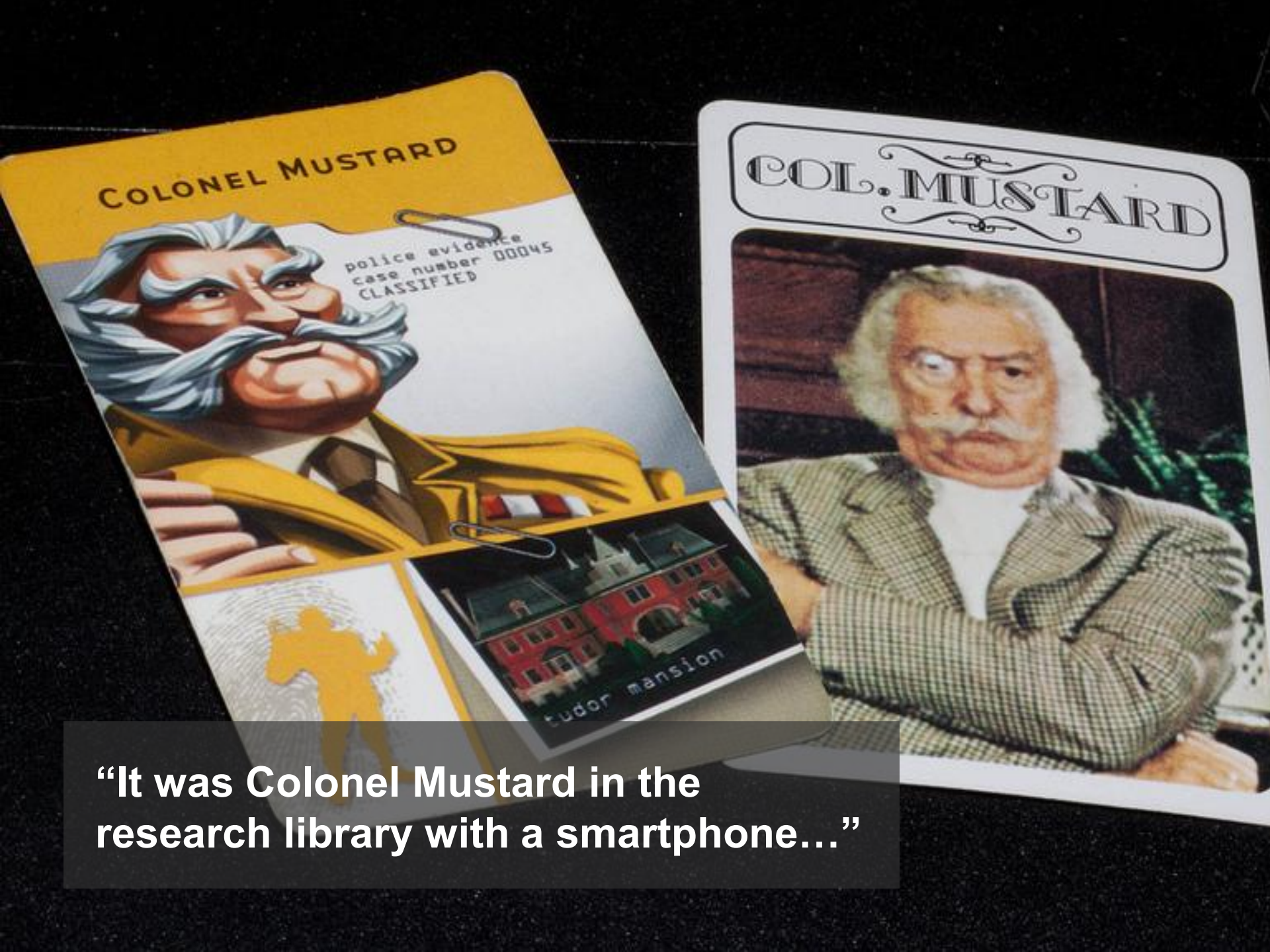
The IAM-as-an-API Era Has Arrived

And You Can Blame/Thank Mobility

Eve Maler, Principal Analyst, Security & Risk

October 30, 2013



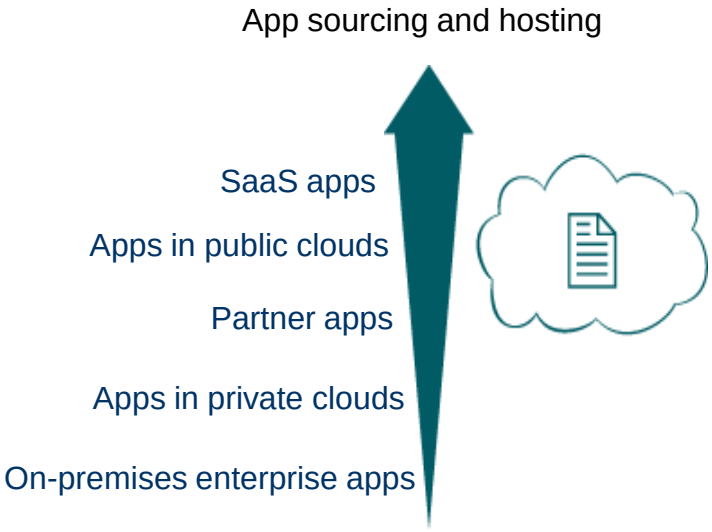
“It was Colonel Mustard in the research library with a smartphone…”

Agenda

- *Consumerization of IT and its cousins are challenging IAM traditions*
- *Apply Zero Trust to your identity, security, and agility problems in "bring-your-own" environments*
- *Leverage emerging technologies to provide identity services that are mobile-cloud ready*

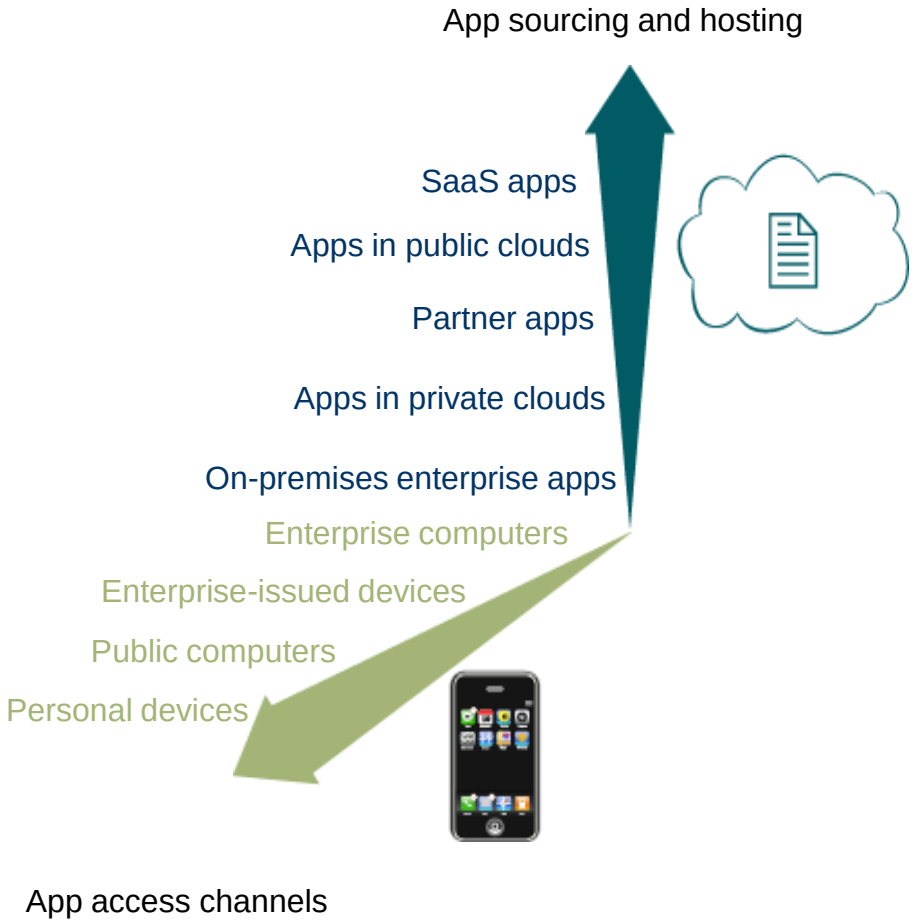
The extended enterprise forces IT to confront bring-your-own-everything

The extended enterprise forces IT to confront bring-your-own-everything



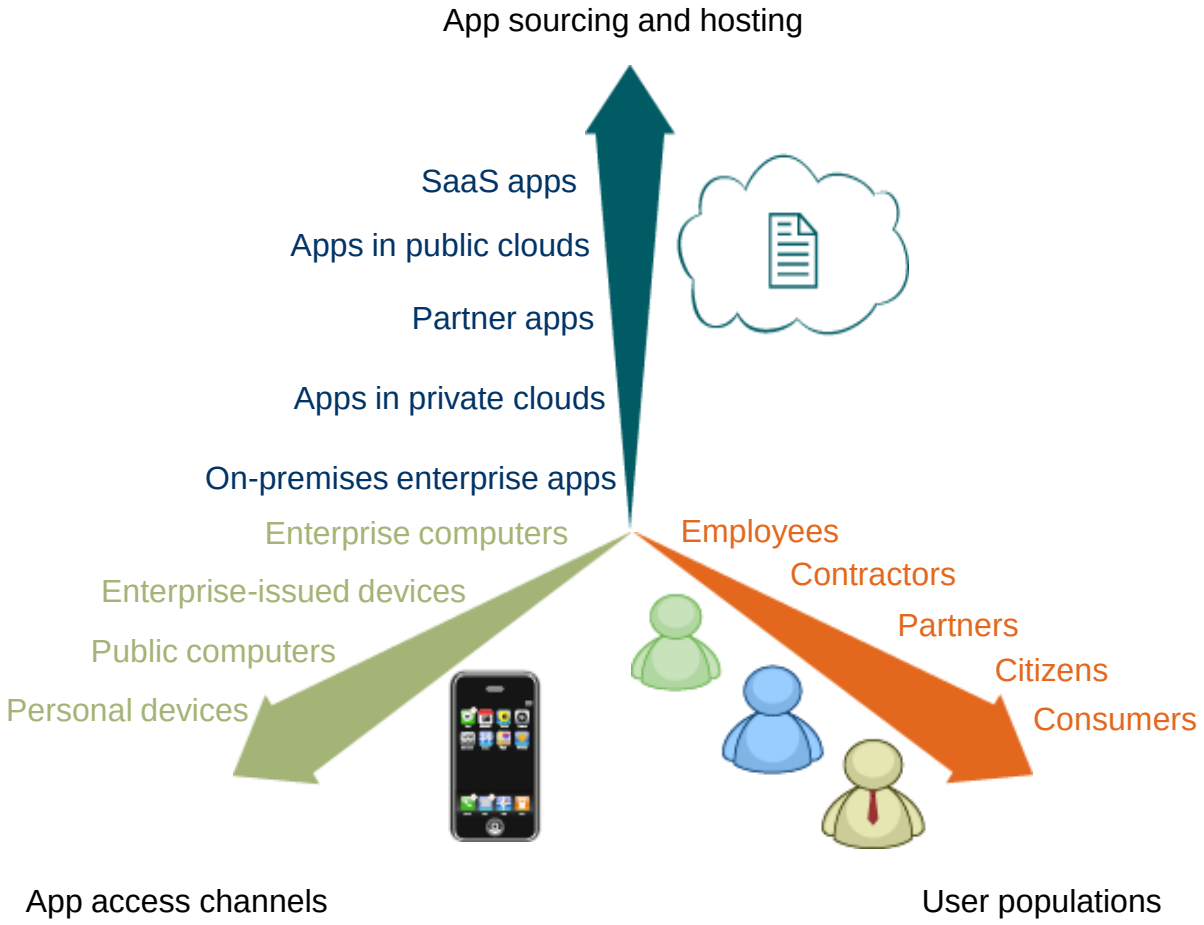
Source: March 22, 2012, “Navigate The Future Of Identity And Access Management” Forrester report

The extended enterprise forces IT to confront bring-your-own-everything



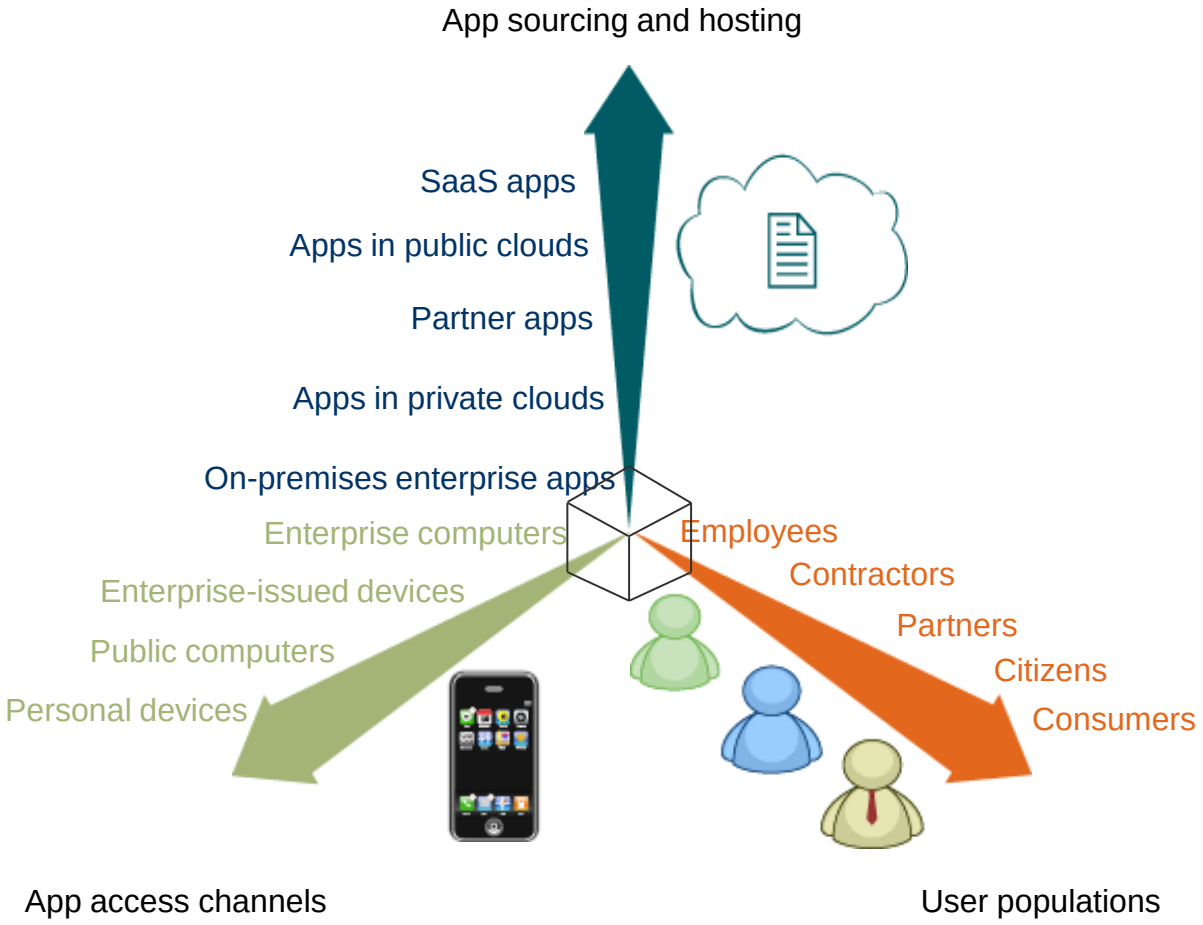
Source: March 22, 2012, “Navigate The Future Of Identity And Access Management” Forrester report

The extended enterprise forces IT to confront bring-your-own-everything



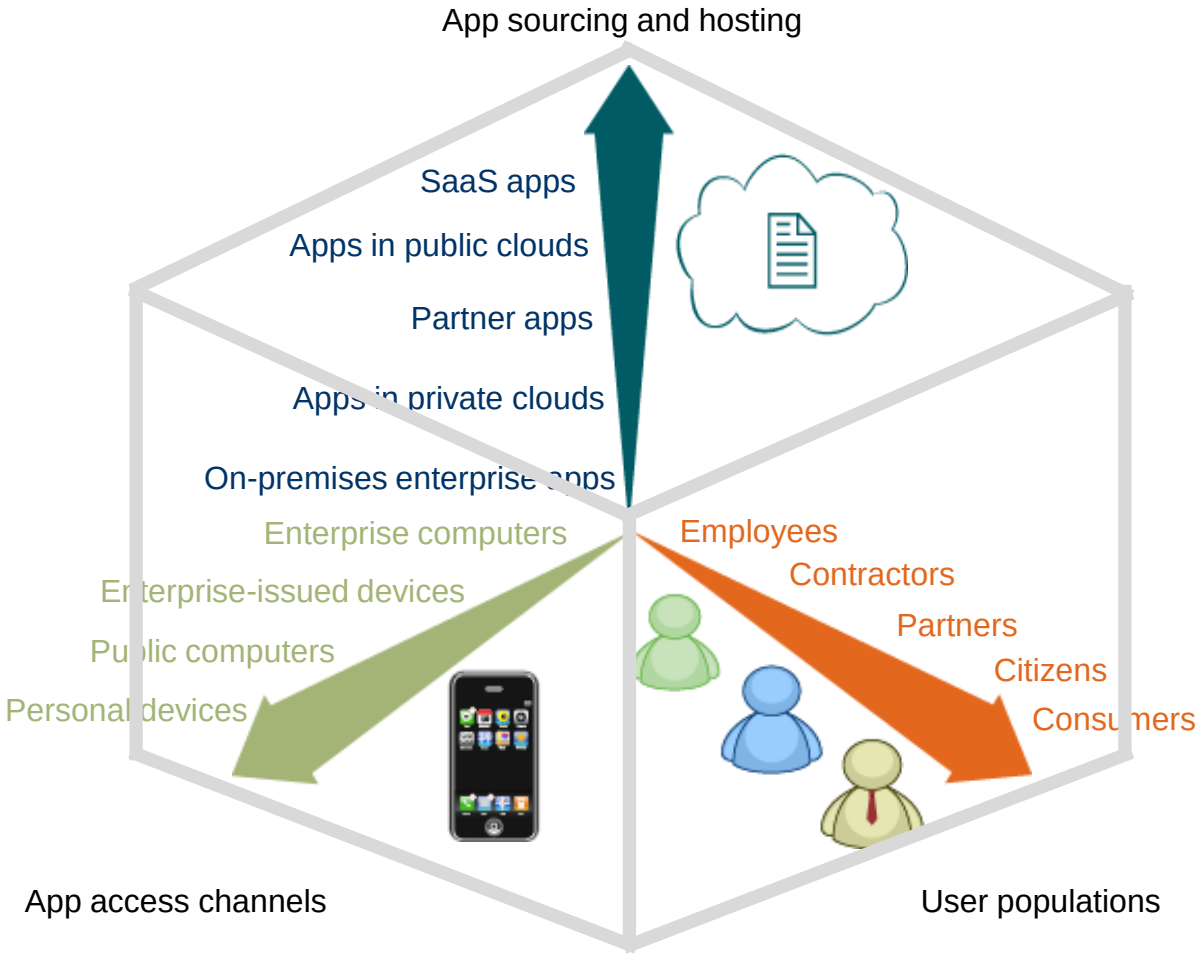
Source: March 22, 2012, “Navigate The Future Of Identity And Access Management” Forrester report

The extended enterprise forces IT to confront bring-your-own-everything



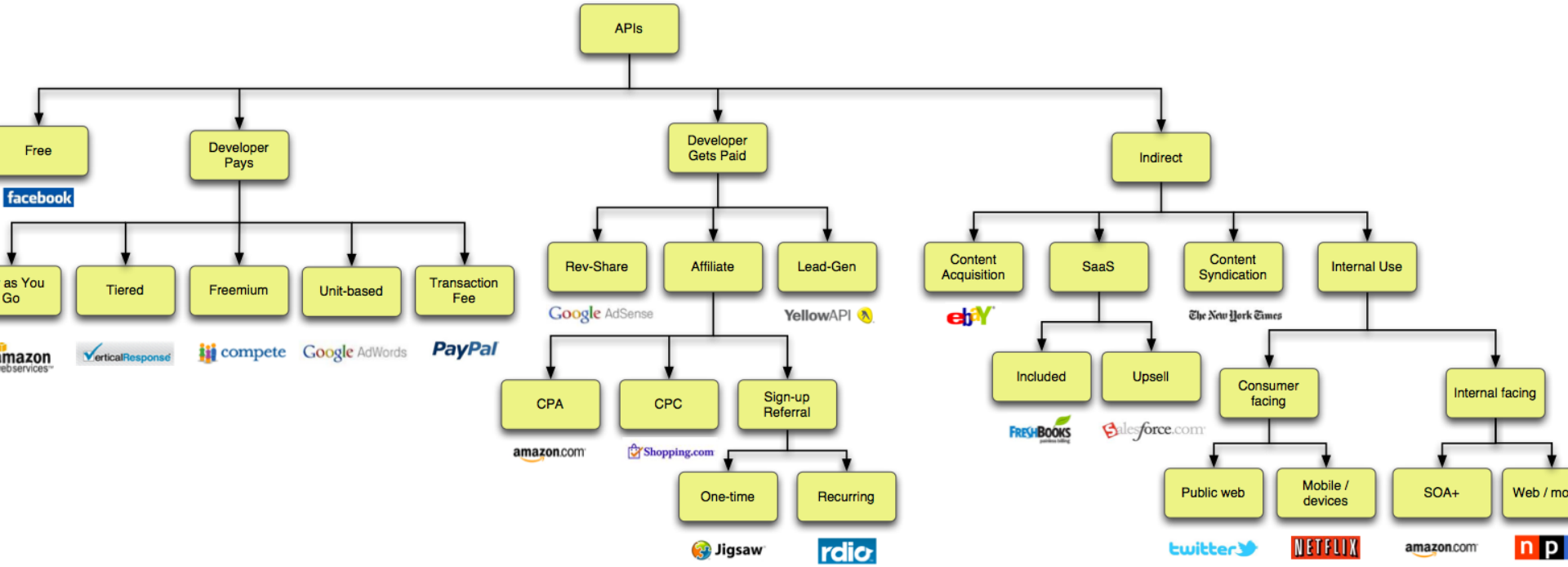
Source: March 22, 2012, “Navigate The Future Of Identity And Access Management” Forrester report

The extended enterprise forces IT to confront bring-your-own-everything



Source: March 22, 2012, “Navigate The Future Of Identity And Access Management” Forrester report

Now many APIs have business models, many predicated on mobile



Source: John Musser of ProgrammableWeb.com

Steve Yegge describes *why* … and the next challenge

[Jeff Bezos] issued a mandate that was so out there, so huge and eye-bulgingly ponderous, that it made all of his other mandates look like unsolicited peer bonuses. … "1) ***All teams will henceforth expose their data and functionality through service interfaces.****" …*

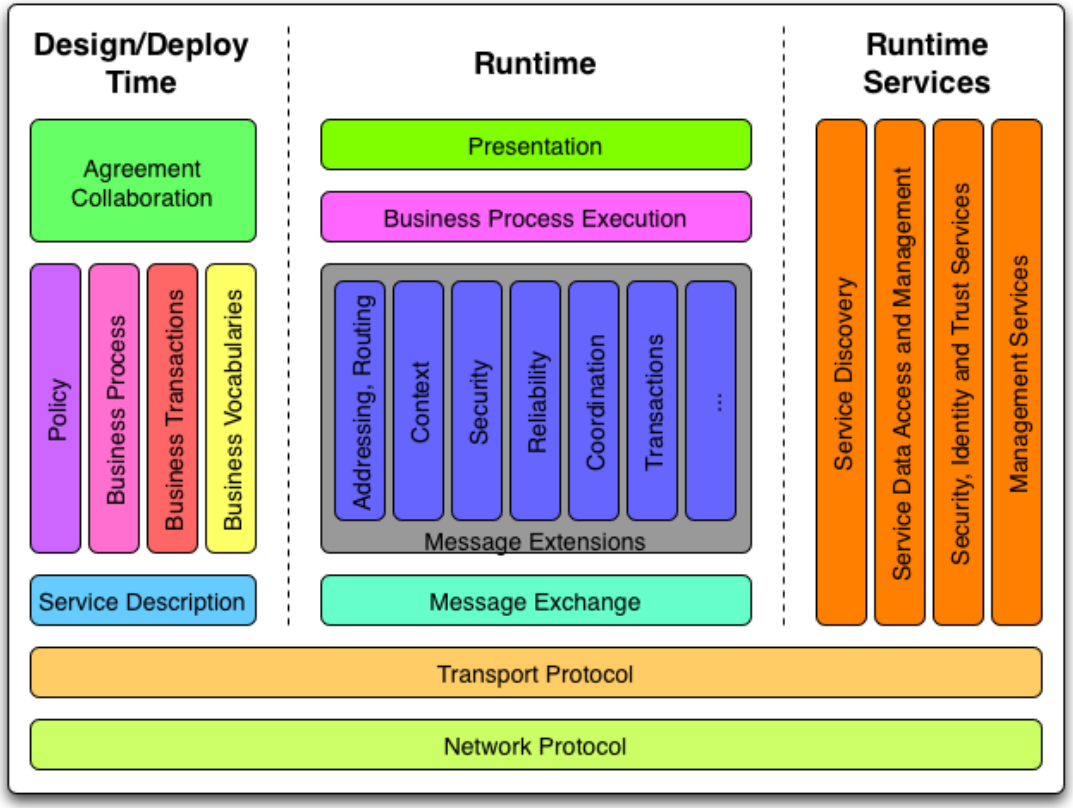
Like anything else big and important in life, ***Accessibility has an evil twin*** *who, jilted by the unbalanced affection displayed by their parents in their youth, has grown into an equally powerful Arch-Nemesis (yes, there's more than one nemesis to accessibility)* ***named Security.*** *And boy howdy are the two ever at odds.*

But I'll argue that Accessibility is actually more important than Security because dialing Accessibility to zero means you have no product at all, whereas ***dialing Security to zero can still get you a reasonably successful product*** *such as the Playstation Network.*

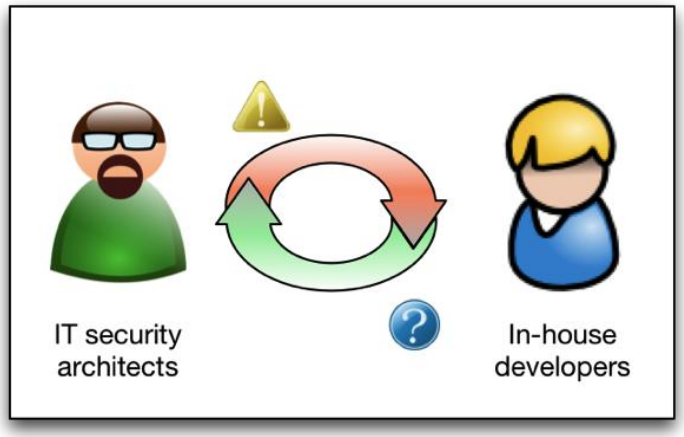
Source: Rip Rowan on Google Plus

Didn’t we already solve the web services security problem?

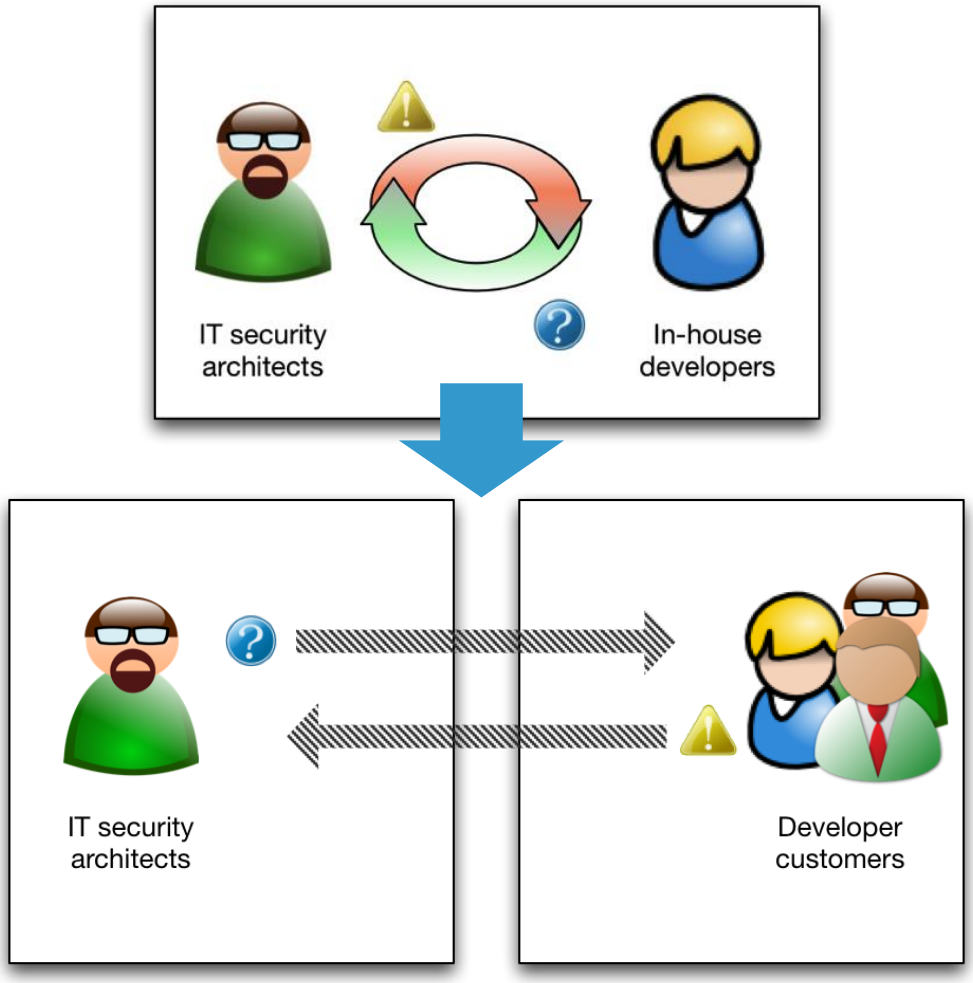
- Transport-layer solutions
- Platform-specific solutions
- XML signature, XML encryption, XML canonicalization
- WS-Security, WS-Trust, WS-I Basic Security Profile
- SAML
- ID-WSF



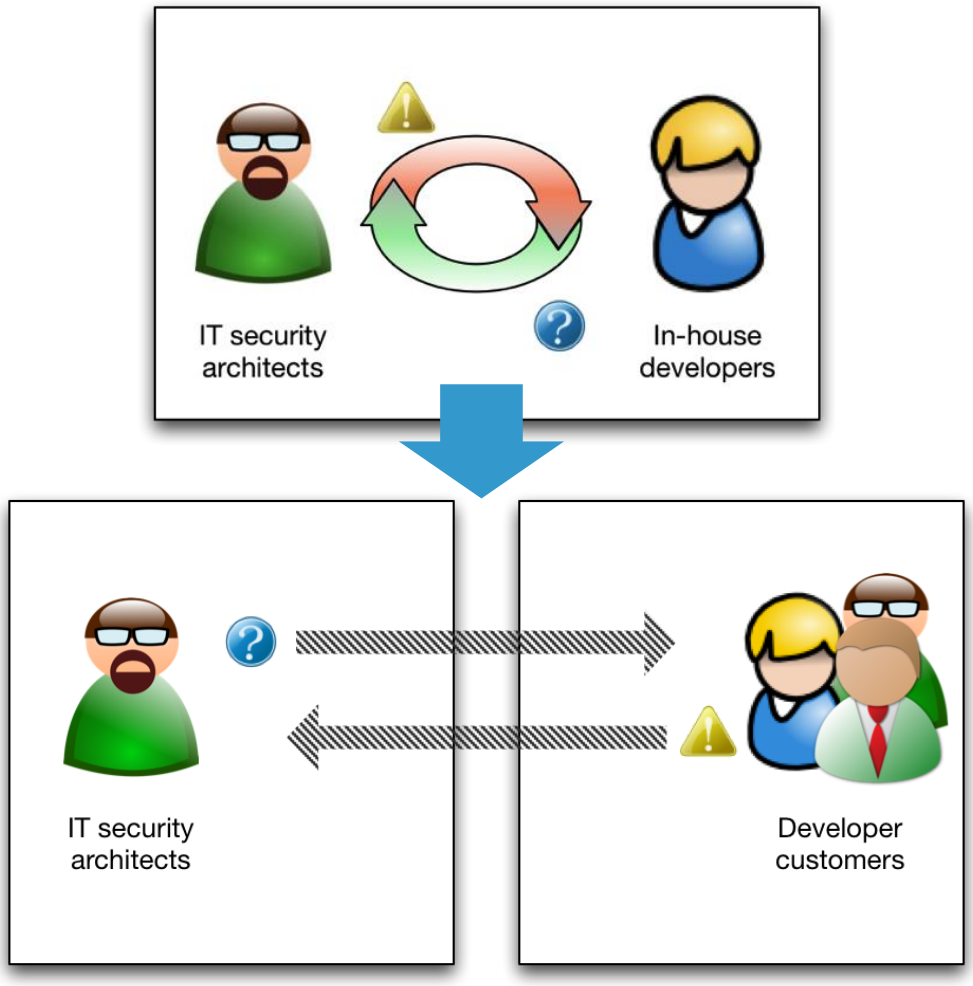
The “API economy” forces IT to confront *webdevification*

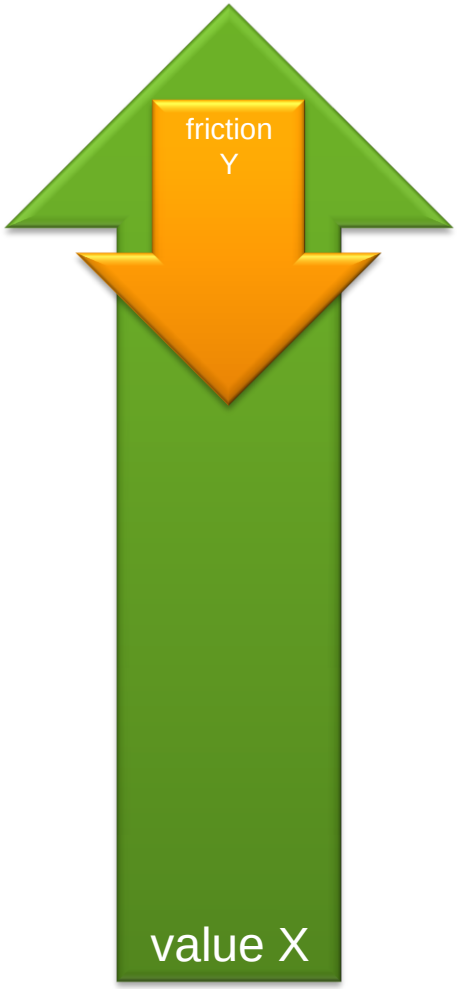


The “API economy” forces IT to confront *webdevification*

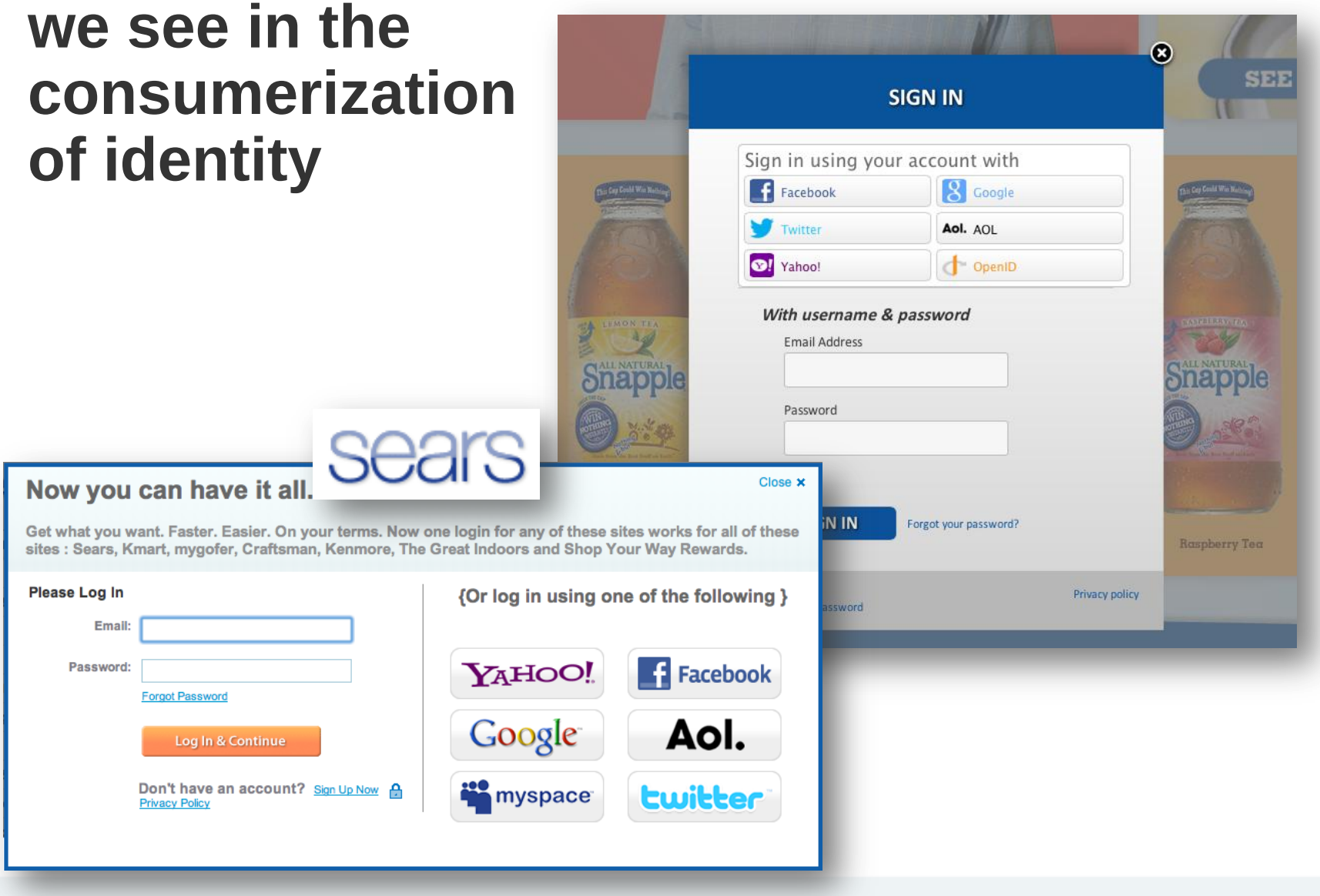


The “API economy” forces IT to confront *webdevification*





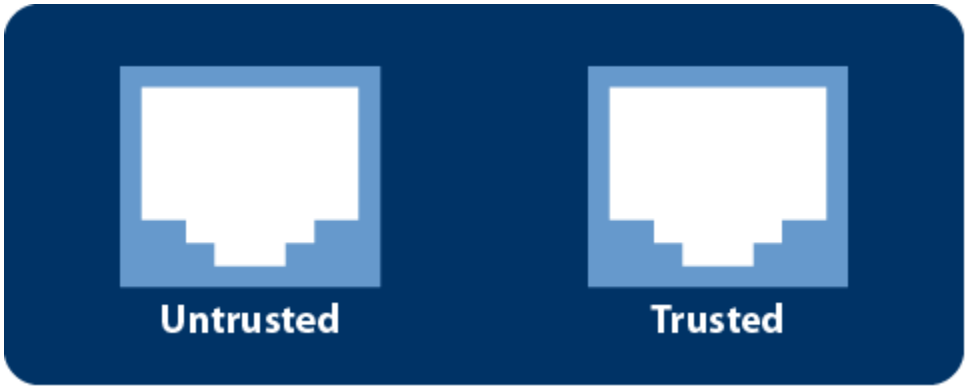
It’s akin to what we see in the consumerization of identity



Agenda

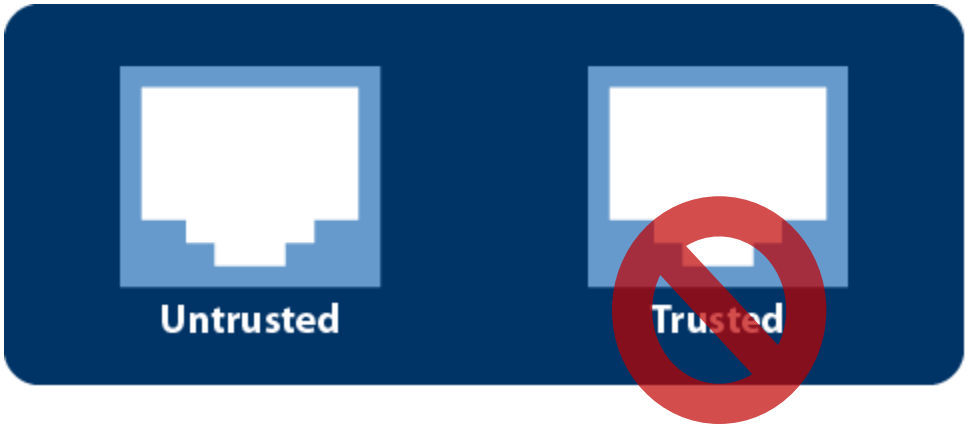
- *Consumerization of IT and its cousins are challenging IAM traditions*
- *Apply Zero Trust to your identity, security, and agility problems in "bring-your-own" environments*
- *Leverage emerging technologies to provide identity services that are mobile-cloud ready*

You can’t trust everything + everyone inside your crunchy perimeter anyway



Source: November 15, 2012, “No More Chewy Centers: Introducing The Zero Trust Model Of Information Security” Forrester report

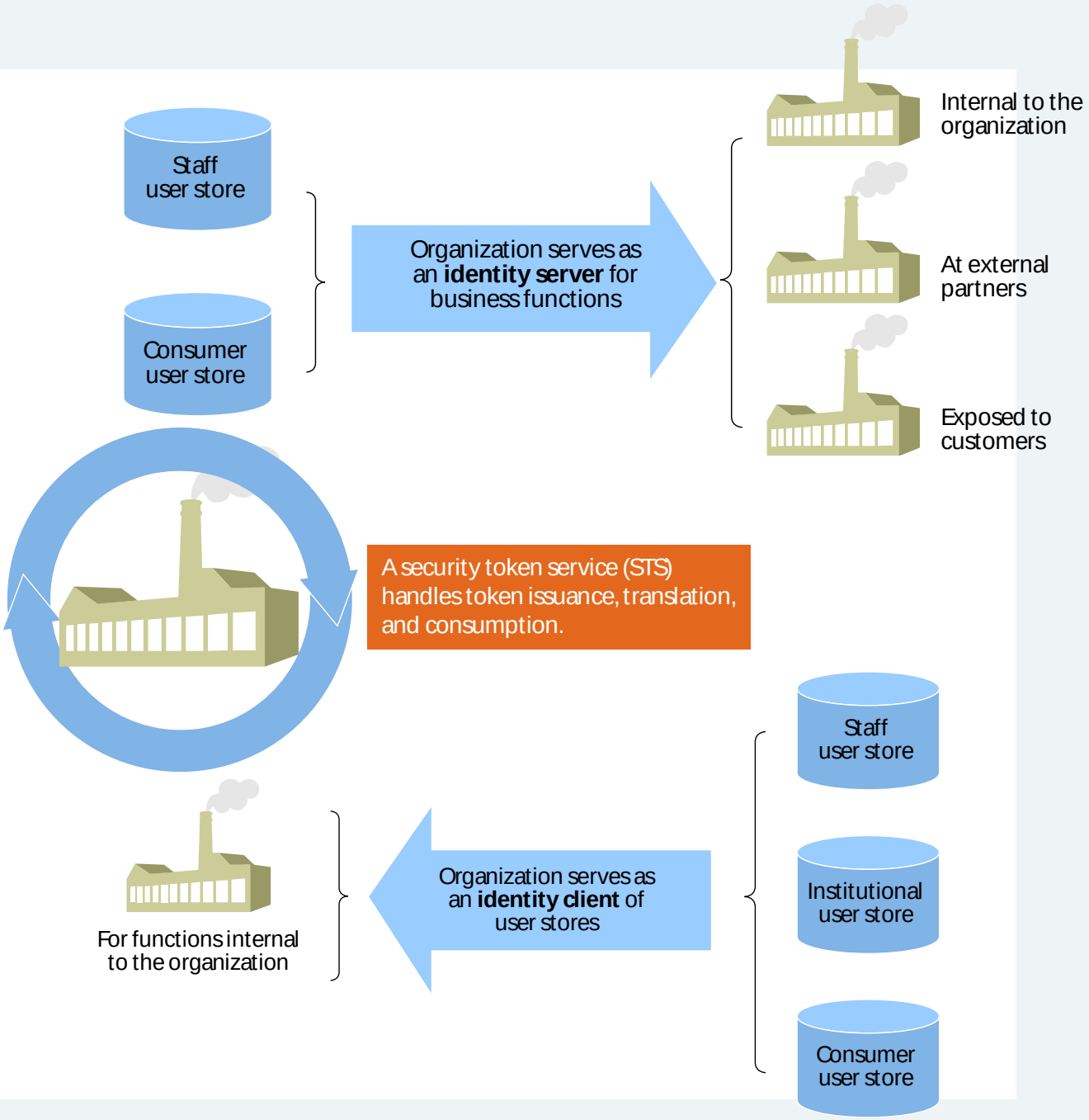
You can’t trust everything + everyone inside your crunchy perimeter anyway



…so stop trying

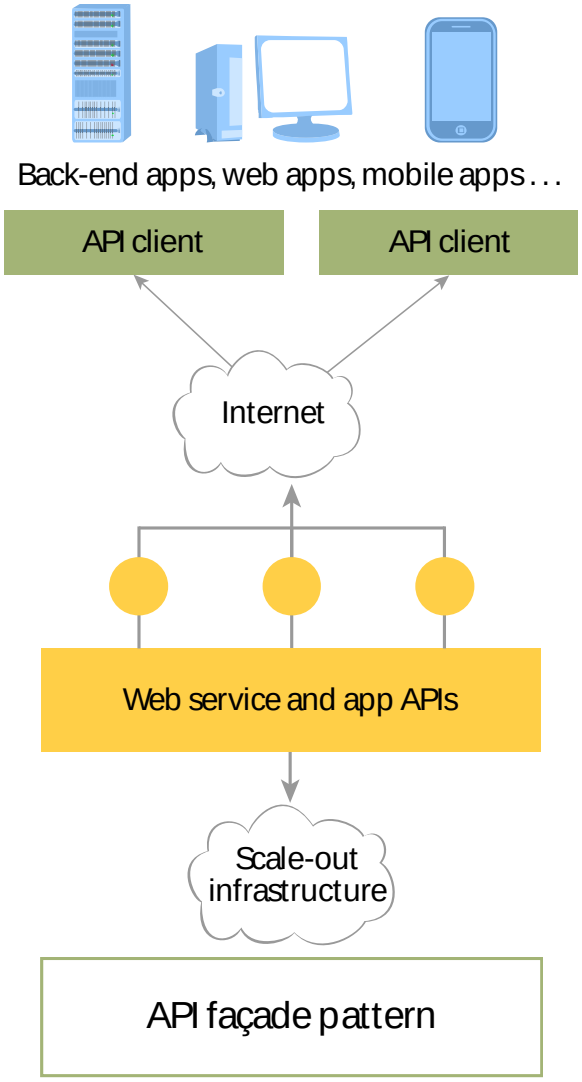
Source: November 15, 2012, “No More Chewy Centers: Introducing The Zero Trust Model Of Information Security” Forrester report

Plan for inward, outward, and circular identity propagation



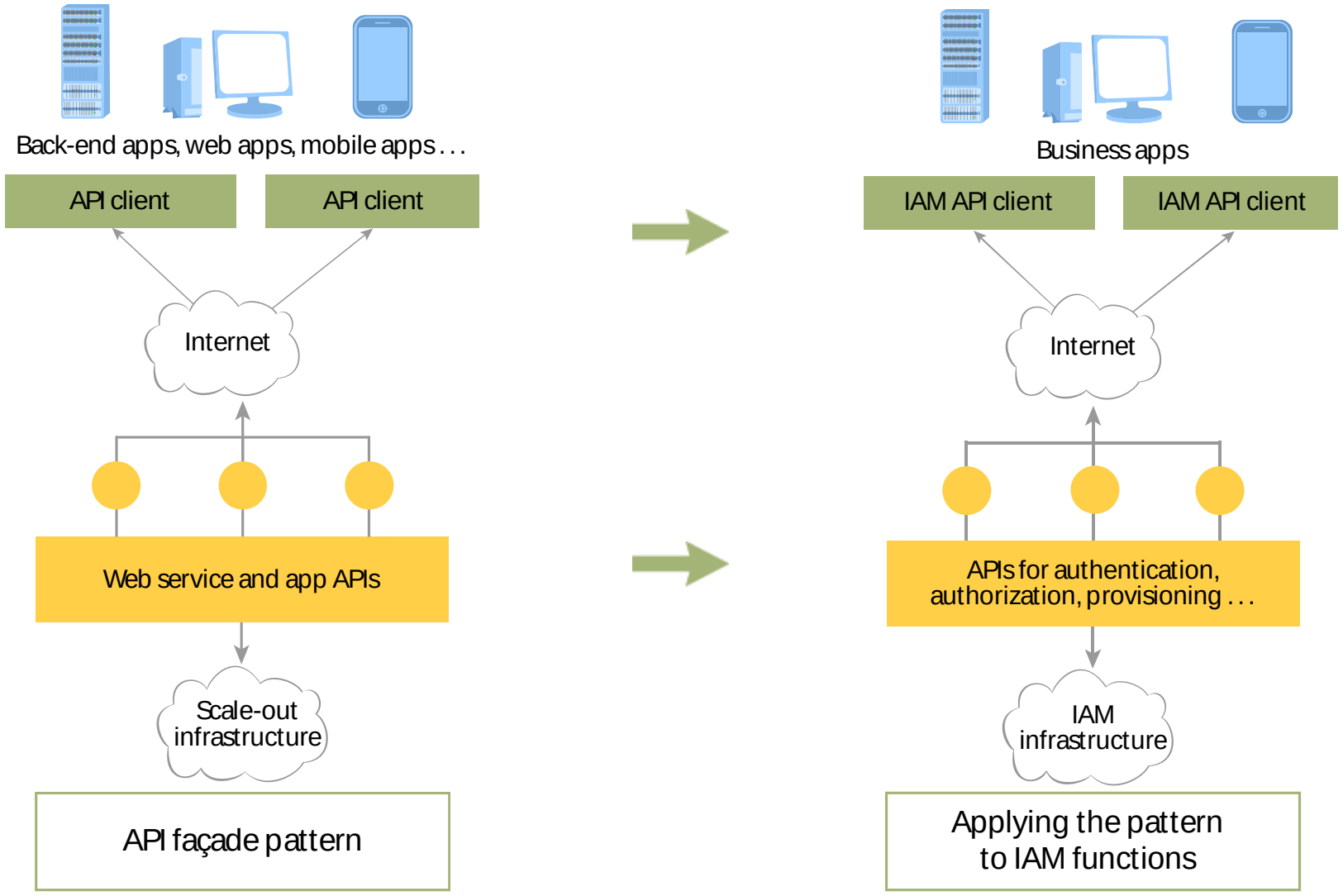
Source: March 22, 2012 “Navigate The Future of IAM” Forrester report

Go from IDaaS to IAM-as-an-API



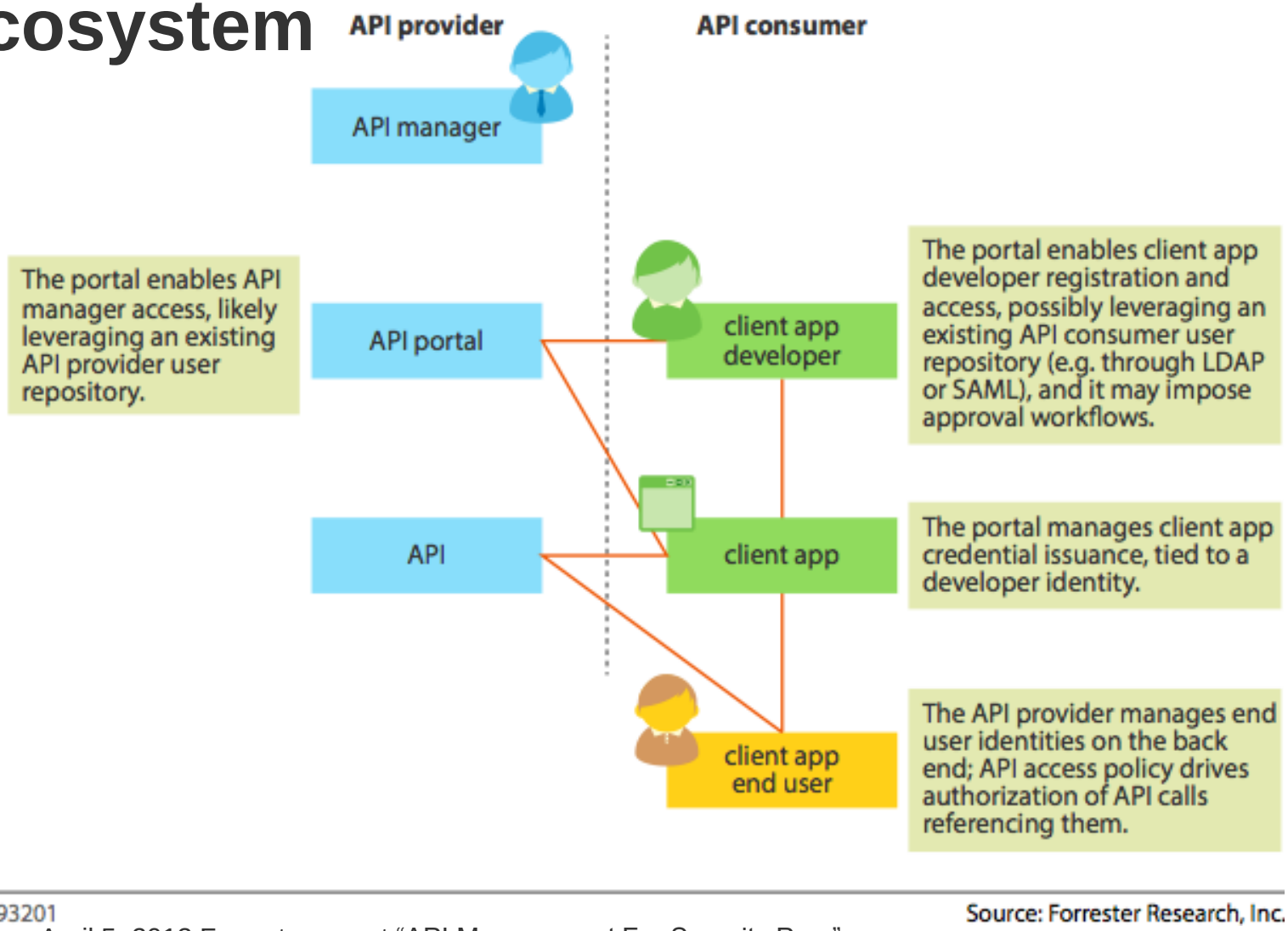
Source: March 22, 2012 “Navigate The Future of IAM” Forrester report

Go from IDaaS to IAM-as-an-API



Source: March 22, 2012 “Navigate The Future of IAM” Forrester report

A lot of identities float around an API ecosystem



Source: April 5, 2013 Forrester report “API Management For Security Pros”

APIs have different “security natures”

Internal APIs

- Most sensitive tasks/data
- Most often security is (too) tightly coupled
- Devs have corporate credentials
- Most control over apps, devices, and security friction

APIs have different “security natures”

Internal APIs

- Most sensitive tasks/data
- Most often security is (too) tightly coupled
- Devs have corporate credentials
- Most control over apps, devices, and security friction

Partner APIs

- Often very sensitive tasks/data
- Partners may be competitors
- Onboarding typically involves workflows
- “SSO in” often desired
- Partners tolerate more friction

APIs have different “security natures”

Internal APIs

- Most sensitive tasks/data
- Most often security is (too) tightly coupled
- Devs have corporate credentials
- Most control over apps, devices, and security friction

Partner APIs

- Often very sensitive tasks/data
- Partners may be competitors
- Onboarding typically involves workflows
- “SSO in” often desired
- Partners tolerate more friction

Public APIs

- Apps often consumer-facing
- May carry transaction value
- Third-party dev self-registration
- Often a direct business model
- Apps and devices most diverse and untrustworthy
- Devs tolerate the least friction

Agenda

- *Consumerization of IT and its cousins are challenging IAM traditions*
- *Apply Zero Trust to your identity, security, and agility problems in "bring-your-own" environments*
- *Leverage emerging technologies to provide identity services that are mobile-cloud ready*

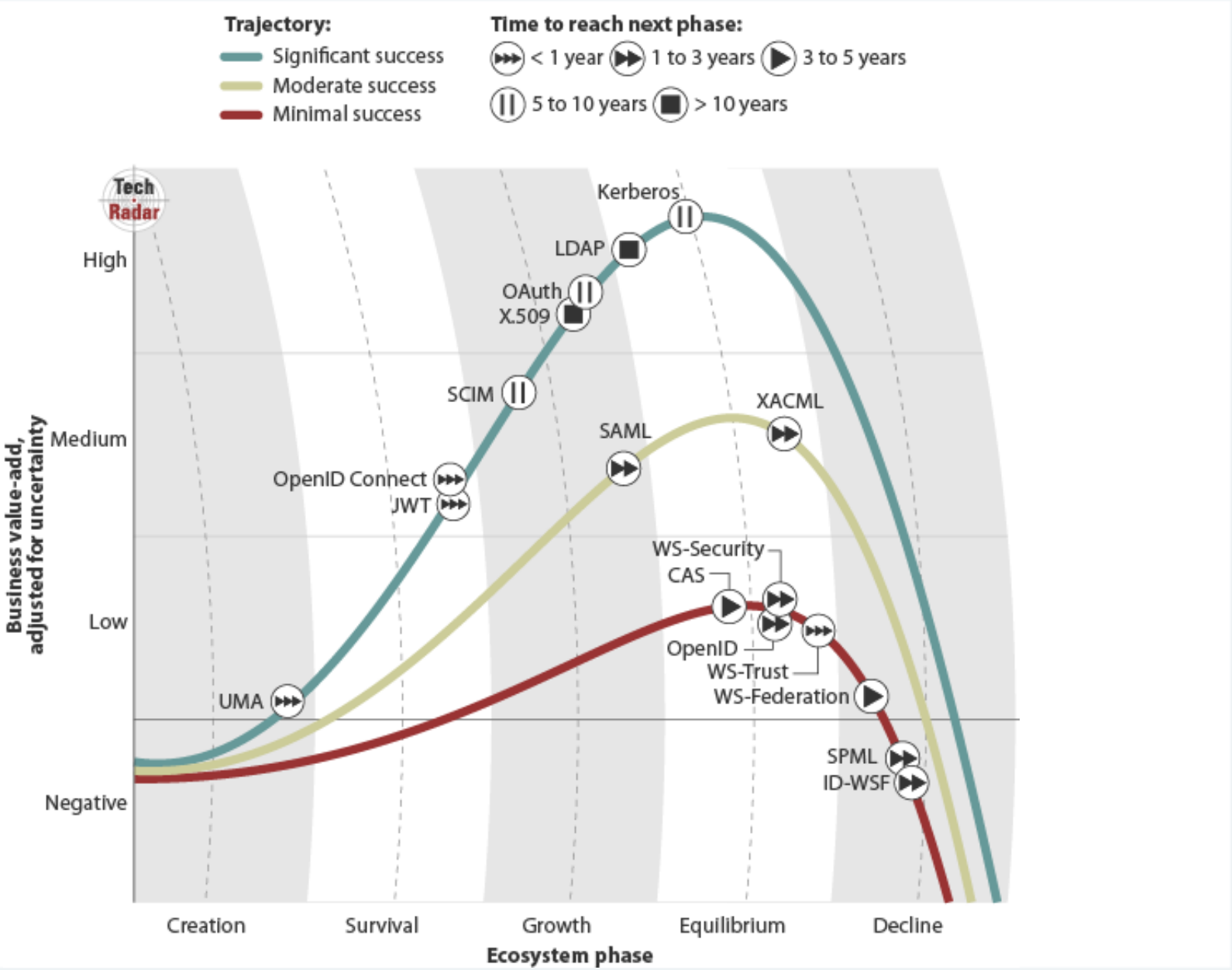
New identity solutions disrupt…but attract.

New identity solutions disrupt…but attract.

Or, The good thing about reinventing the wheel is that you can get a round one.*

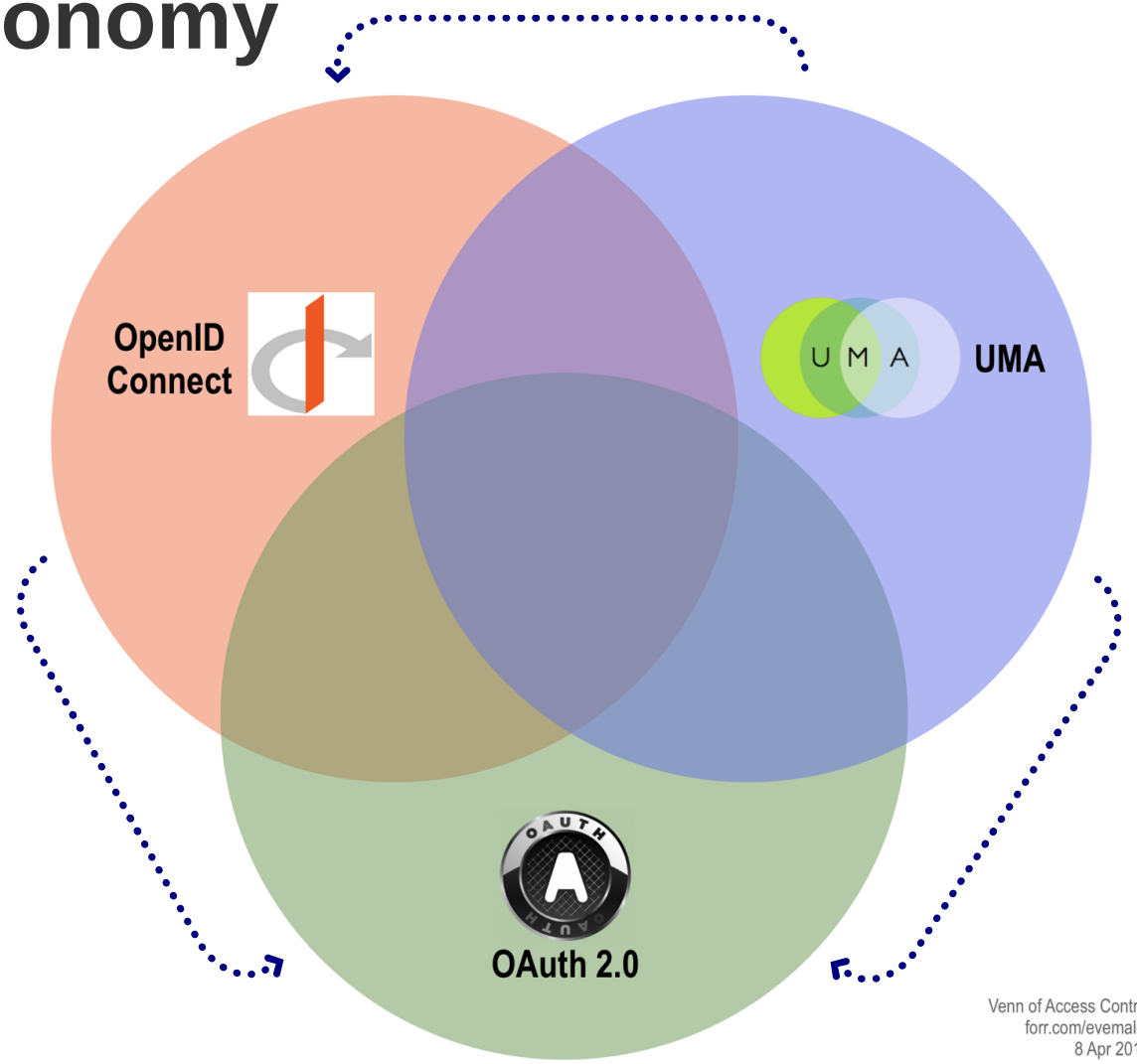
*Douglas Crockford, inventor of JavaScript Object Notation (JSON)

Emerging IAM standards have an edge over traditional ones for Zero Trust



Source: October 2012 “TechRadar™ For Security Pros: Zero Trust Identity Standards, Q3 2012”

The new Venn of access control for the API economy



OAuth can help manage risk, cost, and complexity

FOR INTERNET-SCALE ZERO TRUST, YOU NEED IT ALL

Gets client apps out of the business of storing passwords

Friendly to a variety of user authentication methods and user devices, including smartphones and tablets

Allows app access to be tracked and revoked on a per-client basis

Allows for least-privilege access to API features

Can capture explicit user authorization for access

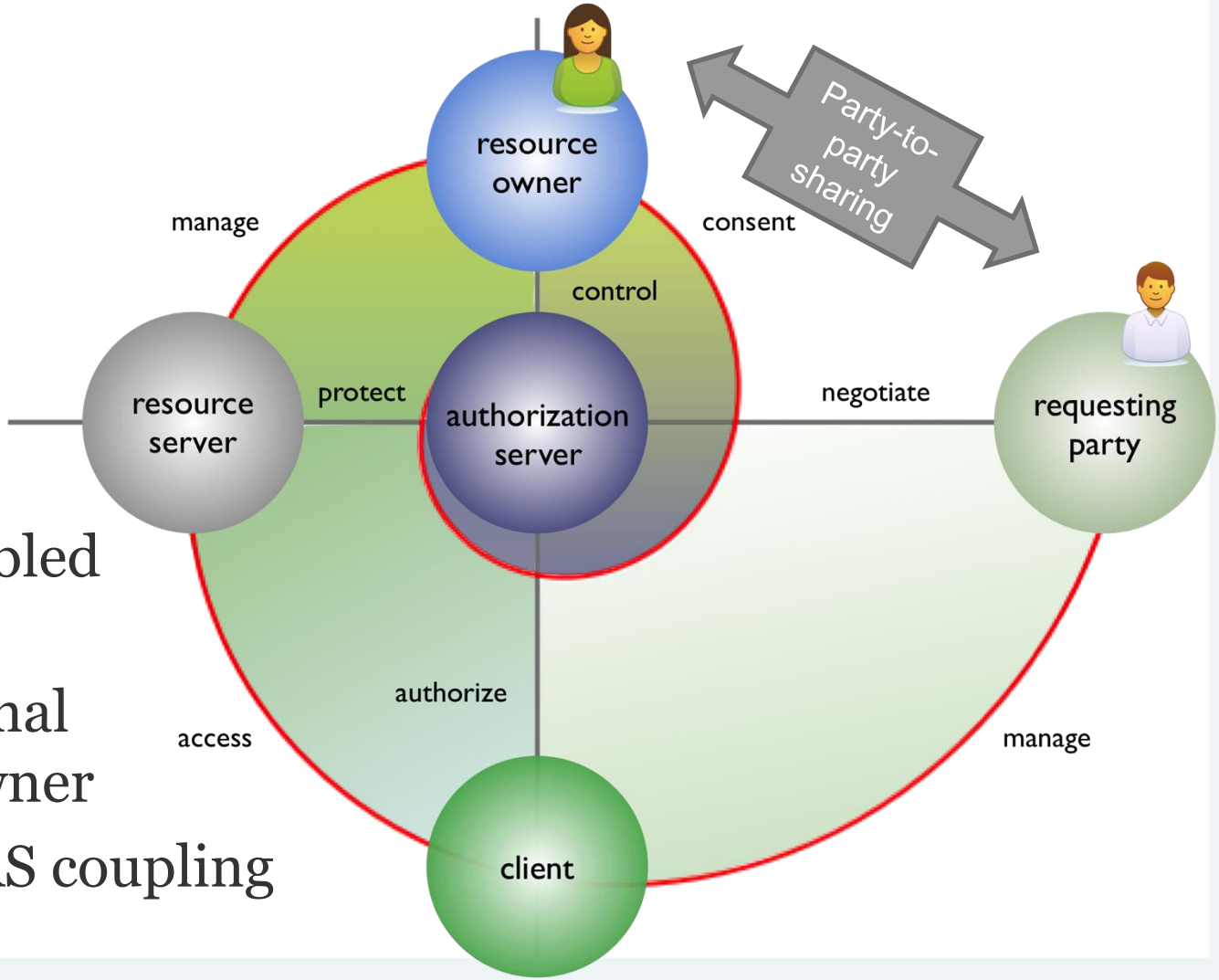
Lowers the cost of secure app development

Bonus: provides plumbing for a much larger class of needs around security, identity, access, and privacy

OpenID Connect turns SSO into a standard OAuth-protected identity API

SAML 2.0, OpenID 2.0	OAuth 2.0	OpenID Connect
✓ Initiating user's login session	✗ Not responsible for session initiation	✓ Initiating user's login session
✗ Not responsible for collecting user consent	✓ Collecting user's consent to share attributes	✓ Collecting user's consent to share attributes
✓ High-security identity tokens (*SAML only*)	✗ No identity tokens per se	✓ High-security identity tokens (*using JSON Web Tokens*)
✗ Distributed and aggregated claims	✗ No claims per se; protects arbitrary APIs	✓ Distributed and aggregated claims
✓ Dynamic introduction (*OpenID only*)	✗ Client onboarding is static	✓ Dynamic introduction
✗ Session timeout	✗ No sessions per se	✓ Session timeout (*in the works*)

UMA enables mobile-friendly scope-grained authorization



- Claims-enabled
- Human or organizational resource owner
- Loose RS/AS coupling

So, what should you do next?

Zero Trust is pulling along new Security solutions to meet new Accessibility needs


Expose accessible identity APIs for (all and only) what you're authoritative for


Assist your smaller partners in exposing identity APIs you can begin relying on


Count on mobility to disrupt old security paradigms and pull API security to the fore

Thank you

Eve Maler

+1 617.613.8820

emaler@forrester.com

@xmlgrrl

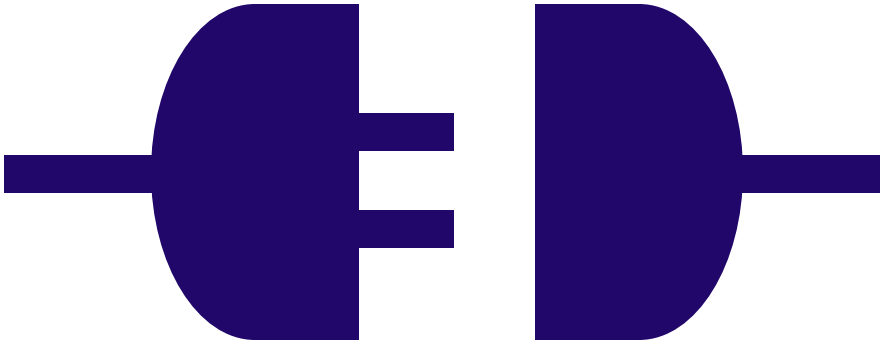
www.forrester.com

The IAM-as-an-API Era Has Arrived And You Can Blame/Thank Mobility

Tyson Whitten – Director Solutions Marketing

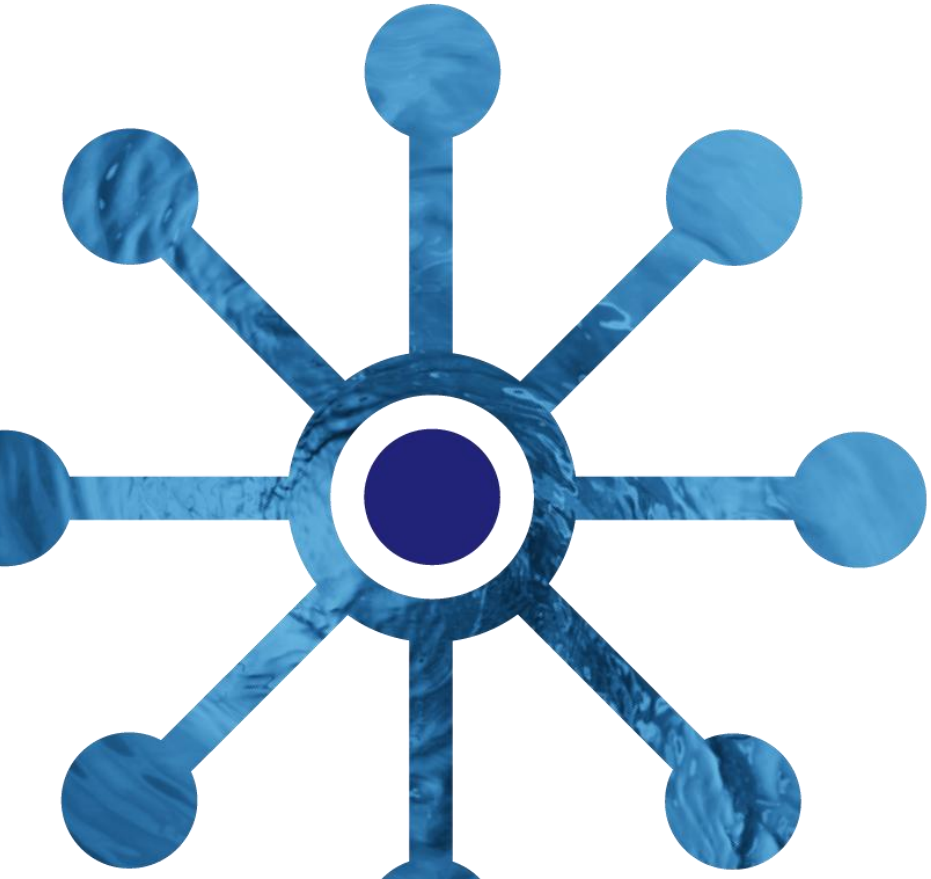
Oct 30th, 2013

While APIs are fundamental to enabling mobile app connectivity . .



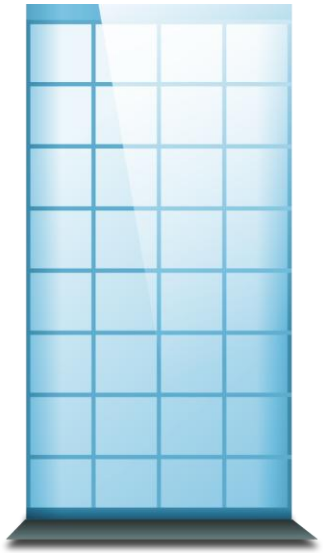
APIs

Multiple App Project Selection Factors



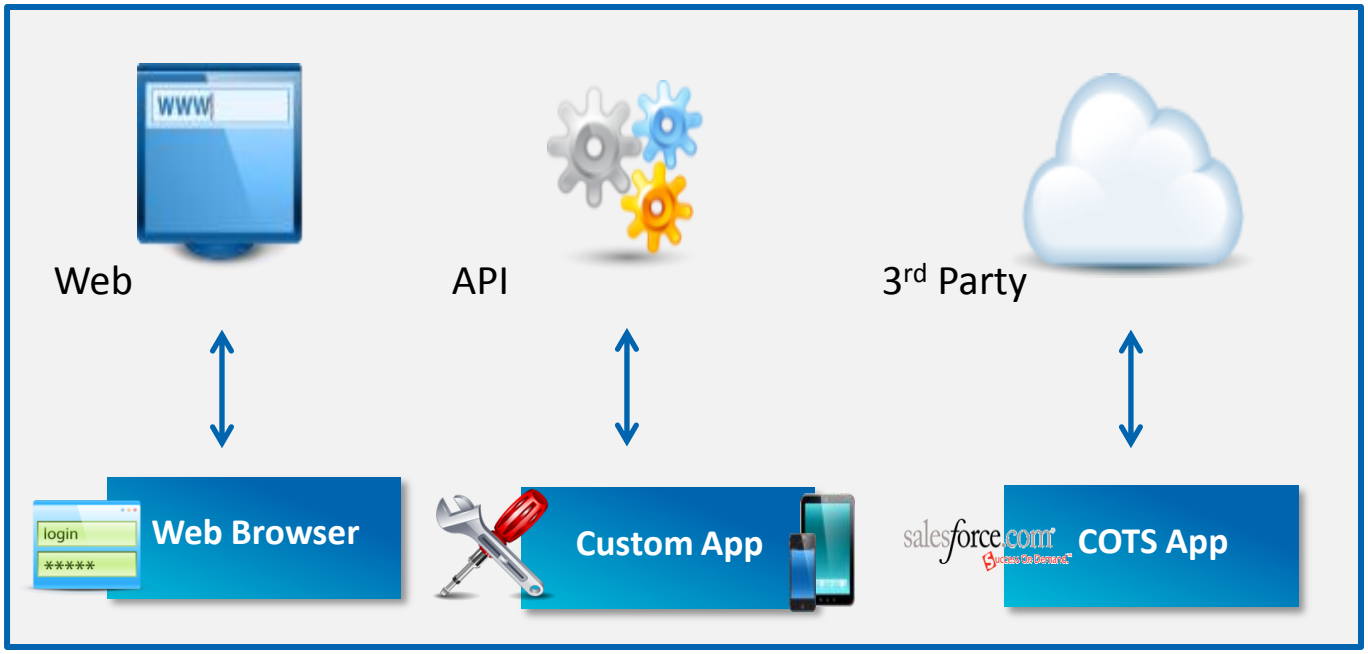
Web browser vs. native apps

Enterprise or the cloud

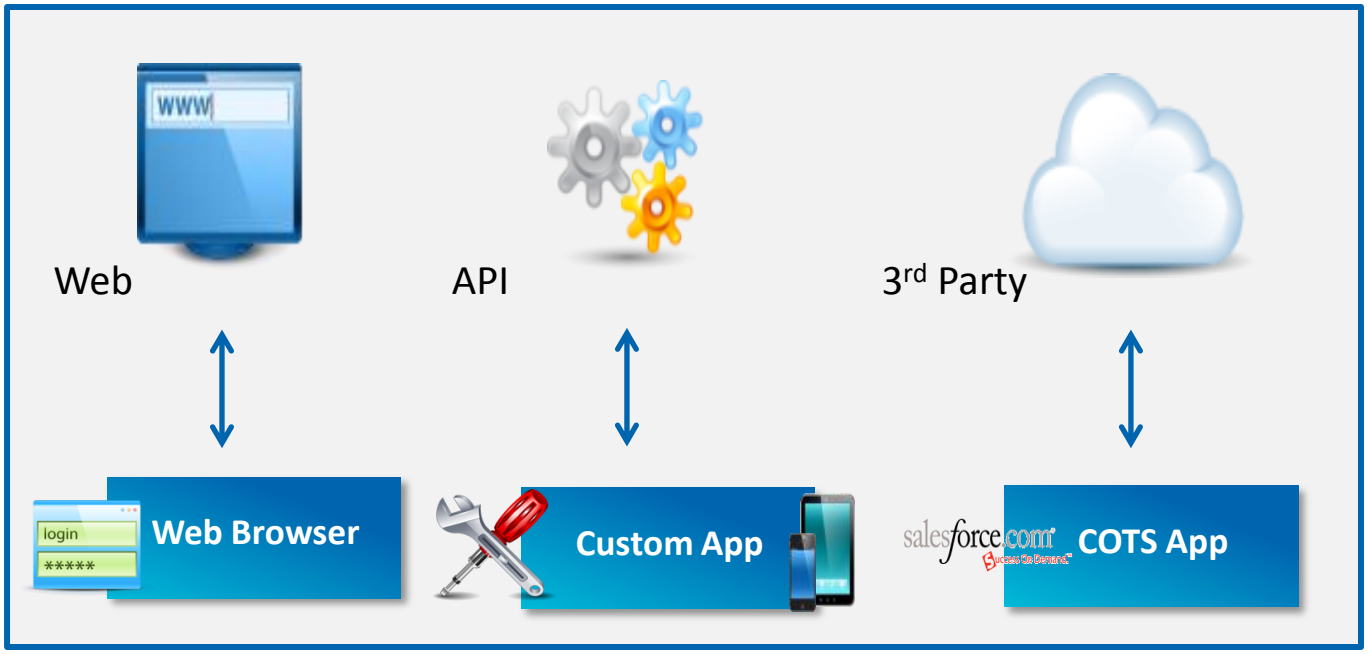


Blended Approach to Security

Different mobile apps require different security solutions



Different mobile apps require different security solutions



- **Access Management**
- **Federation**

- **API Security/Management**
- **SDK: Advanced Auth, SSO**

- **App Wrapping**

CA Mobility Strategy

Device

Device Management

Apps

API Management & Security

Application Development

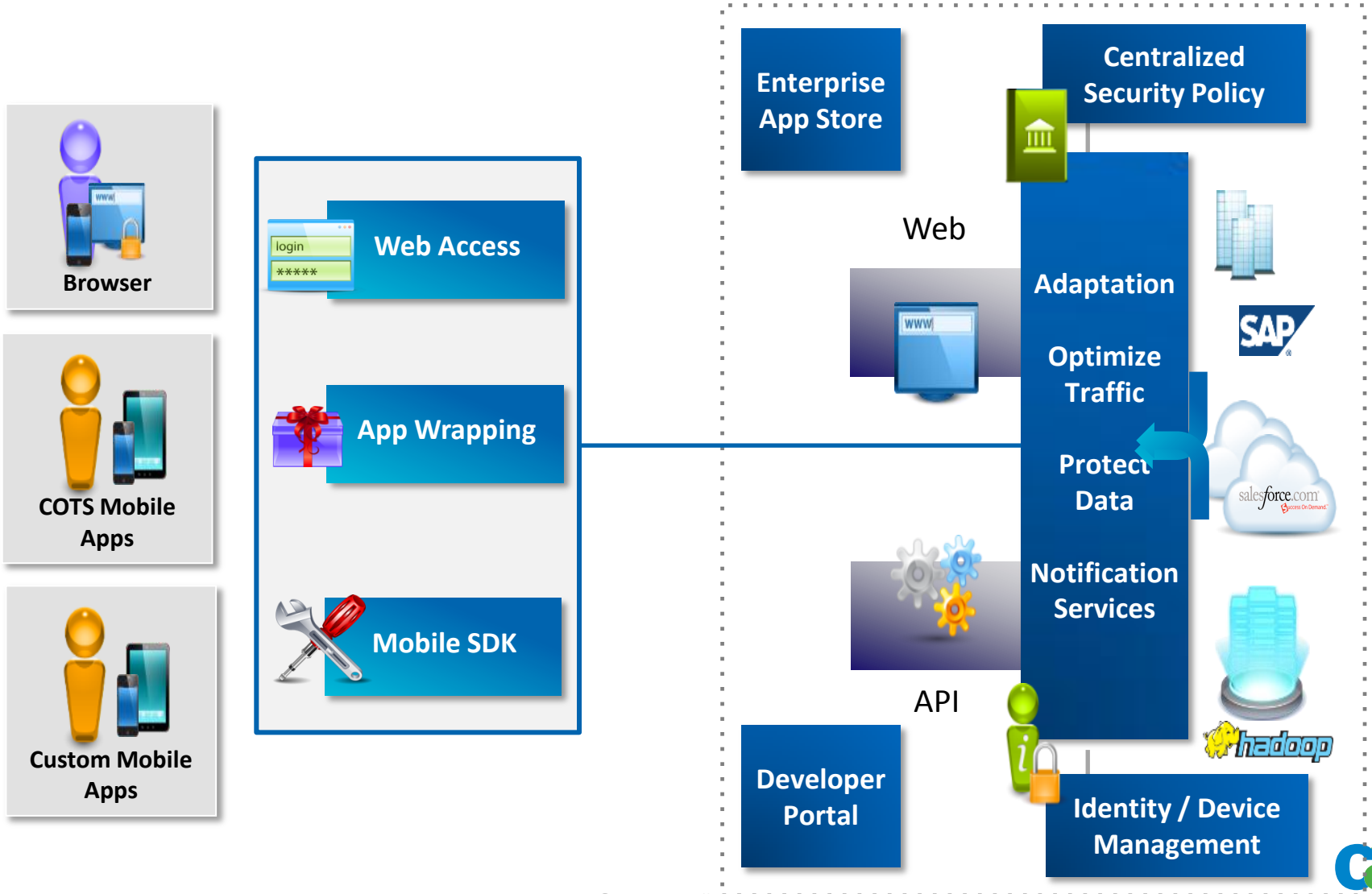
Application Management & Security

Content

Content Management & Security

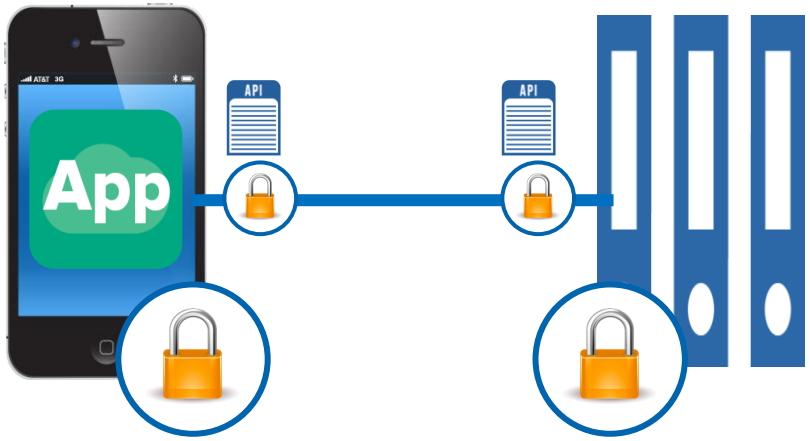
Mobile Security

Unified Security Across Web, APIs and Mobile



How a Unified Model Helps the Business

Multi-Device Universe

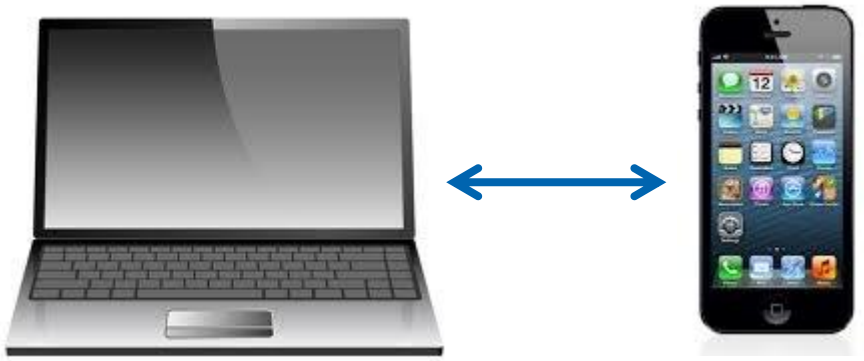


End-to-End Mobile Security

Not Just Run But Build

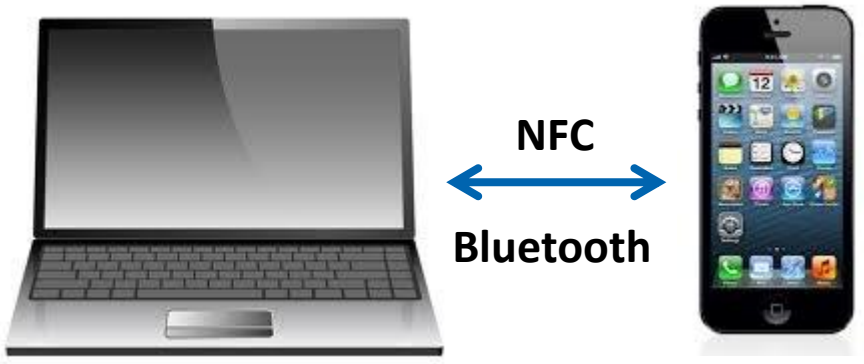
Multi-Device Universe

- Seamless transition, session and security across environments
- Automatic proximity based login (cross-device)
- Convenient access from app to enterprise app (in-domain)



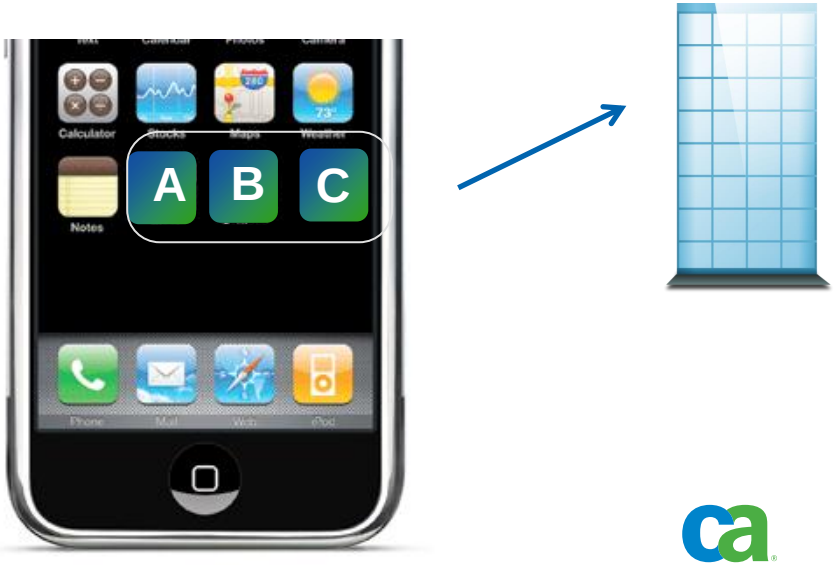
Multi-Device Universe

- Seamless transition, session and security across environments
- Automatic proximity based login (cross-device)
- Convenient access from app to enterprise app (in-domain)

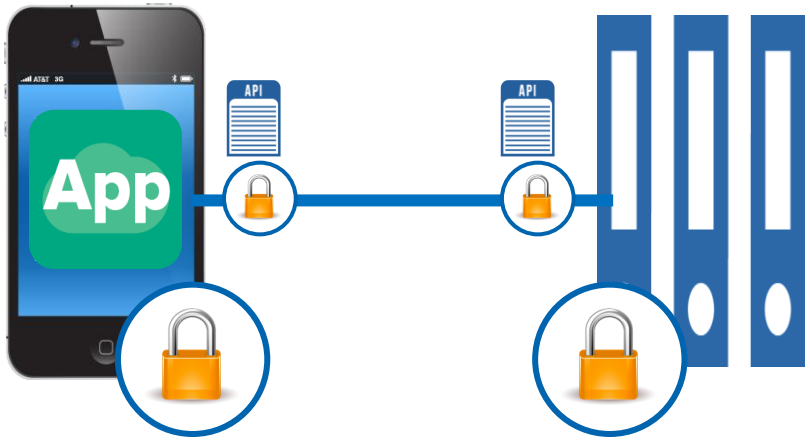


Multi-Device Universe

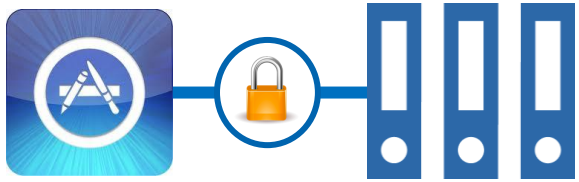
- Seamless transition, session and security across environments
- Automatic proximity based login (cross-device)
- Convenient access from app to enterprise app (in-domain)



End-to-End Mobile Security

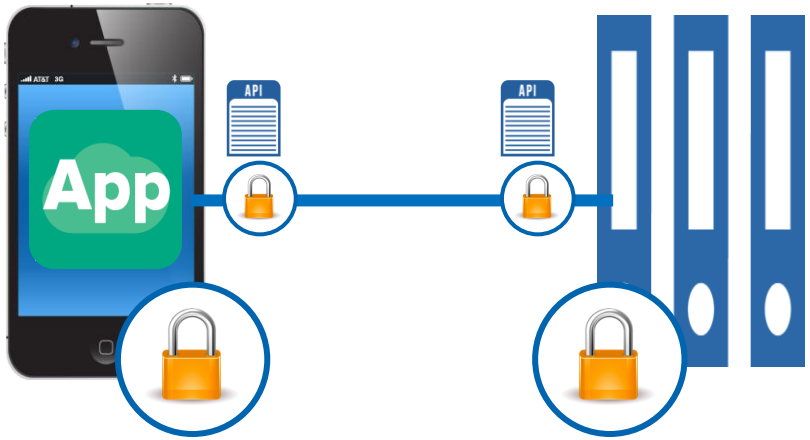


- Protect app to datacenter communication against interception
- Protect datacenter applications and database against rogue apps
- Authenticate user based on level of risk
- Ensure API level DoS for backend applications



SSL

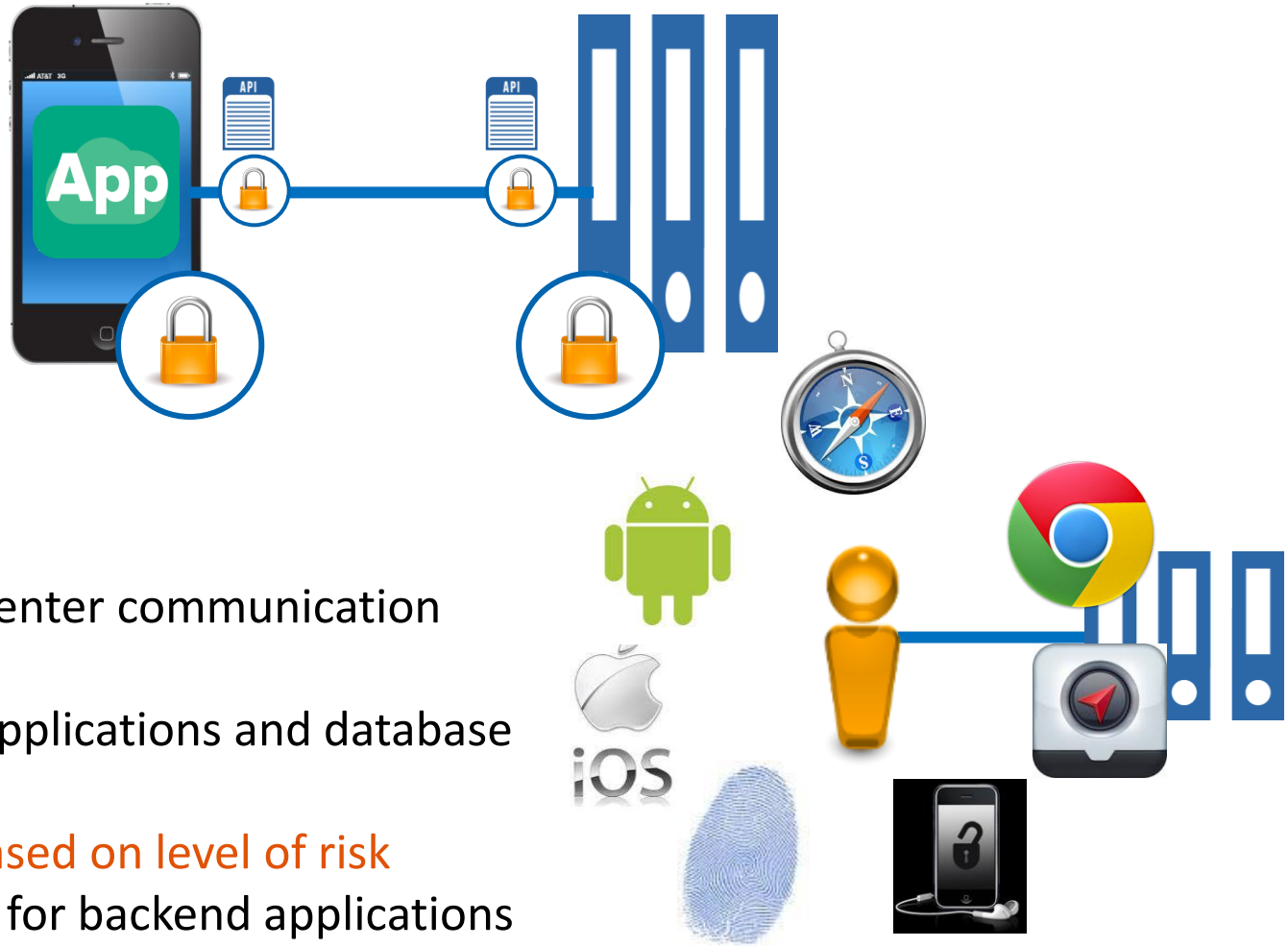
End-to-End Mobile Security



- Protect app to datacenter communication against interception
- Protect datacenter applications and database against rogue apps
- Authenticate user based on level of risk
- Ensure API level DoS for backend applications

ROGUE APP

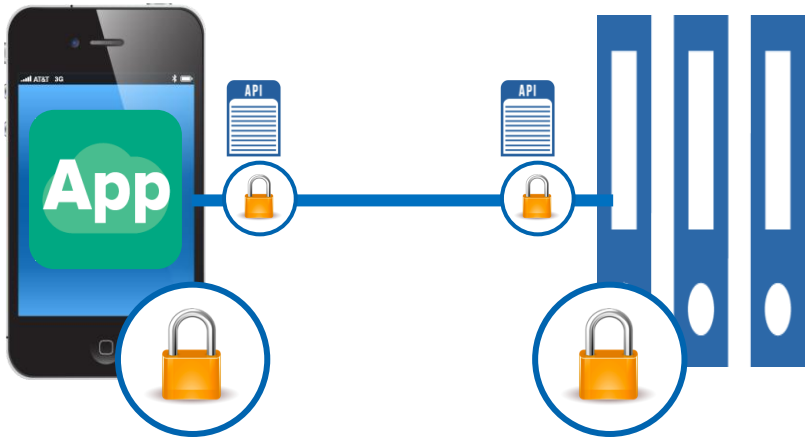
End-to-End Mobile Security



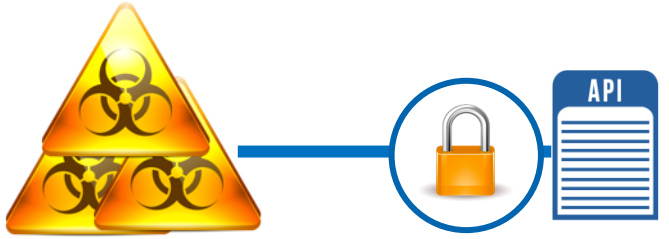
- Protect app to datacenter communication against interception
- Protect datacenter applications and database against rogue apps
- Authenticate user based on level of risk
- Ensure API level DoS for backend applications

RISK

End-to-End Mobile Security

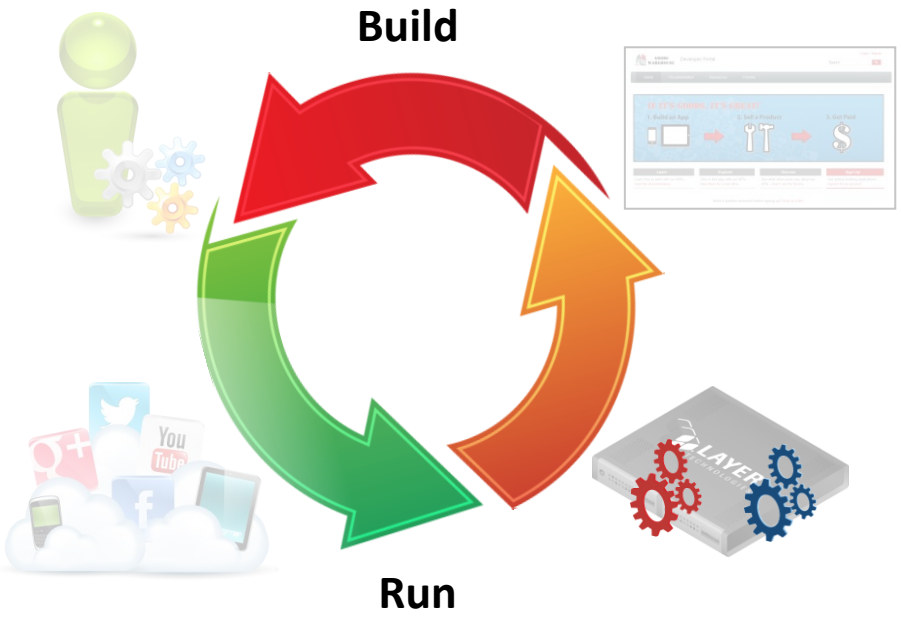


- Protect app to datacenter communication against interception
- Protect datacenter applications and database against rogue apps
- Authenticate user based on level of risk
- Ensure API level DoS for backend applications

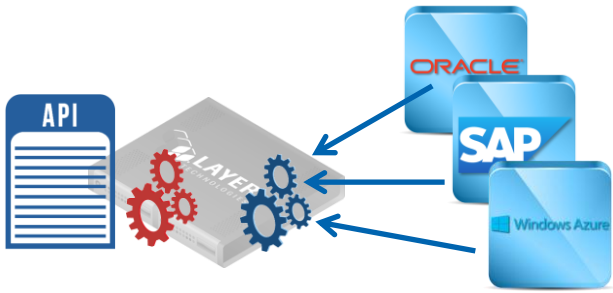


THREAT

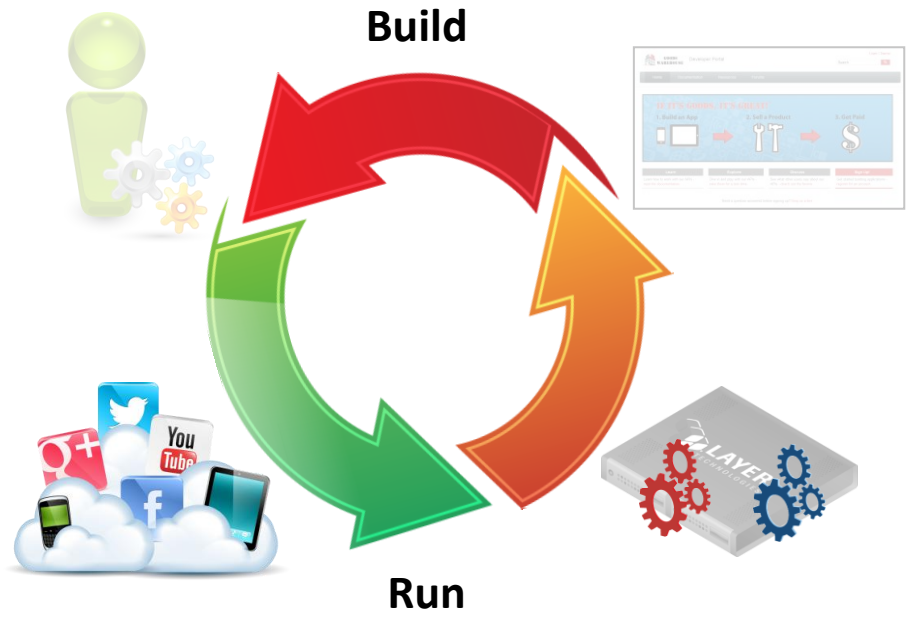
Not Just Run But Build



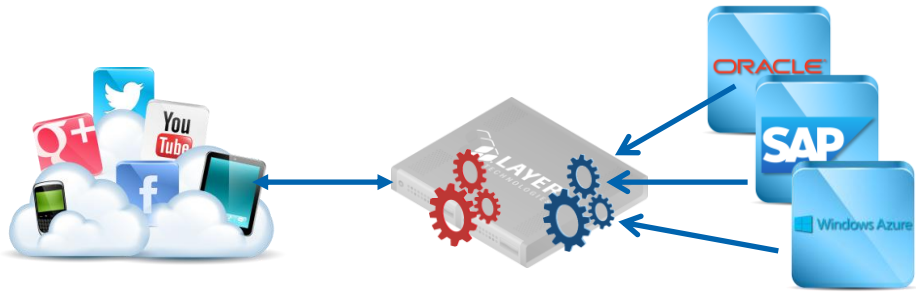
- Adapt existing services to RESTful APIs
- Optimize app caching and transactions
- Consumable services through API portal
- SDKs and security built directly into the app



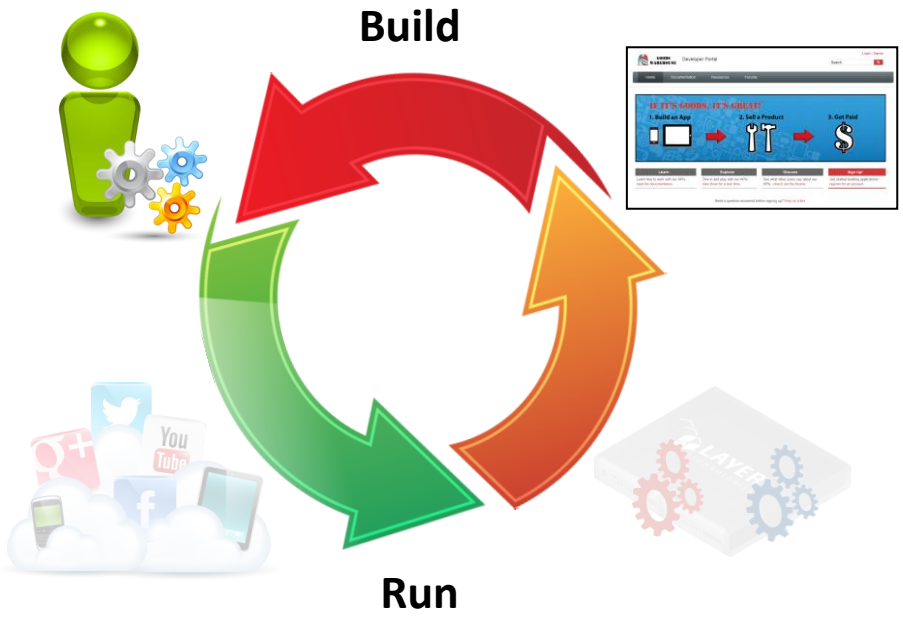
Not Just Run But Build



- Adapt existing services to RESTful APIs
- Optimize app caching and transactions
- Consumable services through API portal
- SDKs and security built directly into the app

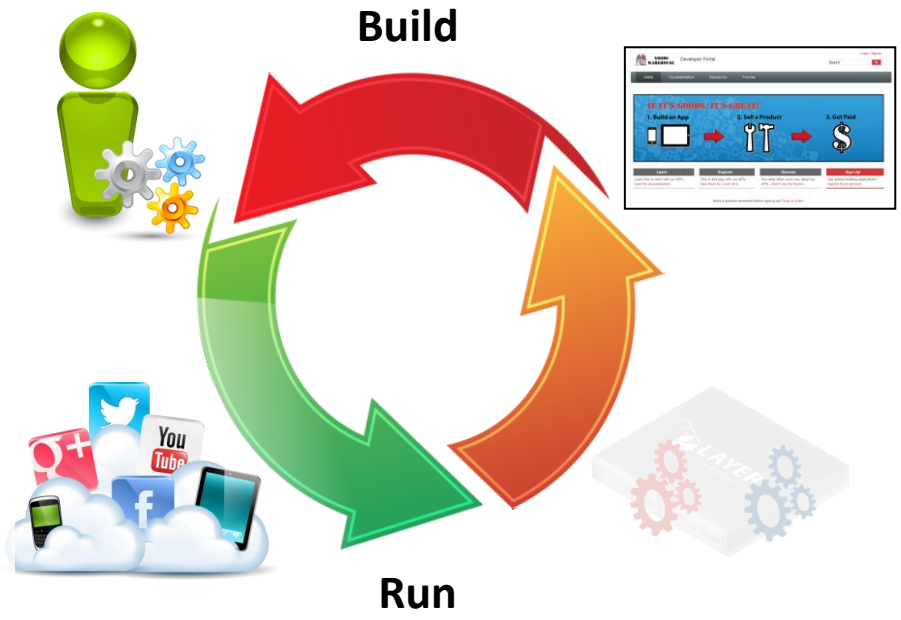


Not Just Run But Build



- Adapt existing services to RESTful APIs
- Optimize app caching and transactions
- Consumable services through API portal
- SDKs and security built directly into the app

Not Just Run But Build



- Adapt existing services to RESTful APIs
- Optimize app caching and transactions
- Consumable services through API portal
- SDKs and security built directly into the app

- Two-factor authentication
- SSO
- OAuth, OpenID Connect

CA Mobility Strategy

Device

Device Management

Apps

API Management & Security

Application Development

Application Management & Security

Content

Content Management & Security

CA Products

Thank You

notices

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.

Certain information in this presentation may outline CA's general product direction. This presentation shall not serve to (i) affect the rights and/or obligations of CA or its licensees under any existing or future written license agreement or services agreement relating to any CA software product; or (ii) amend any product documentation or specifications for any CA software product. The development, release and timing of any features or functionality described in this presentation remain at CA's sole discretion.

Notwithstanding anything in this presentation to the contrary, upon the general availability of any future CA product release referenced in this presentation, CA may make such release available (i) for sale to new licensees of such product; and (ii) in the form of a regularly scheduled major product release. Such releases may be made available to current licensees of such product who are current subscribers to CA maintenance and support on a when and if-available basis.