Short Thoughts on Clouds, Security, and Privacy: Colliding Mindsets, Depopulated Buildings

John Linn, Sr. Technologist

Office of the CTO, RSA, The Security Division of EMC

MIT Kerberos Conference, October 2010

The Data is Leaving The Building

- Clouds facilitate new storage and processing paradigms
- Trend: Data is mobile across physical and virtual boundaries
  - Need controls based on objects, not locations or perimeters
  - Will subscribers trust providers, or actively protect against them? How to “trust but verify”?
- Trend: Data is moving outside “home” IT control, maybe into other IT control
  - How is inter-authority trust managed?
- Two mindsets:
  - If it’s important, we’ll lock it up
  - If it’s important, we need to get to it whenever and wherever it’s useful

The Users are Leaving The Building

- Clouds facilitate new modes of distributed interaction
- Mobile users need secure interactions with remote peers, increasingly without in-person introduction
- Trend: Users share their identities and computing infrastructures into enterprises
  - Crossovers between personal and professional roles
  - Limited central technology control
- Trend: Users learn from consumer environments, seek to apply lessons in organizations
- Two mindsets:
  - Work in the office as you're supported and told
  - Work as you find most comfortable, convenient, and effective

Who Controls Identities?

- Administratively-directed and user-centric identity management methods diverge, may define different clouds
- Where will users be authenticated? With what methods?
- How broadly will federated identity consumption grow?
- How will privacy controls be managed?
- Two mindsets:
  - “We decide what you need”: administrators dictate what attributes are maintained, how they are established, and how they can be shared
  - “You determine your persona”: users control their identities, what’s associated with them, and where they are applied

The Building is Leaving The Building

- Cloud services can threaten relevance of existing data centers
  - Individual and corporate users gain new provider choices
- Need trust anchors for dynamic, distributed environment
  - Did someone say “keys”?
- Two mindsets:
  - Established enterprises maintain data centers, but may migrate towards cloud services particularly for cost reasons
  - New enterprises start as cloud consumers, seeking cloud capabilities and avoiding need to build and operate IT infrastructure

Constructing Castles in the Clouds

- Cloud services can offer efficiency, economies of scale, and enable new usage paradigms
- Infrastructure and protocol methods can provide critical security capabilities
  - To build securely in clouds, need solid architecture
- Trust relationships must be established and managed
  - And, also, verified or abstracted

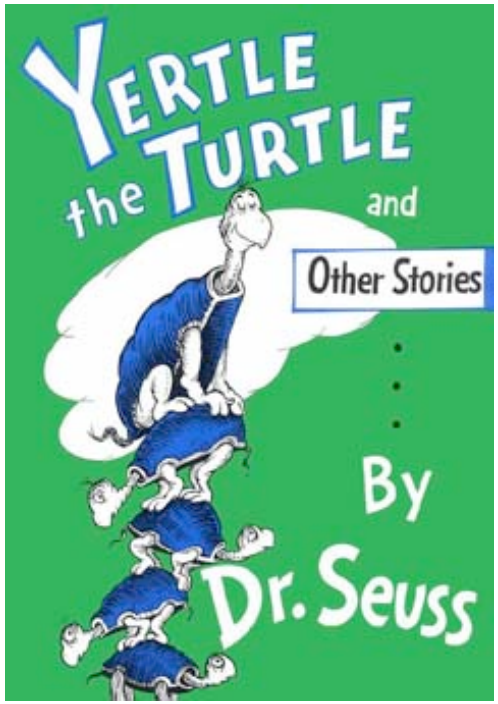
Thoughts on Cloud Security: Turtles All The Way Down

Ned Smith
Principal Engineer, Intel Business Client Platform Group
MIT Kerberos Conference, October 2010

Turtle Analogy

- A turtle shell is a metaphor for security by hardening around the perimeter
  - Security is "Outside-In"

- "Turtles all the way down" adjusts the metaphor so security hardening is applied at every layer
  - Security is "Inside-Out"



Outside-in Security

- Firewalls
  - Hard crunchy outside / soft chewy inside
- VPNs
  - "Private" in VPN implies the network is closed
- Anti-virus checking
  - Add-on "utilities" for hardening software
- Corporate directory services
  - Central user identity management
  - Centralized policy
  - Change control boards

Inside-out Security

- Hardening
  - TPMs, HSMs, tokens and smartcards – FIPS140 and Common Criteria
  - Buffer overflow protection in hardware
  - Cryptographic side-channel prevention
- Isolated environments
  - Roots of trust
    - TCG: RTR, RTS, RTM
    - Intel® TXT: Dynamic RTM
  - Virtual machines
  - Embedded processors
- Attestation
  - NAC
  - Service discovery

Cloud Usage Model Motivates "Turtles all the way down"

- Multi-tenancy
  - Multiple mutually suspicious subscribers co-located on server
  - Multiple mutually suspicious service providers co-located on client
- Endpoint granularity
  - VM, TPM, embedded controllers, browser …
  - Site redirection, load balancers, mesh
  - Device to device
- Strong authentication
  - Subscribers not vetted by in-person interviews
  - Service providers not identified by brick & mortar locations

Security and the Cloud

Dr. Clifford Neuman, Director
USC Center for Computer Systems Security
Information Sciences Institute
University of Southern California
http://clifford.neuman.name

USC Viterbi
School of Engineering

UNIVERSITY OF SOUTHERN CALIFORNIA
INFORMATION SCIENCES INSTITUTE

2010 Kerberos Conference

MIT / Cambridge MA

26 October 2010

Understanding Cloud Security

The cloud is many things to many people

- Software as a service and hosted applications, processing as a utility, storage as a utility, remotely hosted servers, or anything beyond the network card

But above all else the could is

- Federation ... and that means

Something needs to decide how to apply policies to outsiders

- A third party ... trusted by the resource owner
- Placed in the protocol flow right where we find a KDC
- Based on existing authentication (cross-realm or PK) and augmented with a meta-policy database.
- Only part of the problem – still need to apply client side policy

Ping Identity®

Thoughts on Cloud Identity

MIT Kerberos Conference

October 2010

Patrick Harding

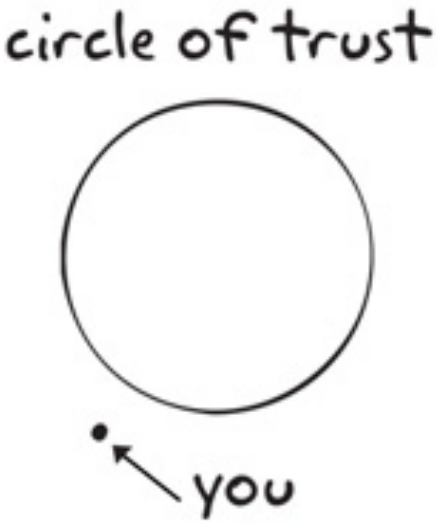
CTO

DESPAIR.COM

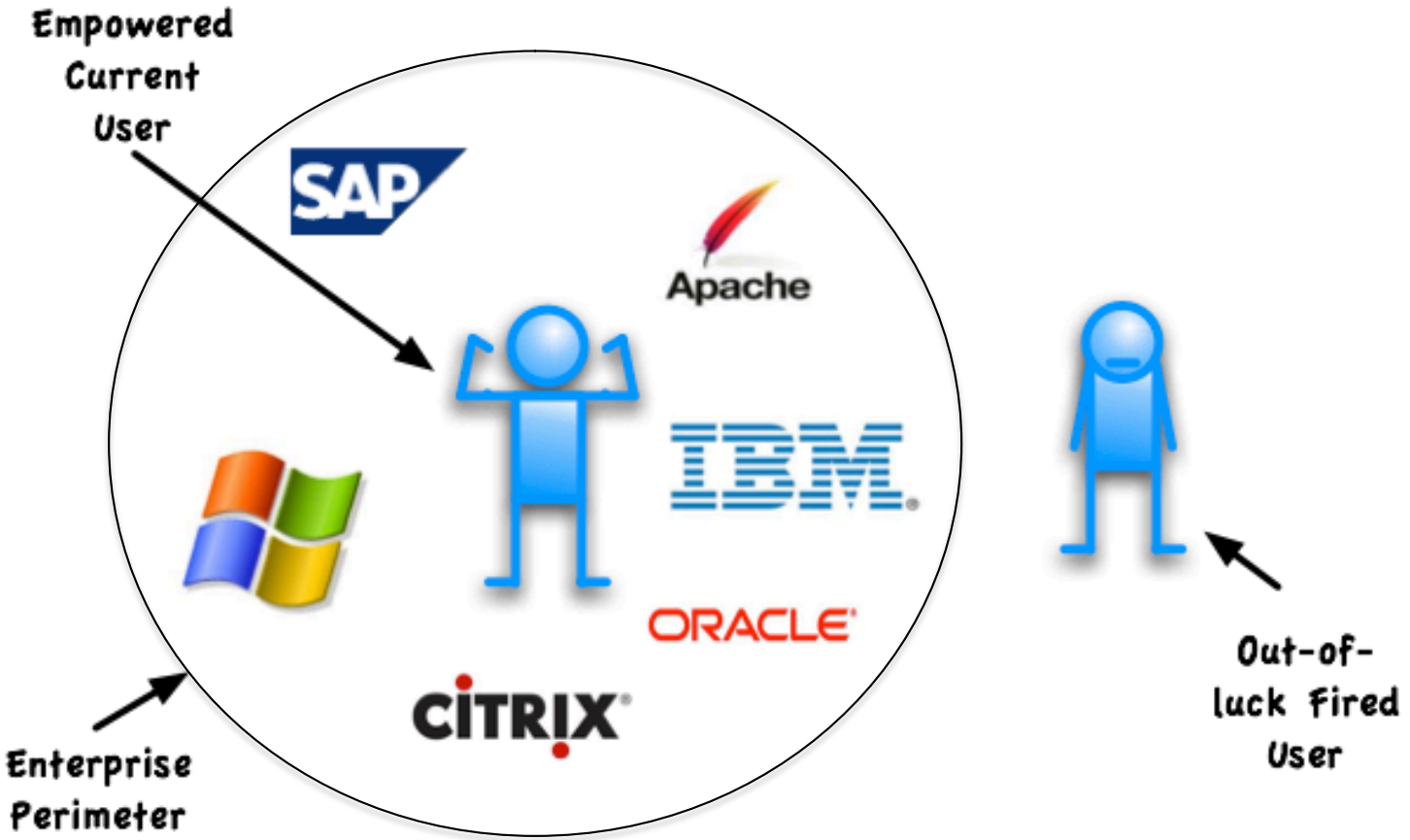
VISION

How Can the Future Be So Hard to Predict
When All Of My Worst Fears Keep Coming True?

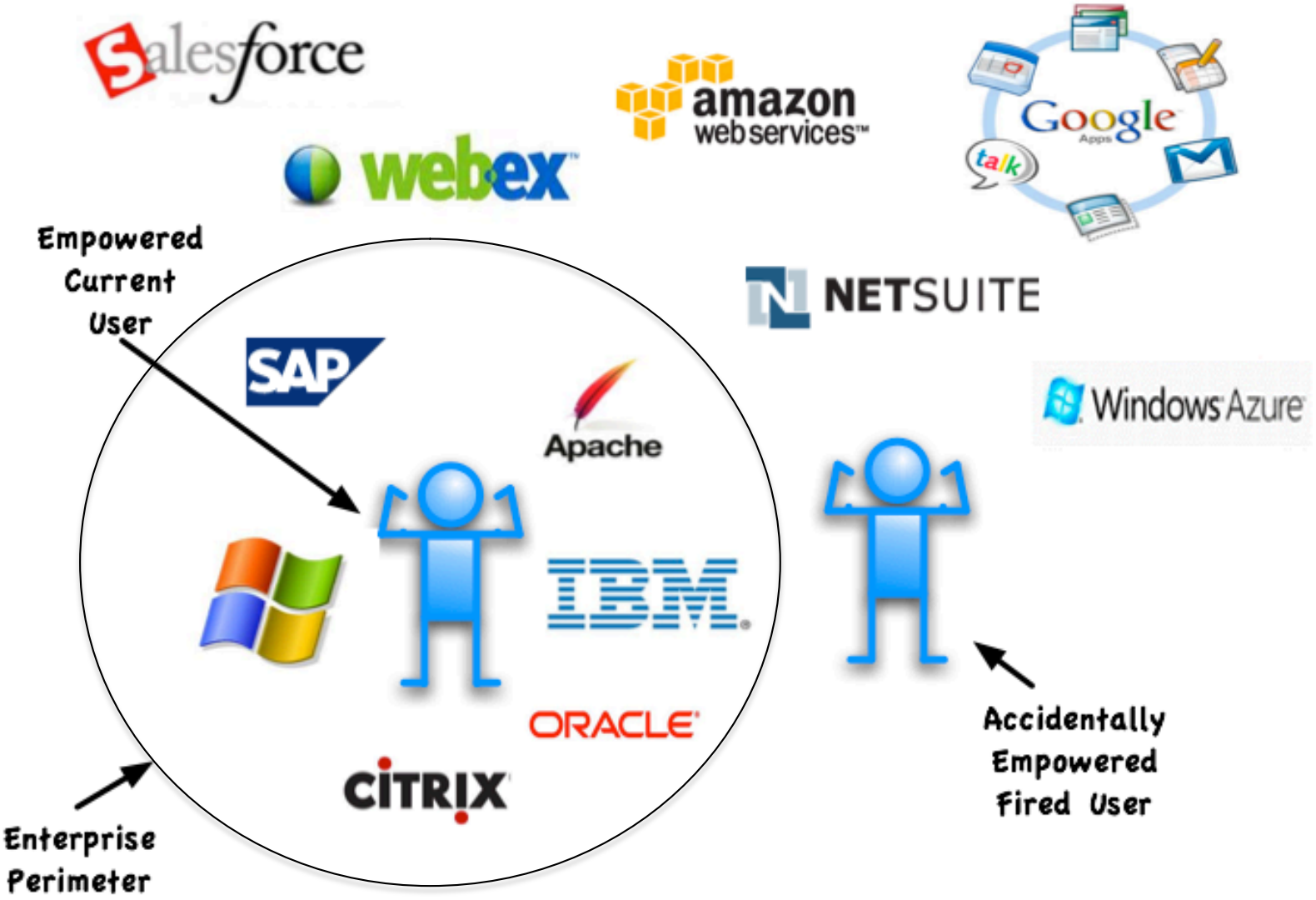
DeNiro Said it Best



The circle had a safety valve



Cloud kills the safety valve



Cloud Security requires a Trust Model

- **A distributed environment demands explicit security over implicit security**
  - Passwords have no explicit security, all you can do is imply context circumstantially
- **Security tokens (e.g. SAML) have explicit statements about scope, validity, integrity and context that have forensic and legal weight**

Theory of Cloud Identity

Ping Identity

Replace multiple weak relationships between user and cloud …

Salesforce

webex

amazon web services™

Windows Azure

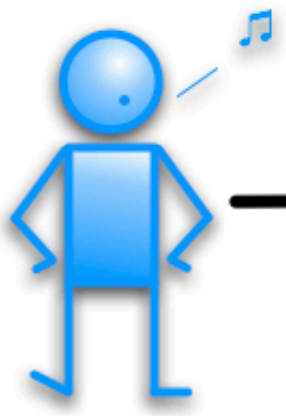
CITRIX

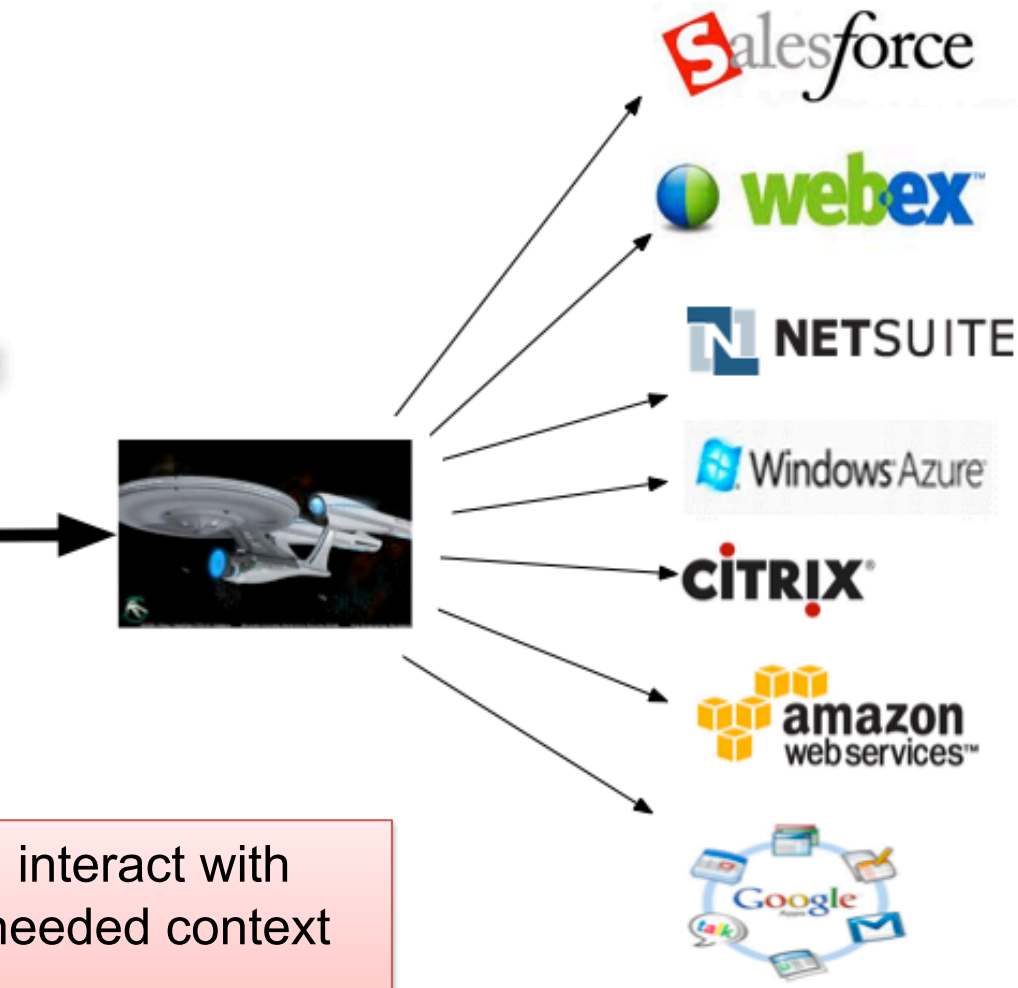
Google

NETSUITE

Theory of Cloud Identity

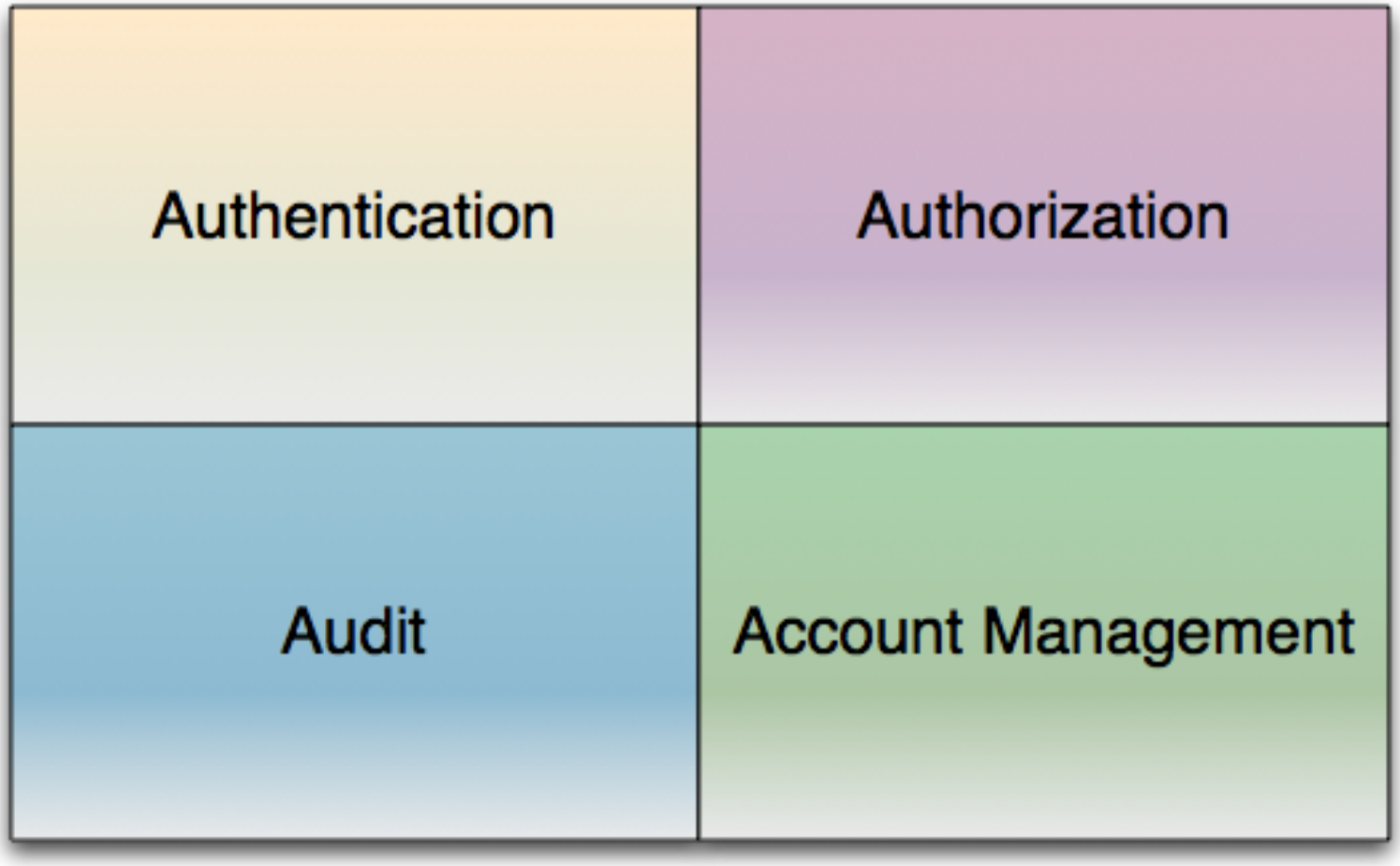
… with a single strong relationship to the Enterprise…



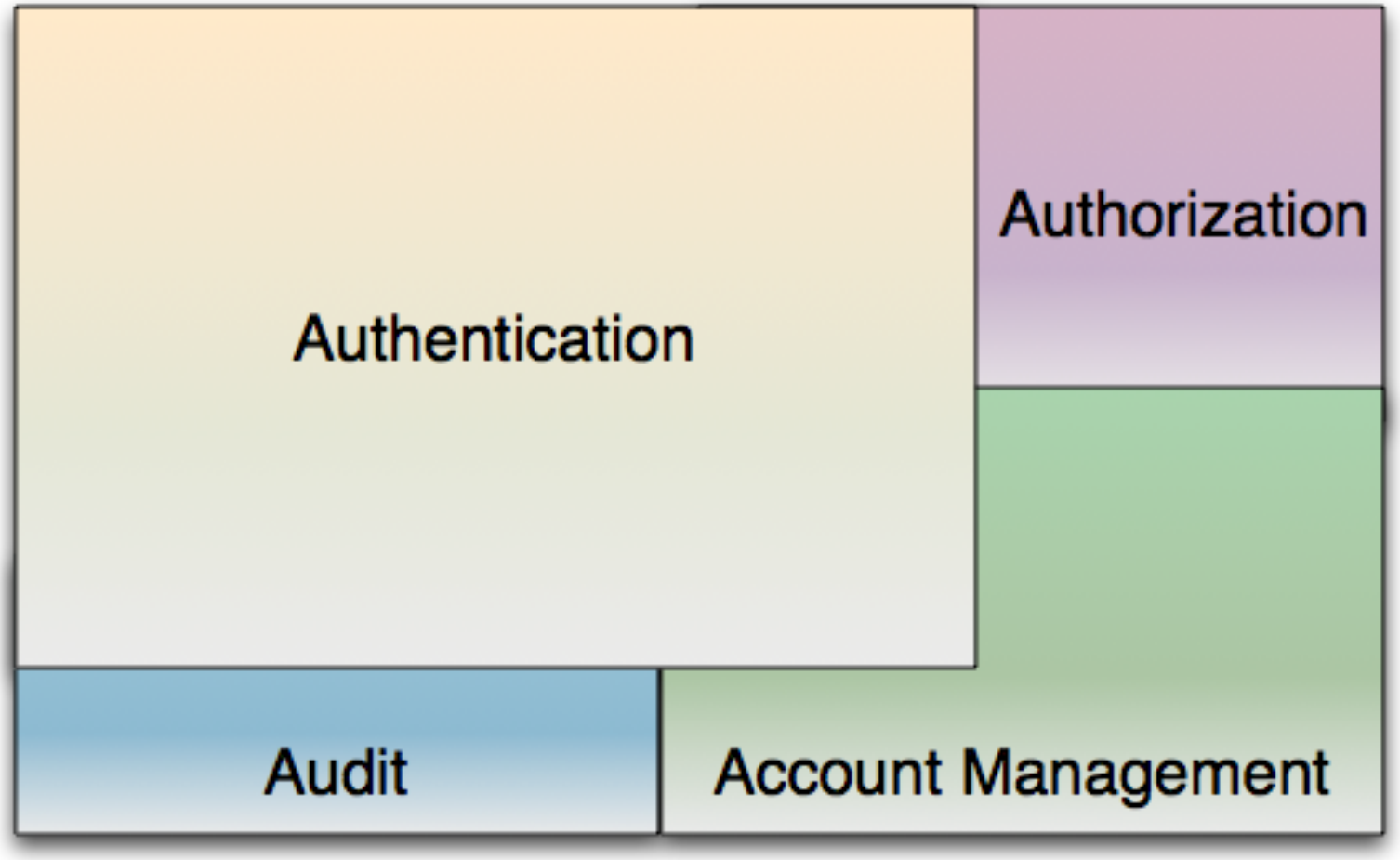


… so that the Enterprise can interact with Cloud Applications with the needed context and control.

Cloud Identity Landscape



Landscape By Maturity



But wait, cloud identity isn't only about Enterprises!

Consumer Identity is Cloud Identity

Imagine this world