partner Web Services	✓ SOAP WS-Security (X.509 or HMAC) ✓ 2-Way SSL	✓ DDoS Protection ✓ Content Attack Protection ✓ API Plans ✓ API Resource Protection
 Internal Apps/ Developers	✓ SOAP or REST ✓ API Keys ✓ No Key ✓ SSO – Use SAML 2.0 or OpenID Connect	✓ API Plans ✓ API Resource Protection

"New" 3-Tier Architecture



- Clients from any channel
- Synchronous or socket communication
- Transport Level Security with session authentication

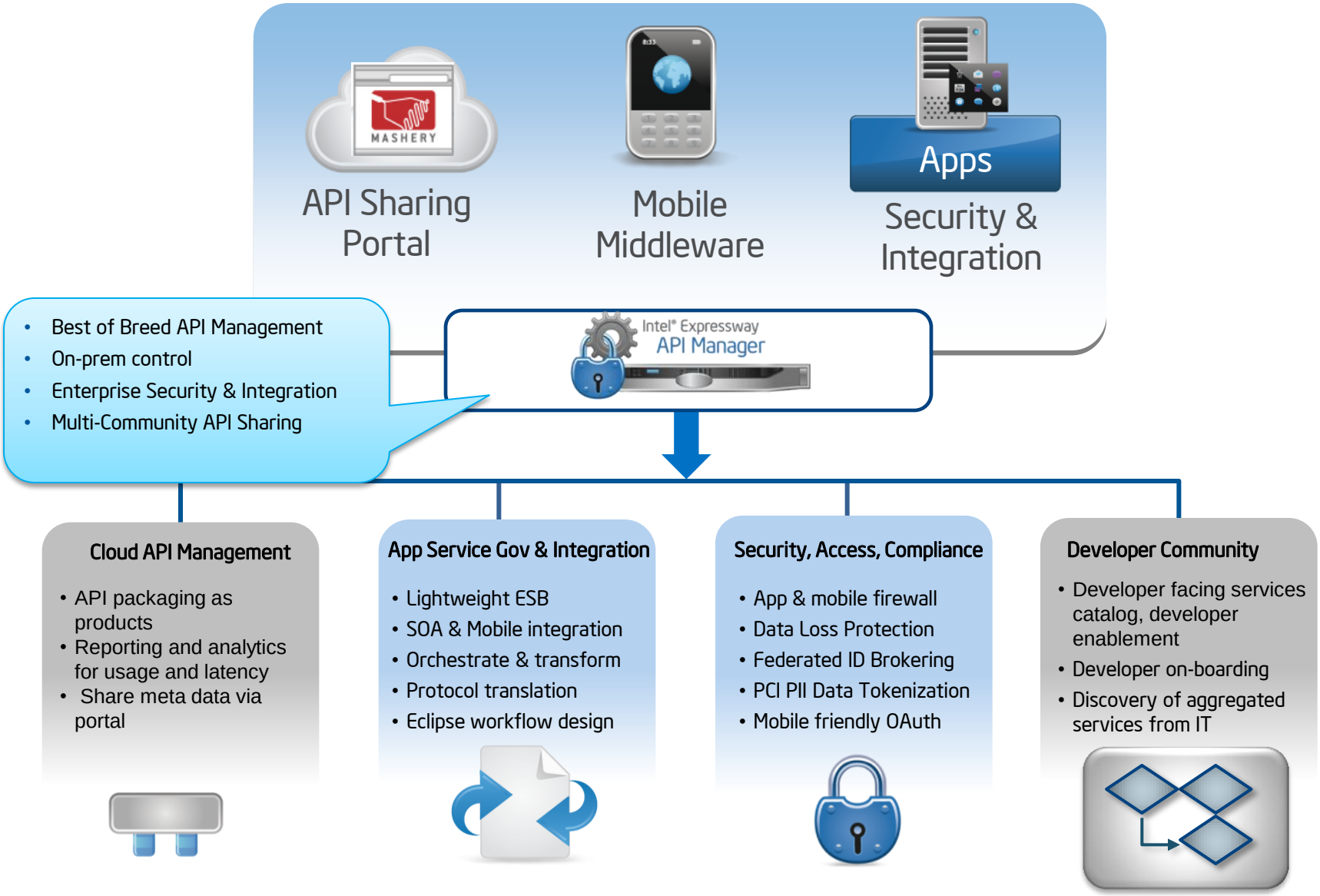
- API Governance Layer – handles scalability, security, and security decoupling
- Single point of audit, security control and compliance

- APIs – The backbone of the architecture
- Surface data from any system

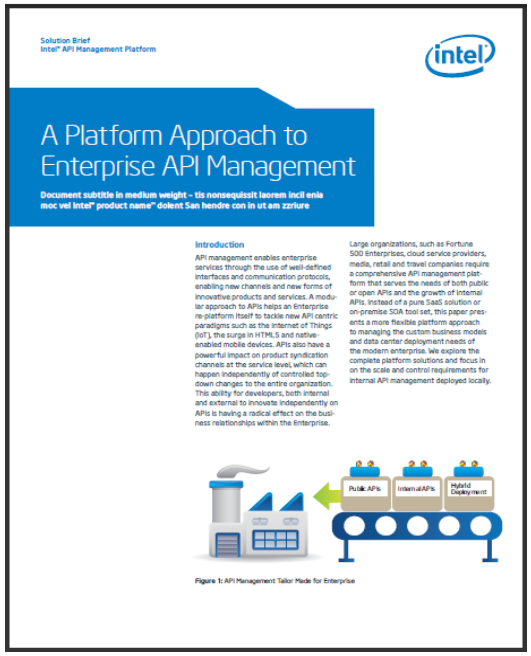
- Logical persistence tier, data may be stored in RDMS or NOSQL stores

The API Governance Layer helps mitigate API trust and threat concerns in the application architecture

Intel® Expressway API Manager



API Resource Center: cloudsecurity.intel.com


Solution Brief
Intel® API Management Platform

A Platform Approach to Enterprise API Management

Document subtitle in medium weight – tis nonsequissit laorem incil enia moc vel Intel® product name™ dolent San hendre con in ut am zzriure

Introduction

API management enables enterprise services through the use of well-defined interfaces and communication protocols, enabling new channels and new forms of innovative products and services. A modular approach to APIs helps an Enterprise re-platform itself to tackle new API centric paradigms such as the Internet of Things (IoT), the surge in HTML5 and native-enabled mobile devices. APIs also have a powerful impact on product syndication channels at the service level, which can happen independently of controlled top-down changes to the entire organization. This ability for developers, both internal and external to innovate independently on APIs is having a radical effect on the business relationships within the Enterprise.

Large organizations, such as Fortune 500 Enterprises, cloud service providers, media, retail and travel companies require a comprehensive API management platform that serves the needs of both public or open APIs and the growth of internal APIs. Instead of a pure SaaS solution or on-premise SOA tool set, this paper presents a more flexible platform approach to managing the custom business models and data center deployment needs of the modern enterprise. We explore the complete platform solutions and focus in on the scale and control requirements for internal API management deployed locally.

Public APIs
Internal APIs
Hybrid Deployment

Figure 1: API Management Tailor Made for Enterprise

Solution Brief: Internal APIs

Use Case Video

Forrester SOA to API Webinar

verizon · CABLE ONE · fiserv. · BlueCross BlueShield · Level(3) COMMUNICATIONS · VOLVO · McKESSON Empowering Healthcare · CSC · WESTJET · UBISOFT