RSA CONFERENCE ASIA PACIFIC 2013

PRACTICAL IDENTITY AND ACCESS MANAGEMENT FOR CLOUD - A PRIMER ON THREE COMMON ADOPTION PATTERNS FOR CLOUD SECURITY

Shane Weeden

IBM

Session ID: CLD-W01

Session Classification: Advanced

Agenda

- Cloud security in context
- Maturity Model
- Cloud Security Adoption Patterns
  - Demonstrations as we go
- Tips for getting started

Cloud security in context

Cloud offerings

- IaaS: Rackspace, Amazon, Openstack
- PaaS: Azure, Heroku, CloudFoundry
- SaaS: GoogleApps, Salesforce, Workday

Security Standards

SAML, OpenID, OAuth, Basic-Auth, OpenID Connect, WS-*, SSL/TLS, SCIM, XACML

API's & Social

Clients

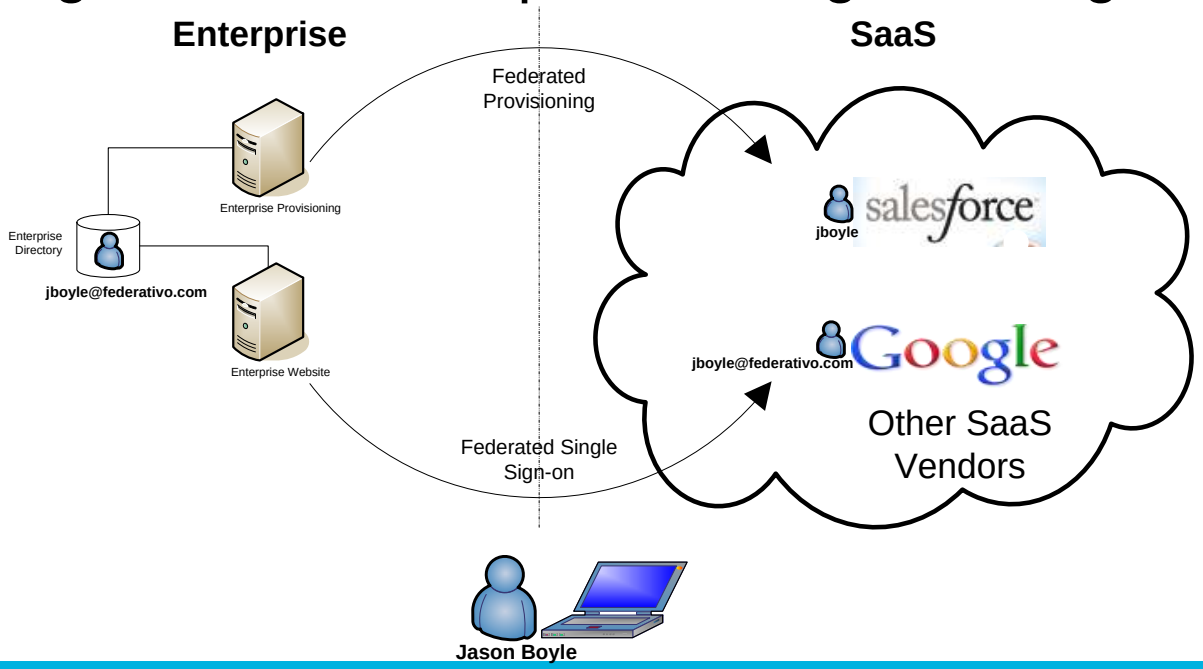
Browsers Mobile B2B

Cloud Security Maturity Model for IAM

Optimized	**Security Intelligence:** User activity monitoring, Anomaly detection, Identity Analytics & Reporting	
	•User Certification for SaaS applications access	•IAM-as-a-Service •User Certification for SaaS application access •Federation to/from IaaS and PaaS
Proficient	•Application based Just-in time Provisioning •Increased Assurance (OTP) •Risk / Context-based Access •Application-to-Application token exchange •Mobile Application Access to SaaS	•Bring Your Own Identity with Increased Assurance •Enterprise based Just-in-time provisioning •Risk / Context-based Access •Identity Propagation •Mobile Application Access to SaaS
Basic	•Federated SSO •Directory Synchronization for Cloud/SaaS providers •Web Application Protection	•Federated SSO •User Provisioning for Cloud/SaaS provider •Securing Web Infrastructure
Owner	**Line of Business**	**Enterprise IT Operations**

Integrating with SaaS

- Pattern: Identity and access to the cloud
  - Examples: Salesforce, GoogleApps, Workday, Office365, IBM SmartCloud for Social Business
- Target: B2E
- Technologies: Federated provisioning and single sign-on



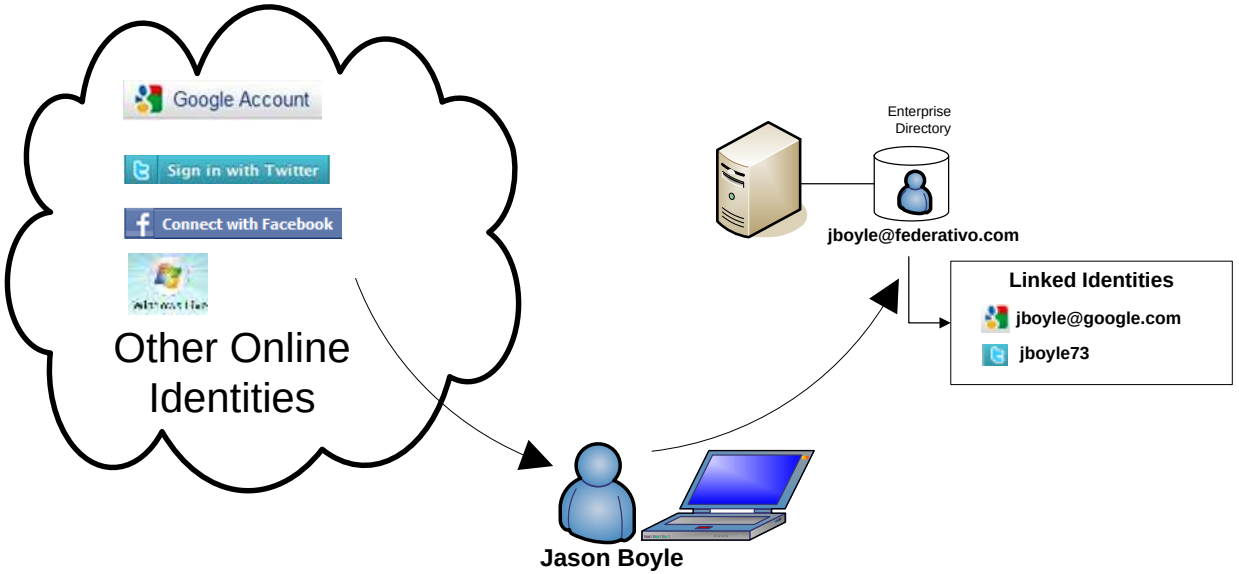
Integrating with SaaS

- Questions to ask
  - How will I provision users to the SaaS offering? Automated?
  - What SSO technologies and standards do they support?
    - What are the deployment requirements (POST, artifact, discovery)?
    - Do you already have the IDP capability?
  - Is user identity mapping required as part of SSO?
  - What about de-provisioning?
  - Is access required when employees are not in the office?
  - Is mobile or thick client interaction available and how does authentication work for that?

Implementing BYO-ID

- Pattern: Bring your own identity
  - Examples: LinkedIn, Facebook, Twitter, Google, Yahoo
- Target: B2C
- Technologies: Self-registration, single sign-on, user self-care

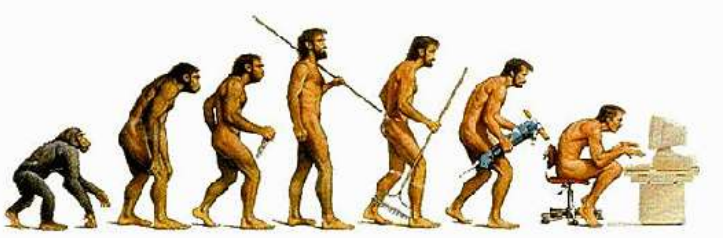
"Making access easy, with a familiar, fast, fun and secure user experience is key to attaining and retaining new customers."



Implementing BYO-ID

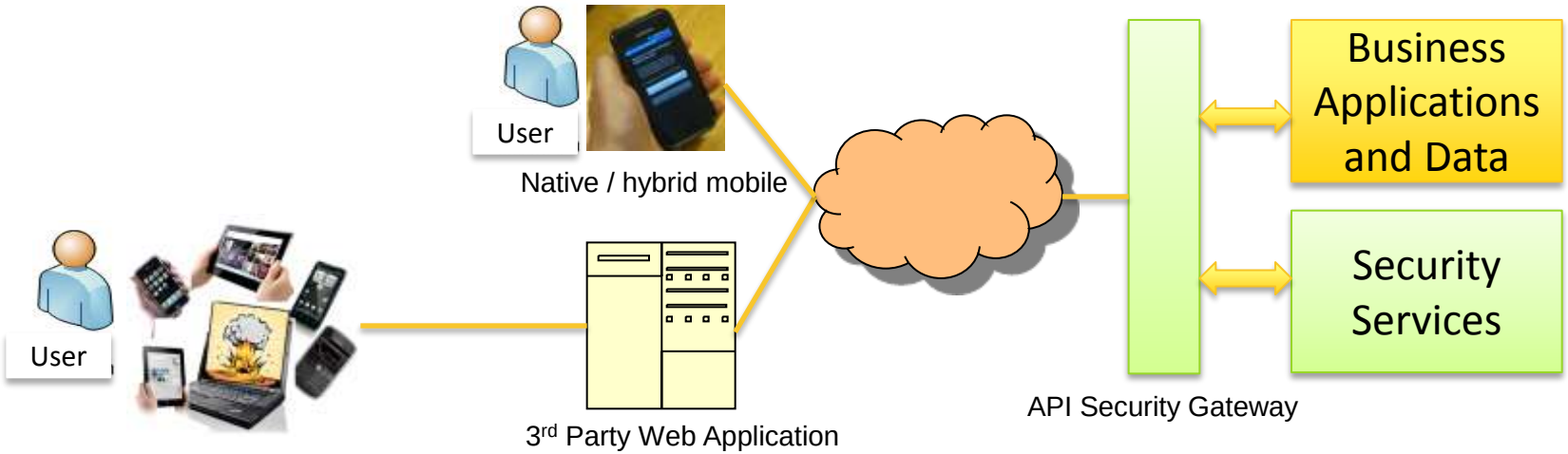
- Questions to ask
  - Which IDP's should I use, and how much trust should I place on the data they assert?
  - What will I use external identities for (self-reg, SSO, data)?
  - What SSO technologies and standards do they support?
    - Loosely coupled rather than strong B2B, so usually OpenID, OAuth.
    - Google – OpenID 2.0, Twitter, LinkedIn - OAuth 1.0, Facebook OAuth 2.0 (early draft)
  - Have I considered the full account and identity lifecycle?
    - There are a lot of "edge cases".
  - If I adopt this technology, are there additional use cases that could be leveraged beyond BYO-ID for self-reg and SSO?
    - Example: integration with social media API's that provides a fun user experience, but which may also attract new customers.

Business via API



No IT➟Internal IT➟Web 1.0➟Business via API

- Pattern: Exposing services via API
  - Examples: Google API's, Twilio, Facebook, CloudFoundry
  - See www.programmableweb.com
- Target: Mobile, B2B
- Technologies: OAuth, Basic-Auth, Mutual SSL, WS-*



Implementing Business via API

- Questions to ask
  - What “business” services do I want to expose?
    - Do they required different levels of access (scope)?
  - What is the revenue model?
  - What standards / patterns am I going to support?
    - Consider client types – browsers (Web 2.0), mobile, B2B
  - Do I want to whitelist clients, or adopt a “Field of Dreams” model?
    - Do my end-users need to have a say?
    - What interfaces will I expose to users and administrators for managing delegated trust, including revocation?
    - What interfaces will I expose to application developers for self-serivce?
  - NFR’s: If this is successful, can I scale it, monitor, etc?

Getting started

- Pick a business problem, get a sponsor
  - Maybe that's already been done for you!
- Focus on the customer experience
  - Example – mobile security device registration
- Research, experiment, evaluate
  - Design for the future, e.g. business via API supports many channels.
- Manage and balance security risk against business value and user experience

Thank you!