

# How the Cloud is Changing Federated Identity Requirements

Patrick Harding  
CTO, Ping Identity  
@pingcto  
March 1, 2010

# The Return of Timesharing

<http://www.flickr.com/photos/quinnanya/2690873096/>



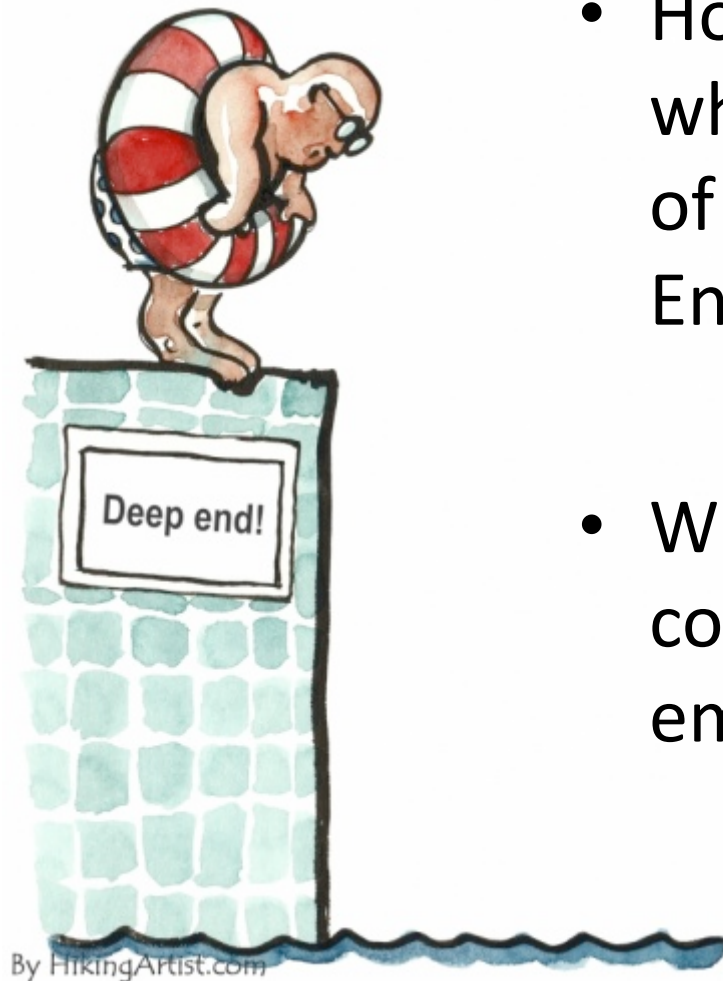
# From Earth to Sky



<http://www.flickr.com/photos/quinnanya/2690873096/>

- No longer build vs. buy
  - Now build, buy or subscribe
- Enterprise data and accounts are moving to remotely run “cloud services”
- Less IT involvement
  - Double edged sword

# But what are the Tradeoffs?



By HikingArtist.com

- How do requirements change when data and access are out of the direct control of the Enterprise?
- What can be done to protect corporate resources while still embracing this new paradigm?

# Oh, How Our Jobs Have Changed

- Remember when all we had to do was lock things up?
- Remember when every application had its own port number?
- Remember when access to the internet was a luxury rather than a necessity?
- Remember the days when your bosses idea of integration was collated paper reports?

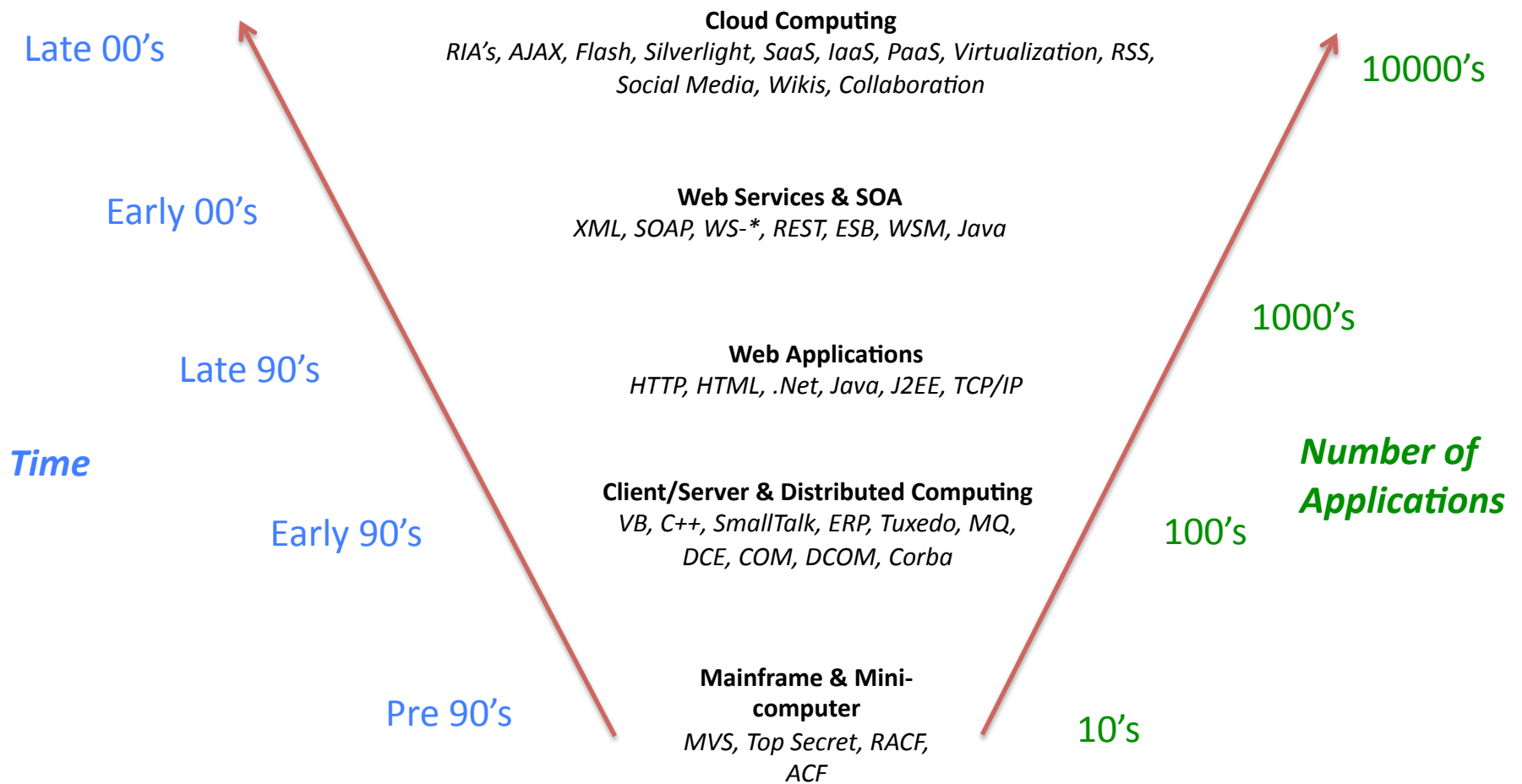


# Protectionism is out

- Now we need to be Open – but Secure
- Porous but Protected
- Easy to use but Hard to Abuse
- Agile but Armored
- Connected but Self-Contained
- Our new job description:

*Implement an Oxymoron*

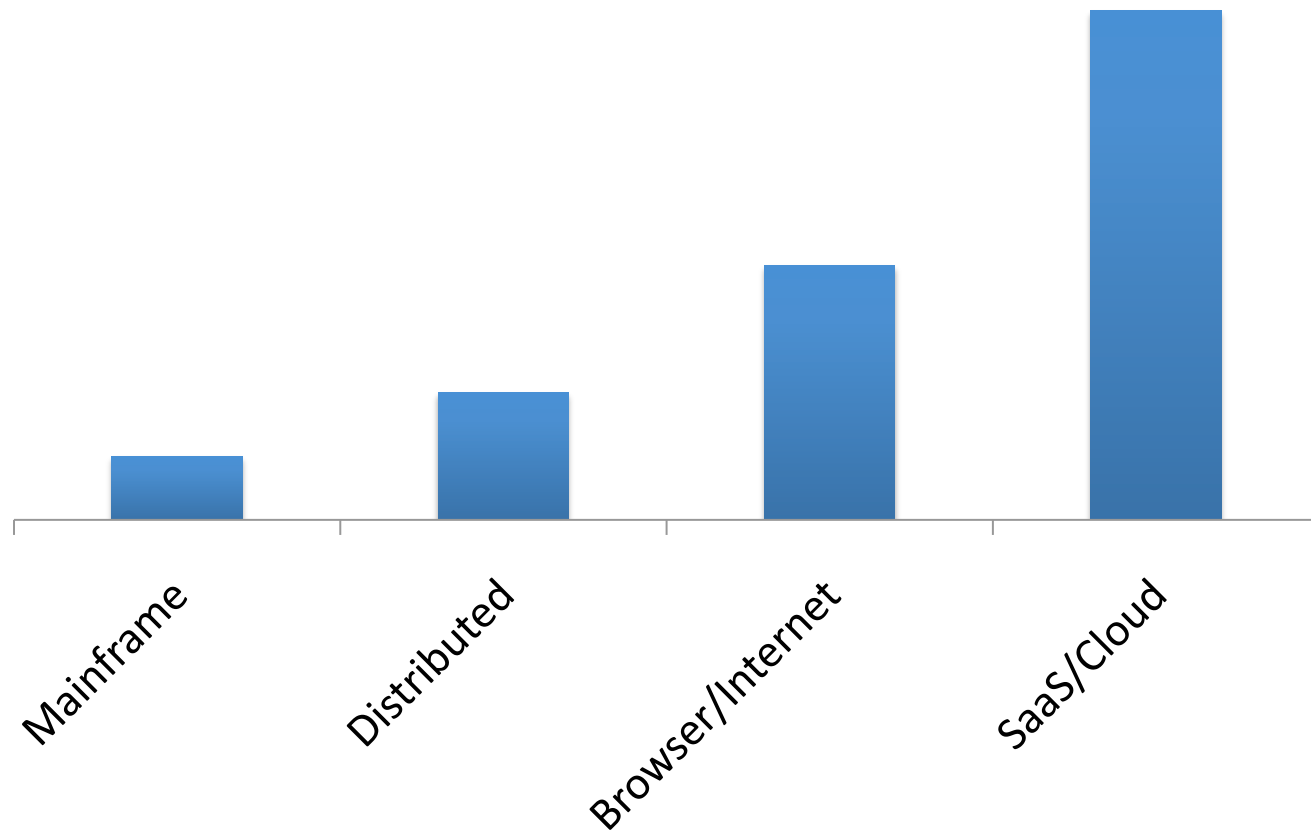
# Security: Last Again





# Complexity: Worse than Ever

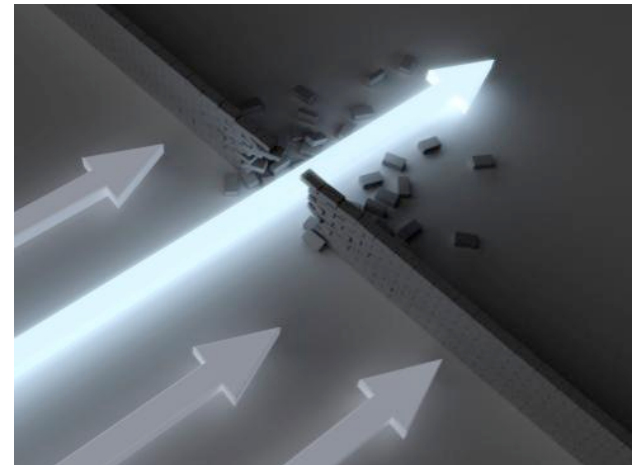
Average # Applications Per User





# Services: Any to Any

- Organizations Need to Support:
  - Internal User Access to Internal Applications
  - Internal User Access to Cloud Applications
    - E.g. SaaS, BPO, Partner, Vendor Apps
  - External User Access to Internal Applications
    - E.g. Customer, Partner, Vendor access
  - “Mashups”
    - Identity-Enabled Web Services



# Audit: No Longer an Afterthought

- Sarbanes-Oxley
- Health Insurance Portability & Accountability Act (HIPAA)
- Gramm-Leach-Bliley
- EU Directive 95/46/EC

## Prerequisites:

- Identity Security
- Data Security
- Access Control
- Internal and External Applications



# Visibility: Expected by Management



[http://www.flickr.com/photos/roman\\_emin/3388408921/](http://www.flickr.com/photos/roman_emin/3388408921/)

- Compliance is the new religion
- Often purchased, rarely achieved
- Personal opinion:
  - Govern, don't comply

# Summary of Challenges

- New Business Application Delivery Models Demand a Internet-friendly, Identity-based Security Model
  - Internal and External Web Applications/Web Services
  - Any Device, Anywhere
  - Secure, Portable, Standards-based
- The Overhead and Risk From Passwords Must Be Reduced
  - Compliance Issues
  - Security and Risk Factors
  - User and IT Productivity Gains



# Enterprise IT Impact

- Significant Enterprise IdM Infrastructure Can Be Made Irrelevant
  - Directories
  - Identity Management Systems
  - Strong User Authentication
    - e.g. Security Tokens, X.509 Certificates
  
- These are Multi-million Dollar, Multi-year Investments
  - Driven by
    - Ease of Use
    - Cost Reduction
    - Risk, Security and Compliance



<http://www.flickr.com/photos/streart-berlin/3374855273/>



<http://www.flickr.com/photos/toffehof/244870161/>

# Requirements Must Change

- Every cloud application **MUST** be treated like a black box
- Every RFP should be asking:
  - “How do I externalize AuthN,? AuthZ? Audit? Provisioning?”
- It isn't any longer about **BUYING** compliance
  - It is about seeing it
- Hooking audit logs into dashboards will be the new metric
  - not promises from IT staff that things are being logged silently



# New: Cross Domain Oversight

- Authentication & SSO
  - SAML
  - OpenID
- Delegation
  - WS-Trust
- Authorization
  - XACML
  - OAuth
- Provisioning
  - SPML
  - Proprietary API
- Audit
  - A6



[http://www.flickr.com/photos/jay\\_que/301153387/](http://www.flickr.com/photos/jay_que/301153387/)



# Long Awaited: Levels of Assurance



<http://www.flickr.com/photos/mnemonic/20530112/>

- Matching protocol to domain of use
  - Not every application is created 'equal'
    - Context is key
  - Multiple Tools for multiple purposes
- Social Networking apps have a place in the Enterprise
  - Conversions are the drawing factor
    - Customers
    - Recruiting
- Alongside regulated applications (e.g. SARBOX, HIPAA)

# Changed Risk: Passwords

- If you don't federate you are faced with two choices:
  - Force your users to set their own separate password at every corporate cloud site you contract with
    - Guess which password they will use?
  - Synchronize your users' passwords to every corporate cloud site you contract with
    - That way the hackers get all the passwords in one fell swoop

## Expanded Utility: SSO

- Cookies didn't cut it – tokens raise the bar
- Access control via EXPLICIT Security
- Ownership of user validation stays in the Enterprise
- User gains access to the resources of multiple software systems without being prompted to log in again



# Today we Push

- Federation with SaaS is Push-Oriented
- IdP-Initiated SSO
  - User must start at corporate portal
  - Portal requires list of all cloud applications
- API Driven User Provisioning
  - Starts with groups in corporate directory
  - Batch oriented



# Tomorrow we Pull

- Push won't scale to support hundreds of applications in the cloud
  - User access anytime, anywhere, any device
  - Just-in-time access verification
- SP- Initiated SSO
  - Must address IdP Discovery
  - Authentication at the Edge
- Assertion Based Provisioning
  - with Attribute Query Services
  - and real time requests for role verification etc
    - via Federated Authorization
- Access & Audit logs accessed via secure Pub/Sub [future]



[http://www.flickr.com/photos/caveman\\_92223/3024787175/](http://www.flickr.com/photos/caveman_92223/3024787175/)

# Domain Based IdP Discovery

**Sign In**

Username:

Password:

[Forgot Password?](#)

Keep me signed in

Use Secure Access

New User? [Sign Up](#) for Free!


---

Sign In using

STEP 1

STEP 2

**Sign in using Google Apps Account**



www.

eg: yourdomain.com

« [Back to Sign In](#)



# Privileged User Management

- Cloud Apps allow ‘super user’ access
  - SalesforceCRM Admins
  - Amazon EC2 Admins
- Equivalent to ‘root’ or ‘Admin’ on production systems
- Business Imperatives
  - Strong authentication
  - Access appropriate to role



<http://www.flickr.com/photos/sillygwaito/348769786>



# Strong Auth Imperative

- “No passwords in the cloud”
- Implement Centralized Strong Auth
- Federated SSO can make Strong Auth cost effective
  - Tokens, Certs, MFA



# Summary

- Cloud requires Internet-friendly, Identity-based Security Model
- # Passwords Must Be Reduced via SSO
  - ‘No Passwords in the Cloud’
- Cloud Scale will require Pull, not Push
- Consider Strong Auth as de-facto Auth Mechanism

*Ping Identity Can Address The Oxymoron*

# Questions