Clouds and Identity Management

The Problem Space

- Cloud computing has changed the landscape for the delivery of new services; for example Microsoft Office 365, WorkDay, Google applications, grid computing, ...
- In addition, some campuses and resource providers have begun exploring a shared services model for some applications. Faculty, students, and staff now can make use of Service Providers that live in public and private clouds, or are shared with another institution.
- What lies ahead at the intersection of identity and cloud-based services?

The panel

- Larry Gilreath II, Security Technology Specialist, Microsoft U.S. Education
- Kevin Kampman, Senior Analyst, Burton Group Executive Advisory Program
- Jack Suess, Vice President of Information Technology and Chief Information Officer, UMBC
- Paul Schopis, Chief Technology Officer, OARnet

The Panel Format

- Four brief perspective presentations from the panelists
- A set of round table topics

Discussion Topics – Current

- What are the most important apps driving your interest in the cloud?
    - Is your interest more IaaS, PaaS, or SaaS?
- Is location within the cloud important? Does it affect availability? Are the US Patriot laws a real issue for foreign users?
- Does the difference in cloud internals be reflected in how IdM is linked to the cloud?

Discussion Topics - Future

- How is the cloud evolving?
  - How is IdM in the cloud evolving?
  - What's driving this evolution - technology or demand or something else?
  - Are their standards we should be paying attention to? What to make of the role of "quasi-standards" groups (e.g. IIW) relative to IETF and OASIS and...?
- Should we, as consumers, be working separately to buy an IaaS or PaaS service, and then work with our app provider to live in that cloud, or should we contract with a SaaS provider directly and have them offer the cloud infrastructure as well

Discussion topics – Tricky Stuff

- Are people just federating to a cloud (single org using an outsourced service) or are they federating through a cloud (lots of federated partners sharing data with each other through a cloud)?
  - Does this distinction have implications on security, privacy and IdM?
- What are the gotchas that few folks are talking about?

The Intersection of Cloud Computing and Identity Management

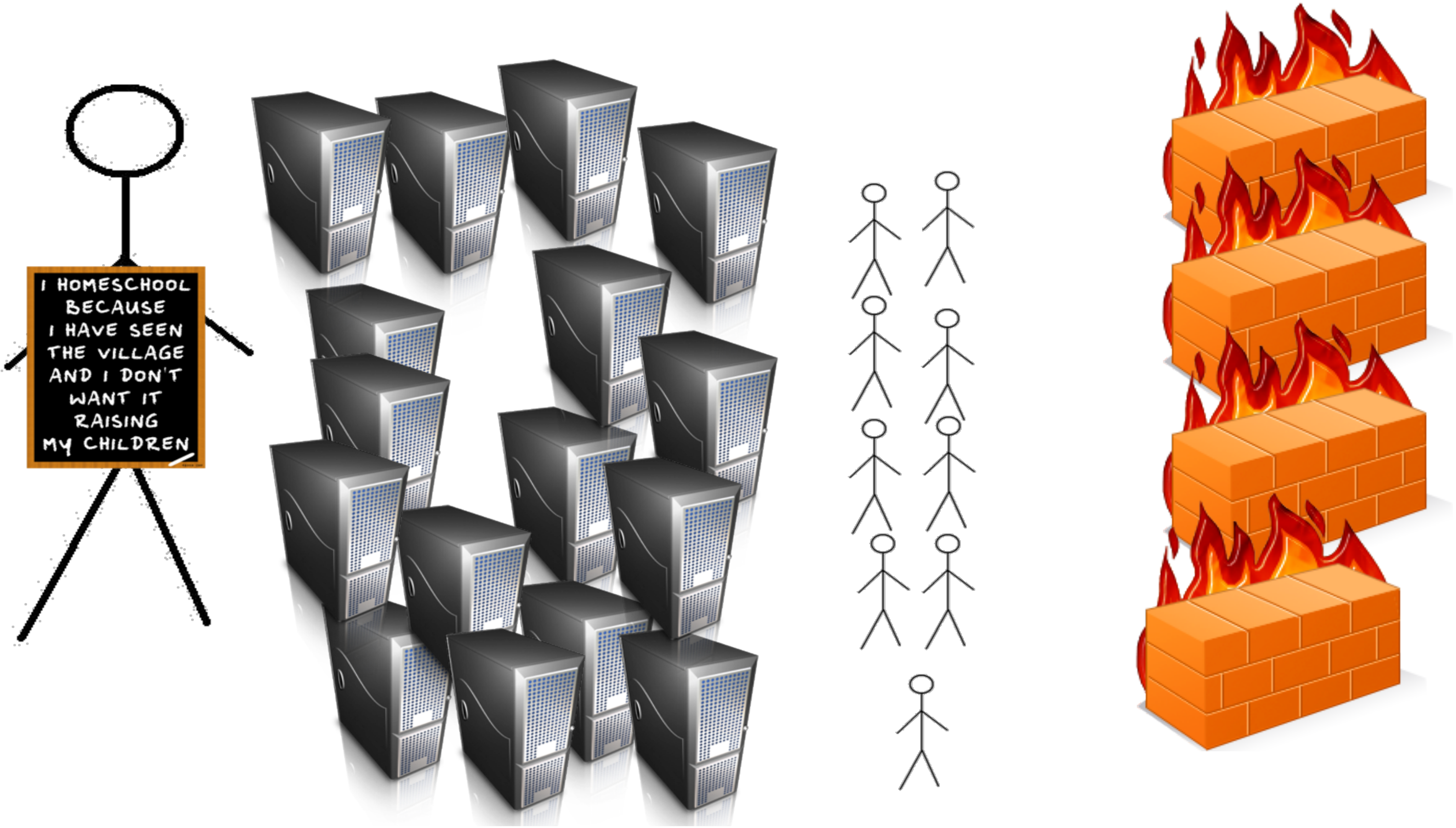
Larry Gilreath II
Security Technology Specialist
E-mail: larrygi@microsoft.com

It Takes a Village …

… Learn from a Specialist

… a community of Specialists

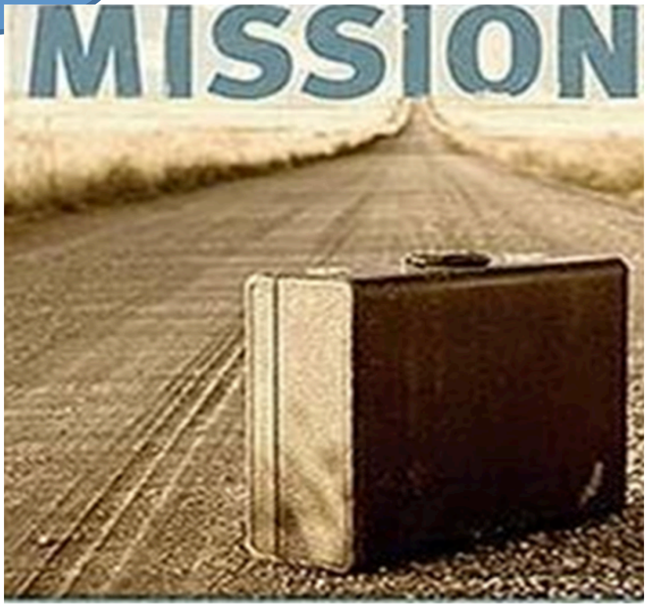
MY specialist!


I HOMESCHOOL BECAUSE I HAVE SEEN THE VILLAGE AND I DON'T WANT IT RAISING MY CHILDREN

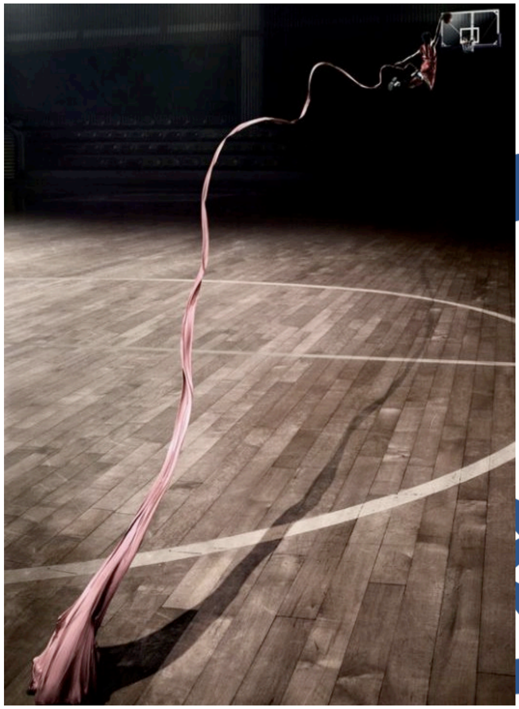
Separated from the “Mission”

When I grow up, I want to spend 7 hours a day patching servers and have nightmares about the second Tuesday or every month!

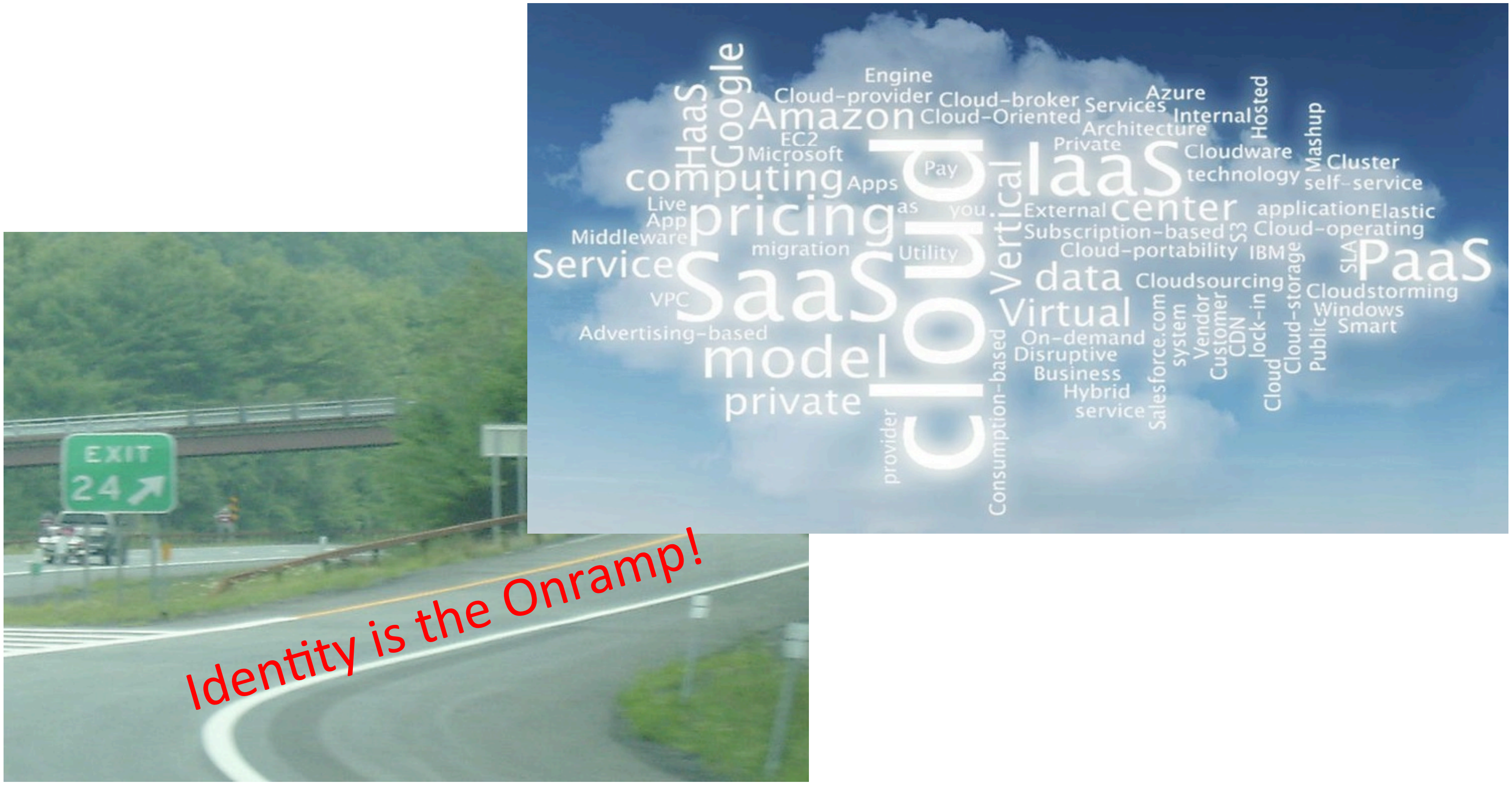
≠



Hosted Cloud Brings …



Your Identity is the Onramp



Identity is the Onramp!

The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.

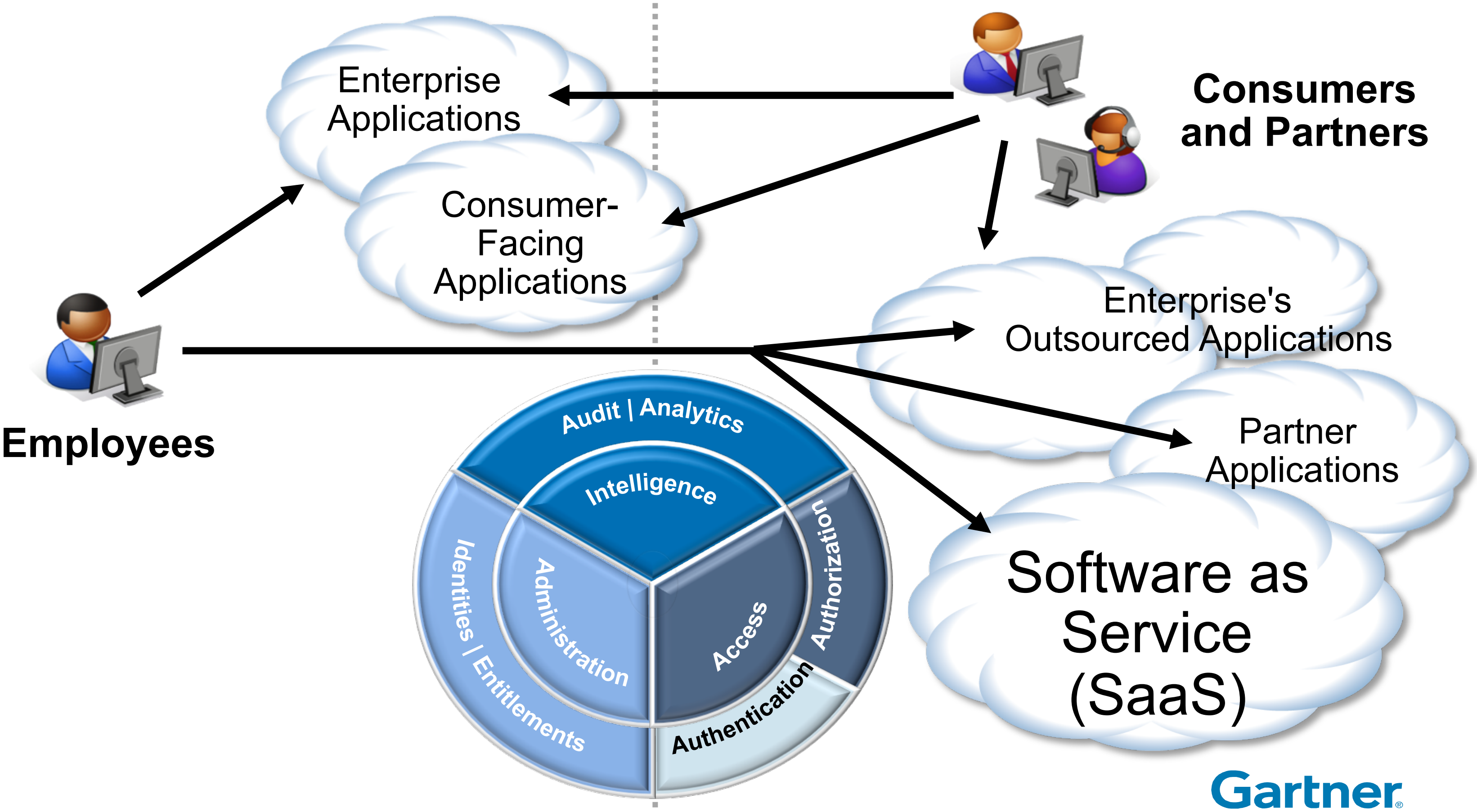
Managing Identity in the Cloud

Kevin Kampman

Research Director

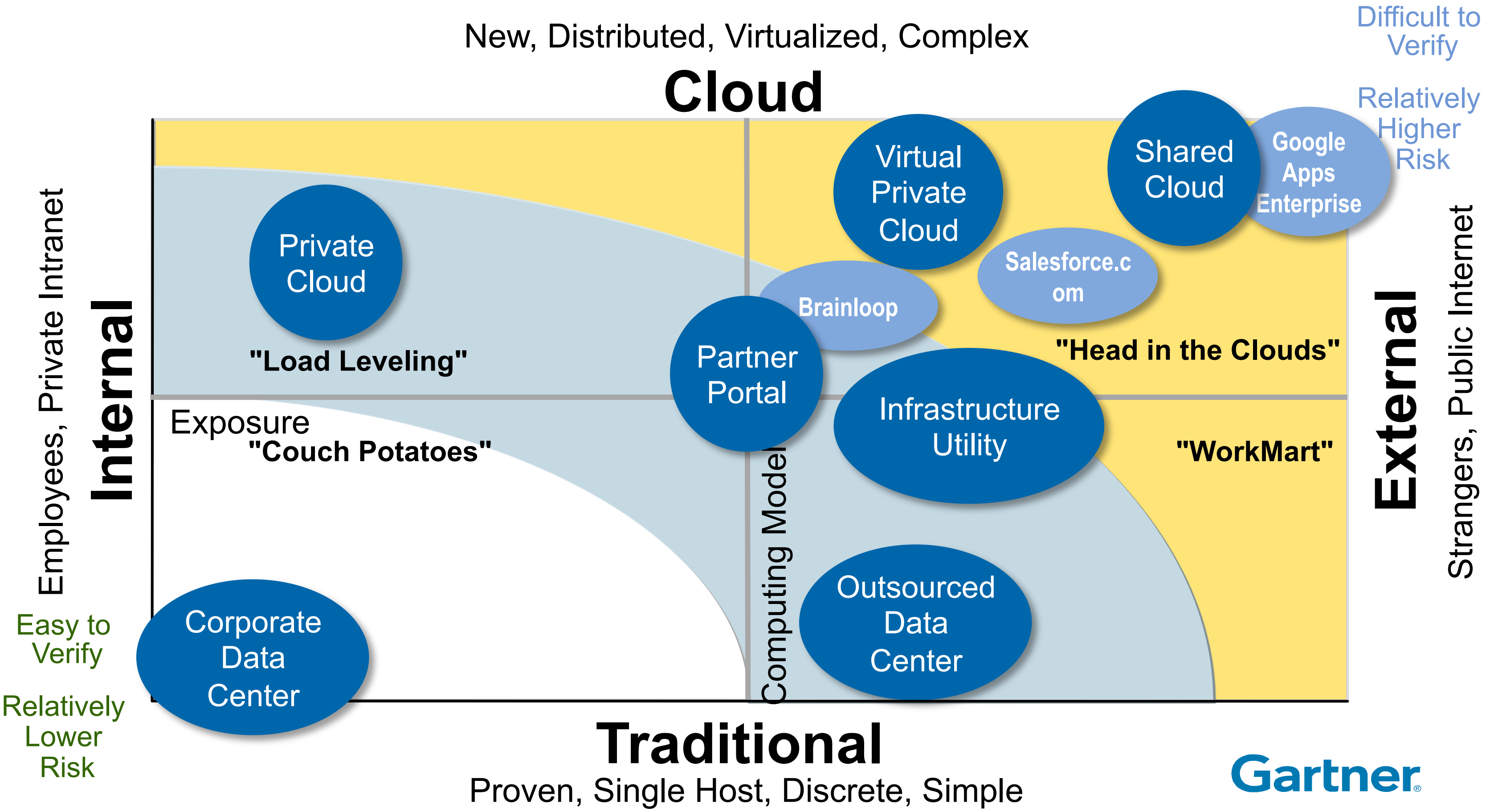
Identity and Privacy

Enterprise IAM Is Being Undone by Cloud Computing



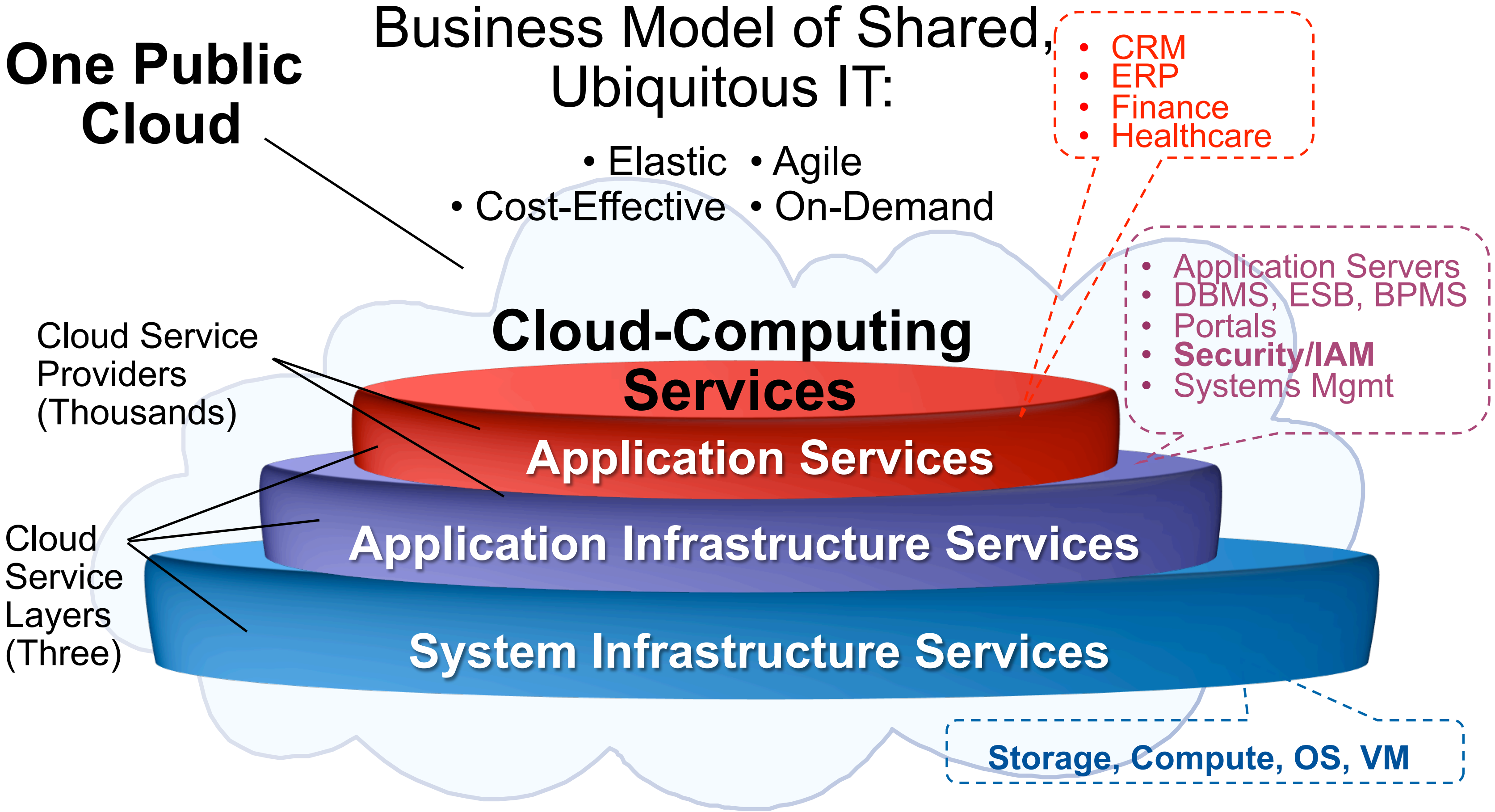
Gartner

Complexity and Exposure Increase Risk



Gartner

Cloud Computing 2014:
Where Does IAM Fit In?



One Public Cloud

Business Model of Shared, Ubiquitous IT:

- Elastic
- Agile
- Cost-Effective
- On-Demand

- CRM
- ERP
- Finance
- Healthcare

Cloud-Computing Services

Cloud Service Providers (Thousands)

Application Services

- Application Servers
- DBMS, ESB, BPMS
- Portals
- **Security/IAM**
- Systems Mgmt

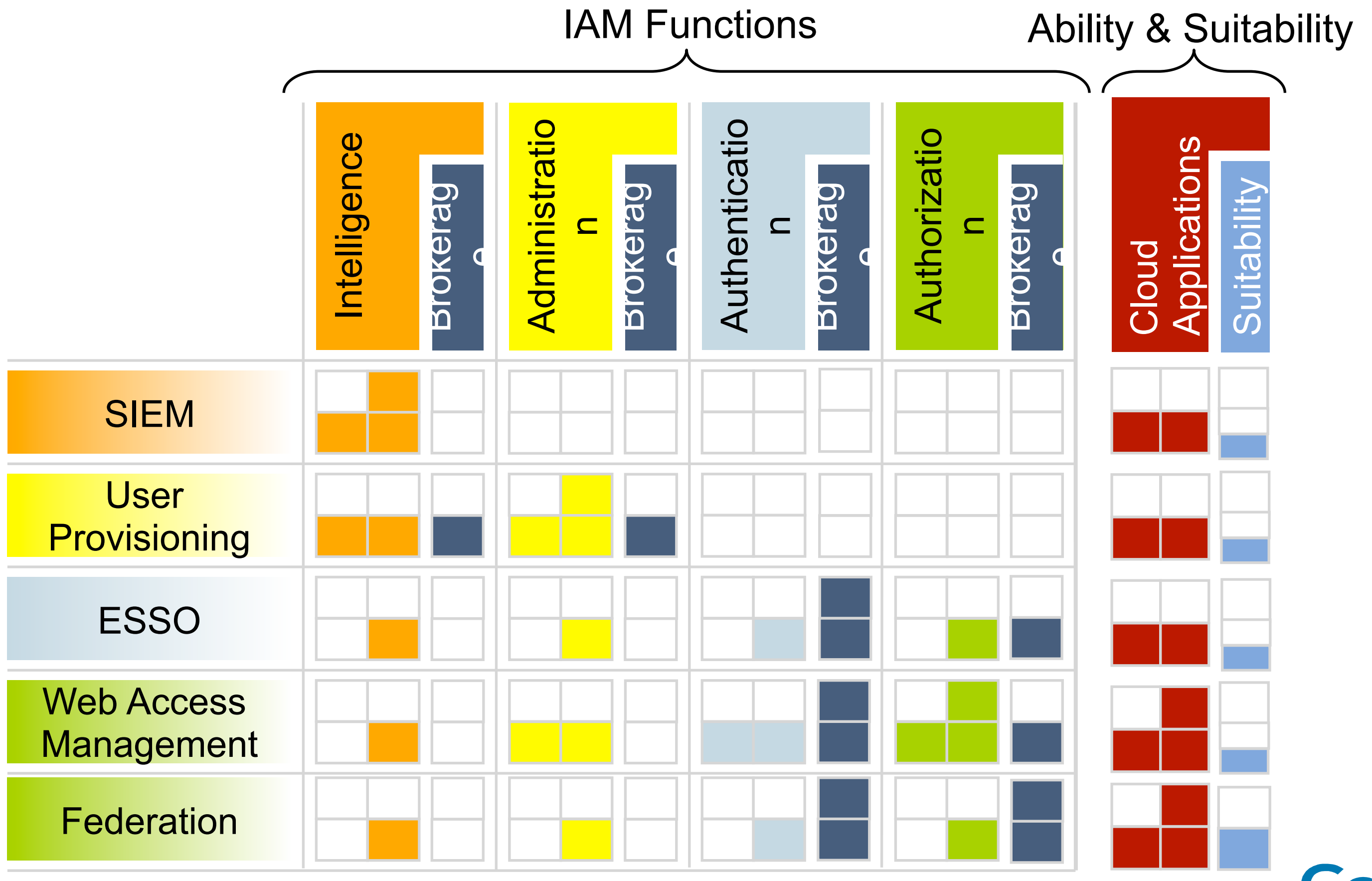
Cloud Service Layers (Three)

Application Infrastructure Services

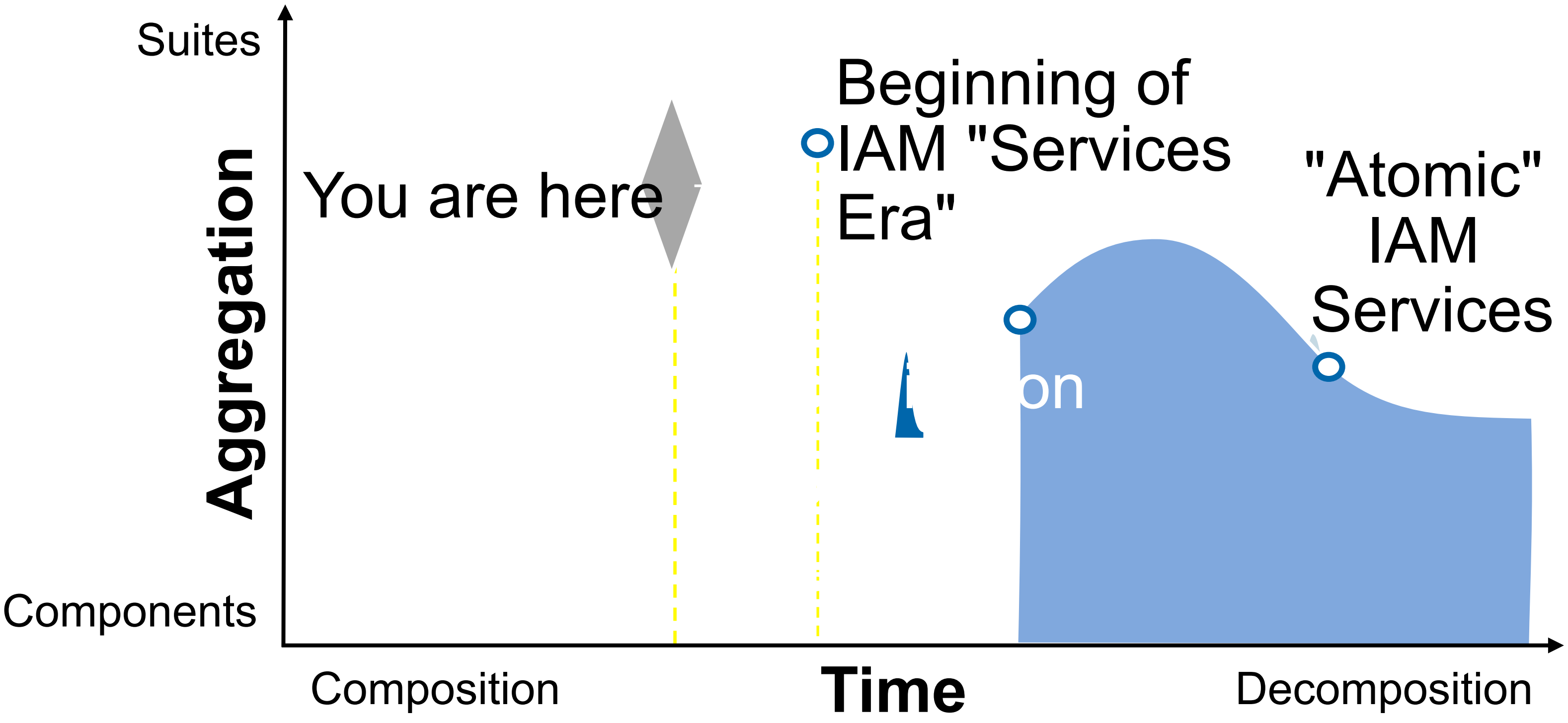
System Infrastructure Services

Storage, Compute, OS, VM

How Capable and Suitable Are Traditional IAM Products for Fulfilling Cloud Requirements



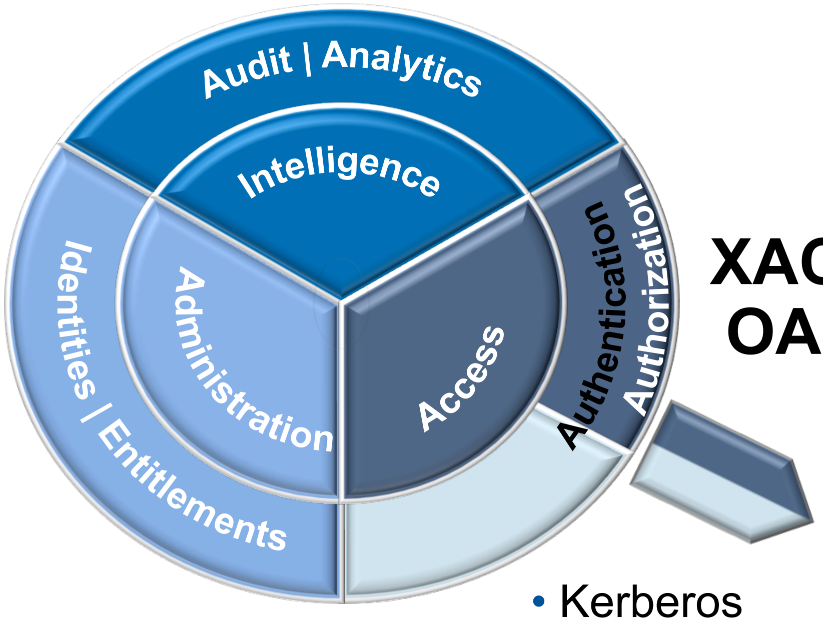
The Messy Deconstruction of IAM and the Birth of IAM Services



"Change is the constant, the signal for rebirth, the egg of the phoenix."
— Christina Baldwin

IAM Standards: A Patchwork With Maturity in Basic Access (Only)

Standard data export formats



SPML

LDAP

XACML

OAuth

Federation:

- SAML
- Liberty
- Shibboleth
- WS-Federation
- OpenID
- ICAM IMI

- Kerberos
- X.509
- OATH
- LDAP

IAM-SOA and Web Services Security Standards Adoption by Enterprises and Vendors

★ Require now

~ Potentially Important

	Enterprise Adoption	Product Integration
OAuth ~	▁	▁
WS-SecurityPolicy	▁	🟨
XACML ★	🟧	🟨🟨
SAML ★	🟧🟧	🟨🟨🟨🟨
WS Security ★	🟧🟧	🟨🟨🟨🟨

	Enterprise Adoption	Product Integration
IMI ~	▁	▁
SPML ★	🟧🟧	🟨🟨🟨🟨
WS-Trust ★	🟧	🟨
WS-Federation ~	🟧	🟨🟨
OpenID ~	🟧	🟨

🟧 Enterprise adoption — estimated percentage of enterprises that are using products that support this standard.

🟨 Product integration — estimated percentage of available products providing security functions that could leverage this standard.

1 square — less than 5%

2 squares — 5-10%

3 squares — 10-25%

4 squares — greater than 25%

Gartner

Key Trends and Considerations

- Cloud security and cloud IAM are tightly coupled
- Hybrid cloud-enterprise models will rule for a *long* time
- Web access management and federation are precursors to cloud services IAM
- Access requirements will be met first — administration will take longer, intelligence — even longer
- The OpenID/OAuth stack has considerable momentum and support
- Don't underestimate the human factor

Recommendation: Develop a Strategy for Safely Leveraging IAM Services

- ✓ Partner with business leaders to include security/ IAM assessments as part of the planning process when procuring cloud-based business application services.
- ✓ Develop contracting and assessment expertise.
  - Including security, compliance and continuity
- ✓ Select and pilot solutions, then implement controls before going operational.
- ✓ Plan for requiring security certifications by cloud applications providers as these certifications mature — likely within 2 years.

Gartner.

Ohio | OARnet

Cloud and IDM
Security & Policy Implecations

Cloud Security
Paul Schopis CTO
OARnet
InCamp
June 23, 2011
Columbus, Ohio

What is Cloud Computing?

Cloud computing is a style of computing using scalability, elasticity and Internet technologies. – *Gartner*

What is Cloud Computing?

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential **characteristics,** three **service models**, and four **deployment models**. - *The NIST Definition of Cloud Computing*

Concerns depend on who you are

- Consumers of a service
  - What is my provider doing to ensure my data is not compromised by someone else?
  - For users of public cloud services what can/must I do to ensure security and data integrity?
- Providers of a service
  - What assurances and services can I provide?
  - How do I know who you are?

Concerns depend on who you are

- For both consumers and providers
  - What is it I’m trying to protect?
  - Does the level of data importance justify the expense?
  - In other words, does my institution/organizations have metrics, methods and policies to map data types on regular basis and assign risk and mitigation strategies etc?
  - Can IDM help me address these concerns?

Question

- Based on the offered definitions what is the most popular cloud solution/device ?

AT&T
9:42 AM
SMS
9
Text
Calendar
Photos
Camera
YouTube
Stocks
Maps
Weather
73°
Clock
Calculator
Notes
Settings
Phone
Mail
Safari
iPod

What's this mean?

- Nothing new really
- Historically technology has moved at a faster pace than security concerns
- BTW the iPhone/iPad iOS does
  - Have key based encryption
  - Ties key generation to the hardware making it uniquely identifiable (banks like that idea)
  - However only Apple's email takes advantage of it and since it decrypts on access anyone with a USB cable can defeat it

What's this mean?

- We now live in a world where consumer devices are used increasingly to access institutional data
- Most institutions do not have policies surrounding use of privately owned smart phones having sensitive data on them
- The old model of tight security around the perimeter is dying
- The notion of only "certified and supported" devices is dead

What's this mean?

- We need to get smart about how to control data
- We need to get smart about how to assign risk
- We need to get smart about how to create decision rights and accountability
- The good news is the "standard" IT governance models address most of these issues
- The bad news is ~80% of organizations have no governance or immature governance

Identity Management

- Make ID management an integral part of data governance
- Become familiar with the standards such as NIST SP 800-63 and OMB M-04-04
- In that context rationalize Level of Assurance (LOA) with access privilege and credentials
- Establishing LOA criteria is a major feature of Identity Federations.

OMB M-04-04

- Defines 4 levels of LOA
  - little or no assurance
  - Some confidence
  - High confidence
  - Very high confidence

NIST SP 800-63

- Maps 4 levels of LOA to required proof
  1. little or no assurance – None i.e. Facebook
  2. Some confidence – Document Presentation
  3. High confidence – Document verification
  4. Very high confidence – Appear in person, two govt' IDs, verified and capture biometric reference

Putting it together

Risk				
Reputation	Low	Mod	Mod	Hi
Financial	Low	Mod	Mod	Hi
Mission		Low	Mod	Hi
Info Disclosure			Mod	Hi
Safety		Low	Low	Mod/Hi
Legal		Low	Mod	Hi
Required LOA	1	2	3	4