Warm Up to Identity Protocol Soup

David Waite

Principal Technical Architect

Ping Identity

The **Cloud Identity Security** Leader™

Topics

- What is Digital Identity?
- What are the different technologies?
- How are they useful?
- Where is this space going?

Digital Identity

The **Cloud Identity Security** Leader™

Concepts

- Authentication / Authenticity
  - –Is this entity (person/machine) who they say

Concepts

- Attributes / Identity Information
  - My name is David Waite
  - I work for Ping Identity
  - I've been in the Identity Space for 10 years
  - My email address is dwaite@pingidentity.com

Introductions

- Ping Identity
  - –Focused on Identity standards
  - –Enterprise and Consumer-oriented solutions
  - –On-site software (PingFederate)
  - –Identity as a Service offerings (PingOne)

Concepts

- Authorization
  - –What are the rules on who can do what
- Access Control
  - –Enforces whether you can or can’t do something

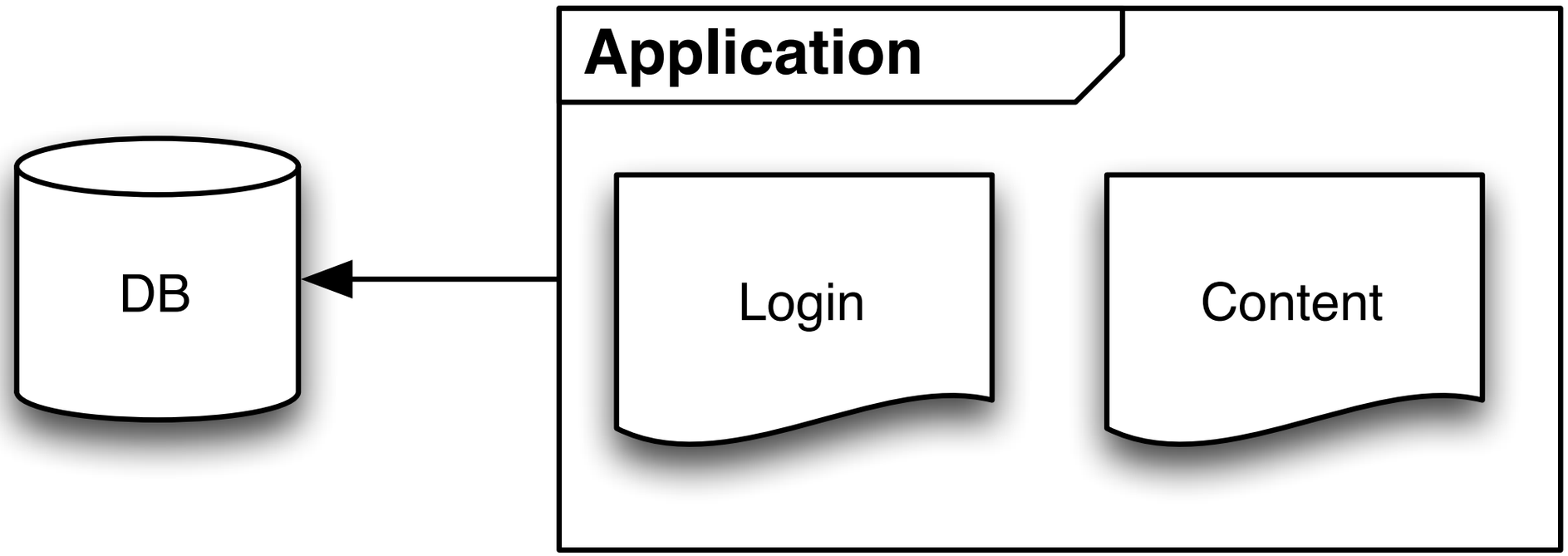
Concepts

- The bundle of credentials, identifiers and attributes makes up the traditional idea of an “Account”
- The services which work by the same system of accounts and authorization make up a “Security Domain”

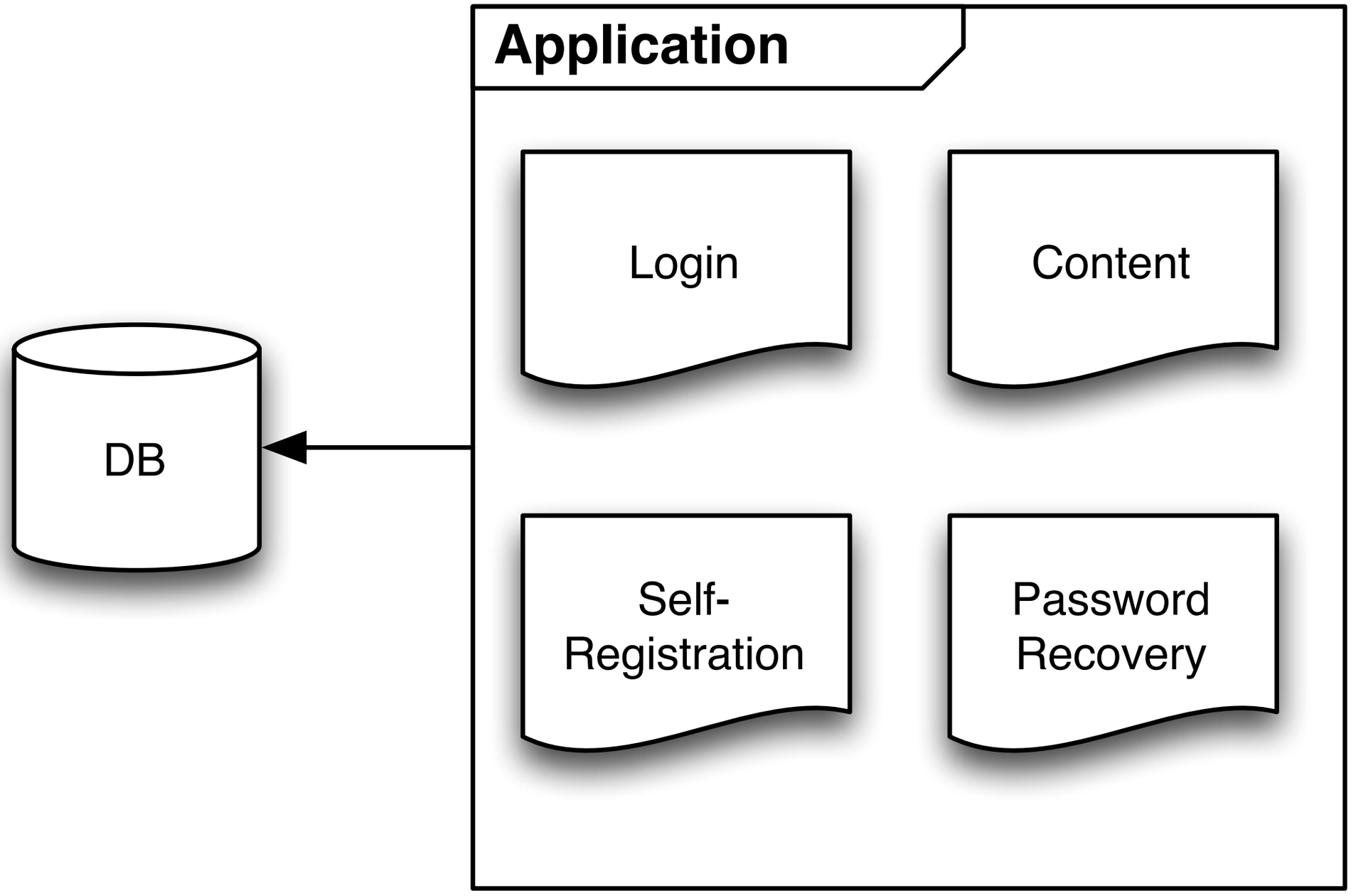
SAML / In the Beginning

The **Cloud Identity Security** Leader™

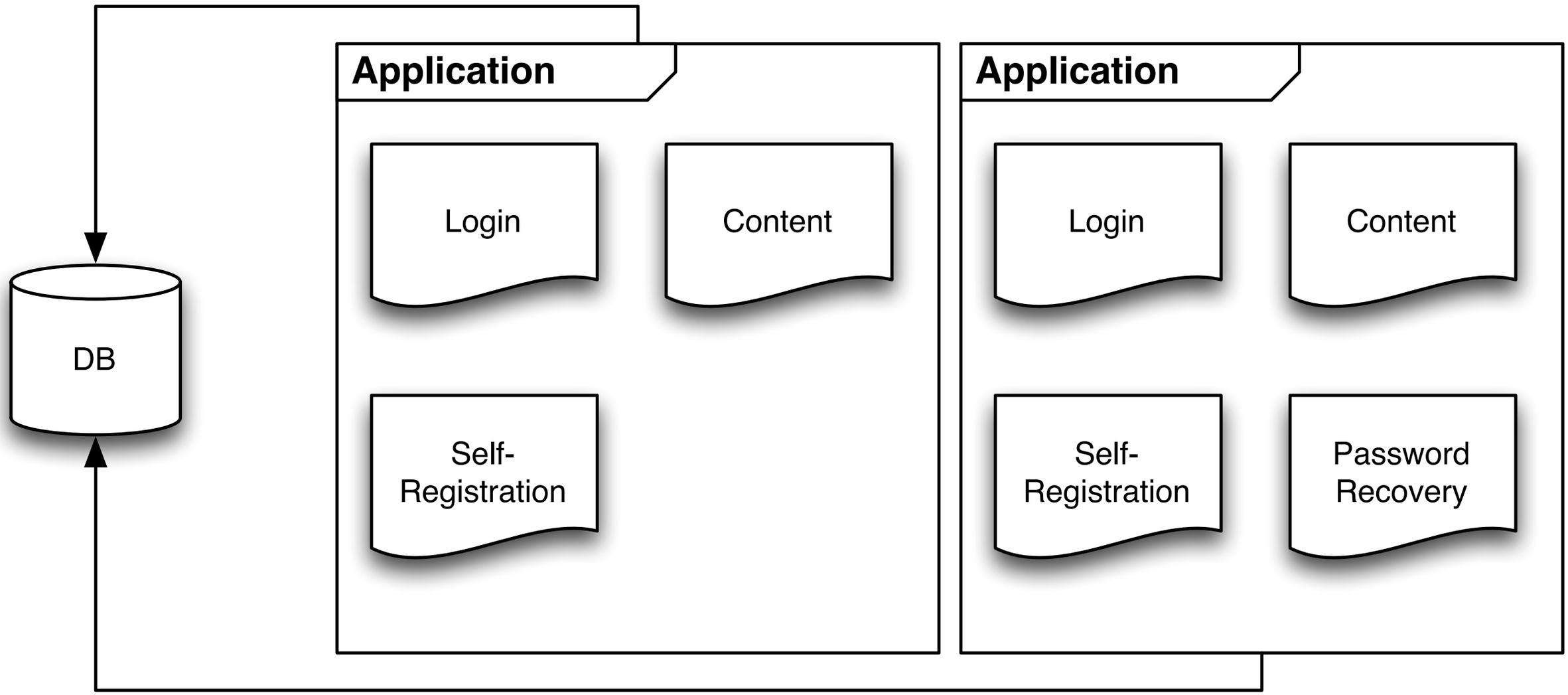
Simple App



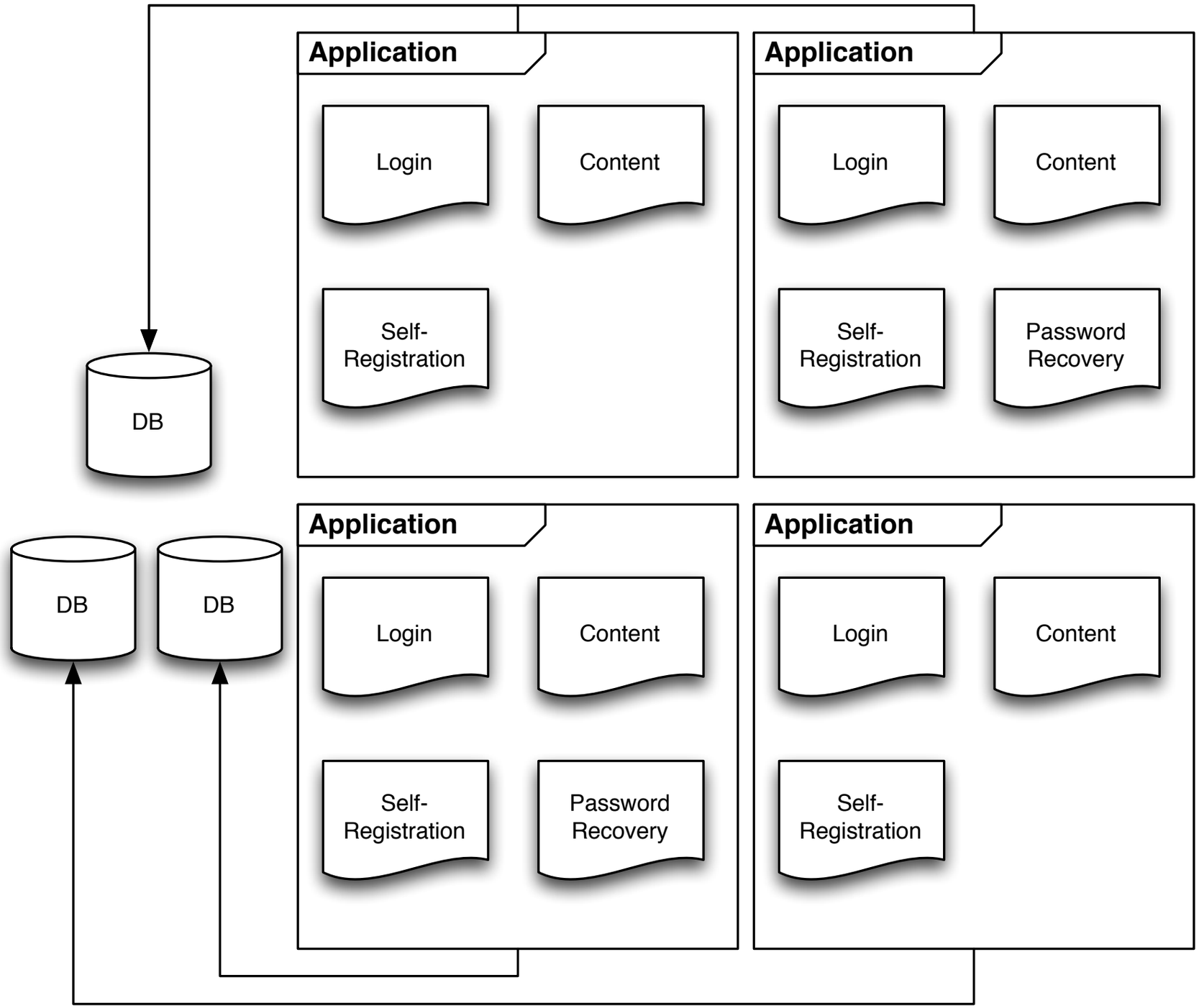
Less Simple App



Uh-Oh



Reality (Simplified)



Supportability Issues

- Multiple accounts
- Different usernames and passwords
- Varying support / recovery processes
- Hard to change Authorization policy
- Provisioning users is error-prone

Security Issues

- Users may retain access to systems
- Duplicated passwords and user info
- Lack of auditing
- Home-grown auth may be insecure
- Difficult to switch to multi-factor

Architectural impact

- Decomposing applications is hard
- Difficult to mash up APIs
  - –Data Silos
- Code for authz policy changes
- Rebuilding same components

Solution?

- Identity and Access Management
  - –Infrastructure shared by apps
  - –Centralized resources and management

- Examples:
  - –Use LDAP for account attributes
  - –Create groups representing authorizations rather than departments

Identity and Access Management

- Single Authentication Mechanism

  –Transport: Client X.509, Kerberos

  –Domain cookie w/App Server Plugin

  –Authenticating Proxy in front of apps

Identity and Access Management

- Central Authorization Policy
- Set policy at HTTP resource level
- Responsible for Access Control at resource level

Drawbacks

- Time/TCO to retrofit existing apps
- High cost of infrastructure upgrades
- M&A often be a nightmare
- There are no standards
  –huge amount of vendor lock-in.

Failings

- Not always possible to support

  –COTS software

  –3rd Party / Hosted software

SAML

The **Cloud Identity Security** Leader™

SAML

- Security Assertion Markup Language

- 1.0 in November 2002
- 2.0 in March 2005

"Securely Assert Identity Information"

SAML Roles

- "Identity Provider" (IDP)
  - –provides identity information
- "Service Provider" (SP)
  - –consumes identity information
  - –provides access to services

SAML Pieces

- Assertion
  - –XML document
  - –a signed and/or encrypted
  - –containing identity information

SAML Parts

- Protocol - messages built on assertions
- Binding - sending protocol over the wire
- Profile - combination to accomplish some use case

SAML Web SSO

- Most popular profile is Web Browser Single Sign-On Profile
- Use browser as a communication channel
- Authenticates browser that delivers the message

Bridges Accounts for the different Security Domains

SAML Used by

- Web Browser SSO Profile
- WS-* (as token)
- WS-Federation (as token)
- OAuth 2 (as authentication mechanism)

OpenID

The **Cloud Identity Security** Leader™

OpenID

- Created by Brad Fitzpatrick in 2005
- Came out of blogging space
  - Don’t want to manage accounts just to let people comment on blog posts
- Initially for Lower Assurance
- Dynamically Managed relationships

OpenID

- Your “username” is a URL
- Your login proves ownership
- Your identity/persona is that URL

OpenID - How it works

- Relying Party
  - –Similar role to SP, requests/relies on OpenID
- OpenID Provider
  - –Similar role to IDP, authenticates users

OpenID - How it works

1. User enters OpenID or selects OP at Relying Party*
2. RP figures out appropriate OP
3. Sends browser to OP so the user can prove who they are
4. OP sends authenticated user back to RP

Advantages

- User-Centric Identity
  - –user maintains control
  - –determines who sees what

- Can run infrastructure without coordination

Disadvantages

- Users do not understand URLs
- Hidden complexity in implementing
- Interoperability is poor
- Many sites are non-compliant
- Some sites require extensions

Recommendation

- Support specific partners/software
- Choose a mature product or library
- Hide OpenID from user
  - Use a NASCAR page

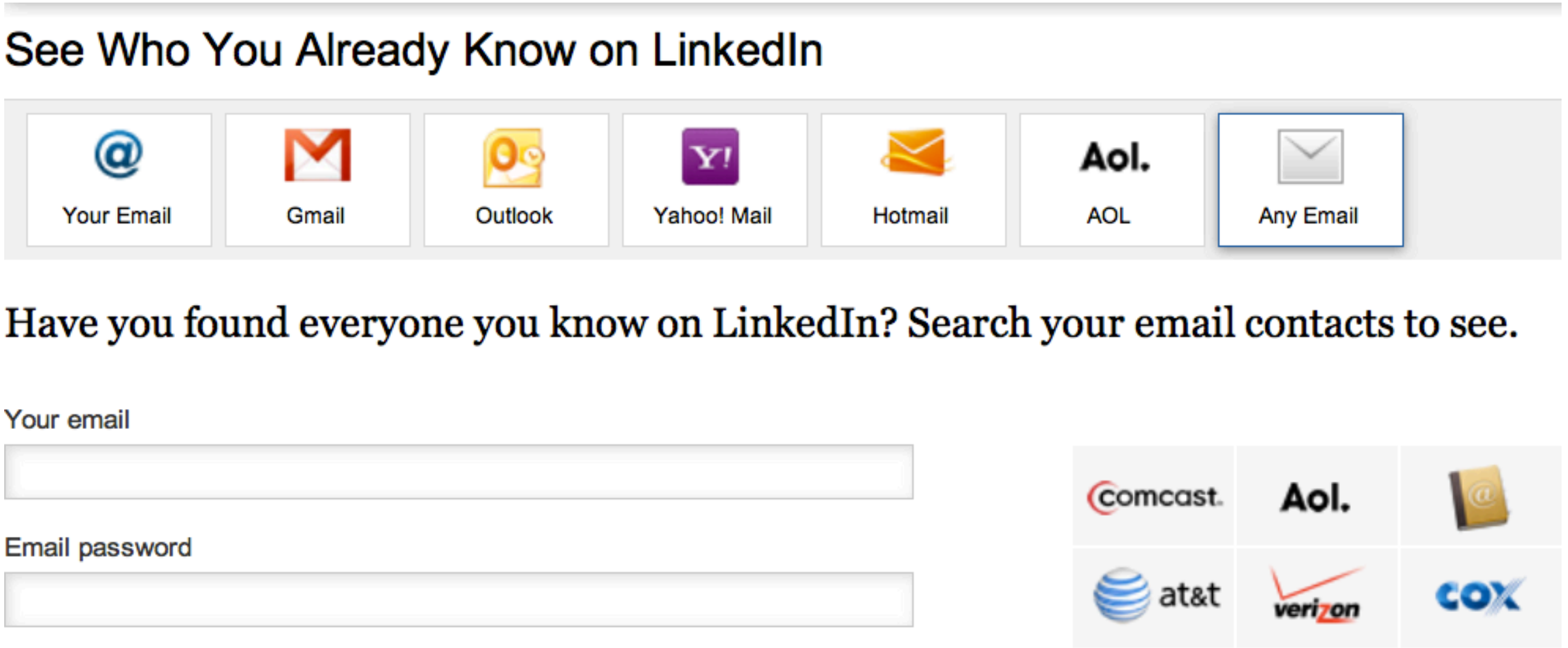
OAuth 1 and 2

The **Cloud Identity Security** Leader™

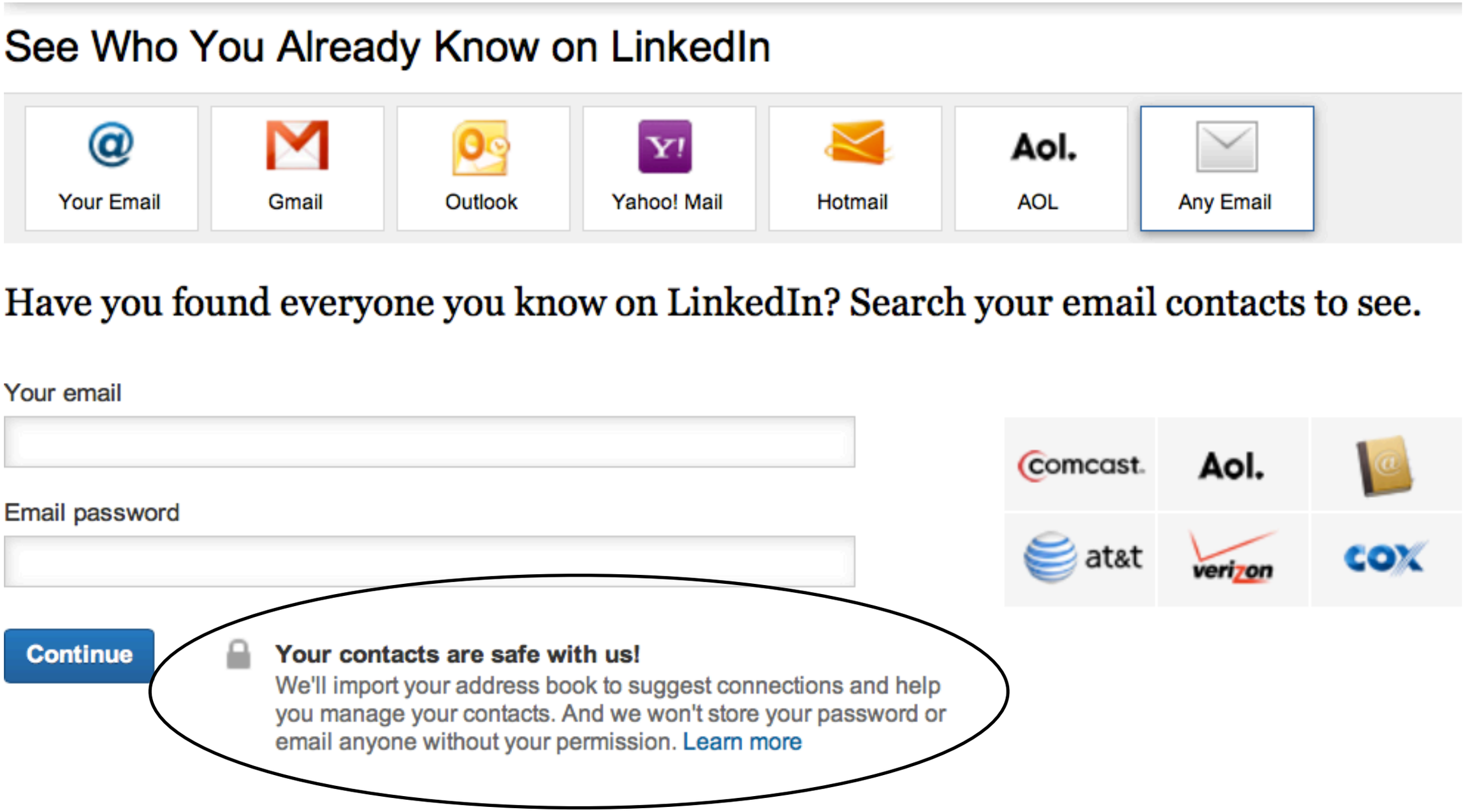
OAuth

- Negotiate/Represent Authorization for Apps
- Per-user
  - –Delegation of user access
  - –User participation in authorization policy

The Old Model*



The Old Model*



OAuth 1

- Created in 2007
- 2-legged
  - –Server to Server
- 3-legged
  - –User authorization

OAuth 1 Flow

- User selects to add/authorize third party
- App sends user to third party site
- User authenticates with site if needed, indicates what the app is authorized for
- User is sent back to App with token

OAuth Benefits

- App access is limited
- App behaviors are auditable
- User makes their own policy decisions
- Users can revoke access to their data

OAuth 2

- Removes complex signature requirement
  - –Must use SSL
  - –Resource access is simple
- Separate roles for resource protected, authorization service
- Adds new flows for new native client use

OAuth 1 vs 2

- OAuth 1 is very pragmatic
  - Hits two use cases
  - Details them thoroughly with examples
- OAuth 2 is broad, extensible
  - Pieces used to solve particular problem
- Do not recommend OAuth 1 for new projects

OAuth vs Web SSO

OAuth is for authorization, not authentication

- Web SSO lets you know who the user is
- OAuth is permission to act for the user
- NOT a replacement for Web SSO

OAuth vs Web SSO

- OAuth does not give you
  - –User attributes
  - –Confirmation (that the user is present)
  - –Audience (this token was meant for you)

OpenID Connect

The **Cloud Identity Security** Leader™

OpenID Connect

- In-process specification building on top of OAuth 2
- Adds first-class identity information to protocol
- Supports additional use cases
  - (hybrid client)

OpenID Connect

- New “ID Token”
- Normal Access token is for the resource, about the client application
- ID token is meant to be understood by the client, about the user

OpenID Connect

- Defines UserInfo service
  - –To get user attributes in a standard manner
- Has Simple discovery mechanism to authenticate by URL or email address
- Defines dynamic client support

OpenID Connect

OpenID Connect provides a single way to securely support both Web SSO, and API access by native clients.

Closing

The **Cloud Identity Security** Leader™

Closing

- Digital Identity is a broad topic representing the user authentication, attributes, and authorization policies for a domain
- Applications should not be their own security domains
  - –does not scale

Closing

- Web SSO is a way to bridge the gap in security domains
  - –SAML - Security Assertion Markup Language
  - –OpenID

Closing

- For native clients, the browser flow of Web SSO is not appropriate
- SOAP services have WS-*
  - –supports SAML tokens
- REST services have OAuth
  - –supports SAML tokens

Closing

- Going forward, OpenID Connect bridges Web SSO and API access.
- Supports authentication and authorization
- Previous protocols will stay in use

Questions?

- Ask me about:
  - –WS-Federation
  - –WS-Security/WS-Trust
  - –SCIM
  - –ID-FF/Shibboleth

http://www.flickr.com/photos/horiavarlan/4273168957/

Questions?

- Visit www.pingidentity.com or www.pingone.com for more information
- Email sales@pingidentity.com with questions

Are you a SaaS company interested in getting started with PingOne for free?

Contact us at sales@pingidentity.com to learn how!