Cloud Security and Privacy

Tim Brown
Vice President and Chief Architect Security Management
CA, Inc.

July 2009

Transforming IT Management

Agenda

> The Evolution to Cloud computing

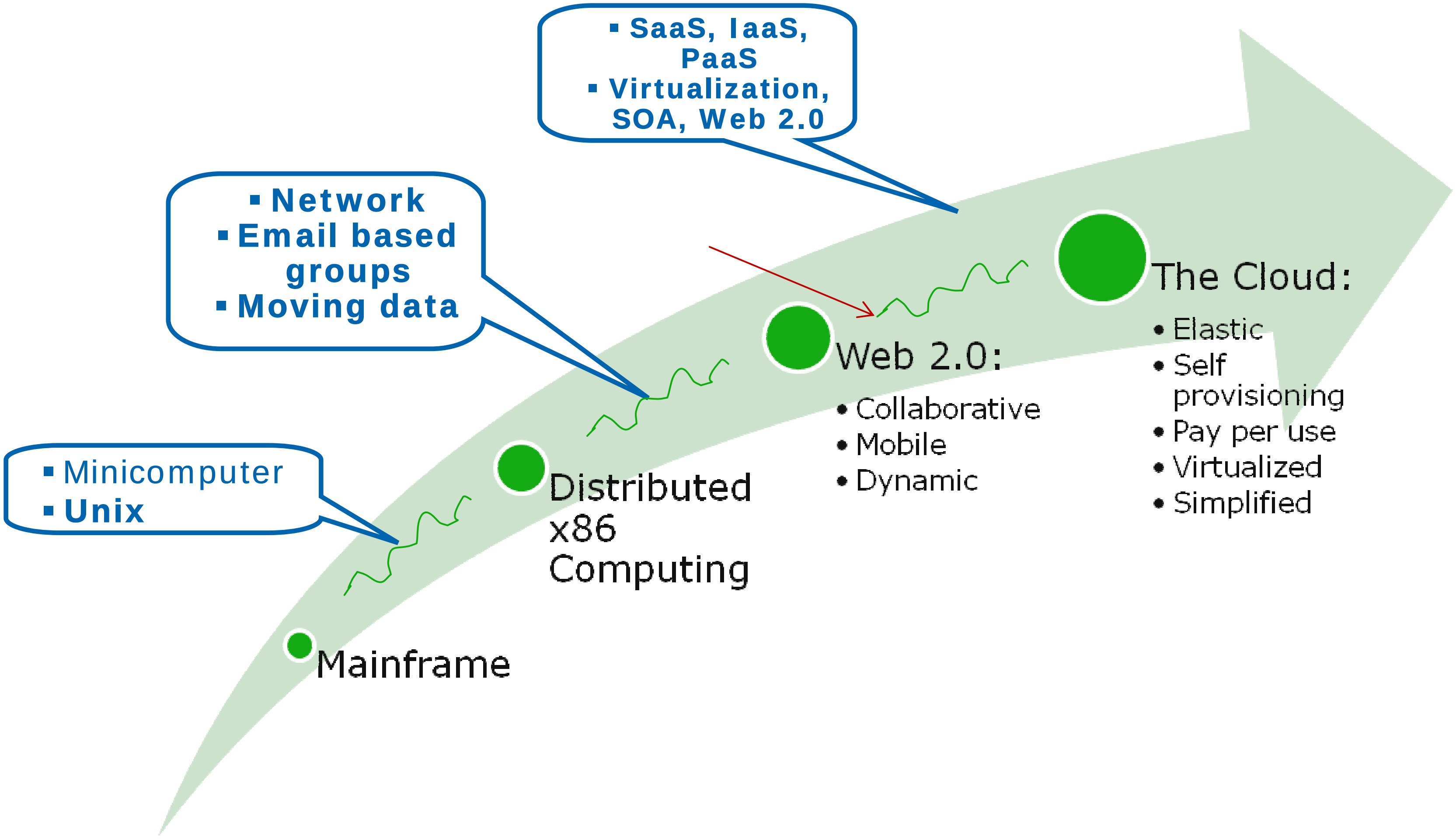
> Opportunities for the Customer and the Vendor

> The cloud Models their benefits and challenges

- Internal
- Private
- Public
- Hybrid

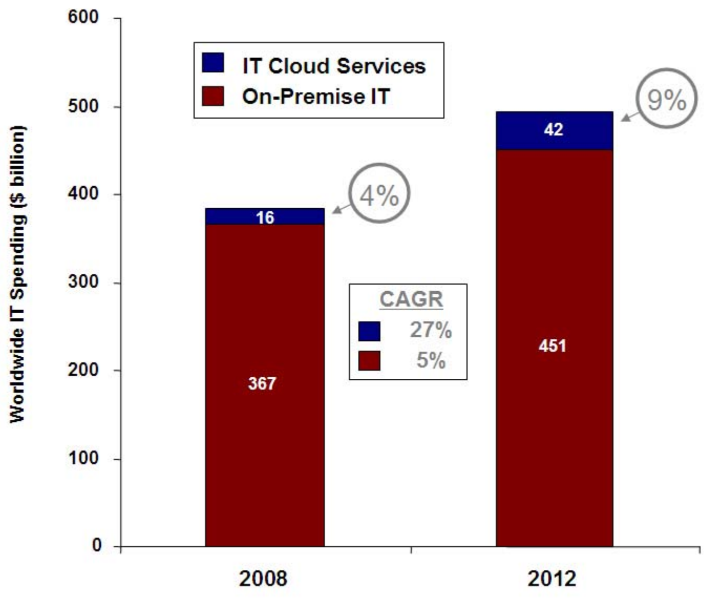
> Conclusion

Our market is undergoing a transition to "Elastic" IT



Cloud Services are expected to be a key driver of new growth

Worldwide IT Spending* by Consumption Model
2008, 2012

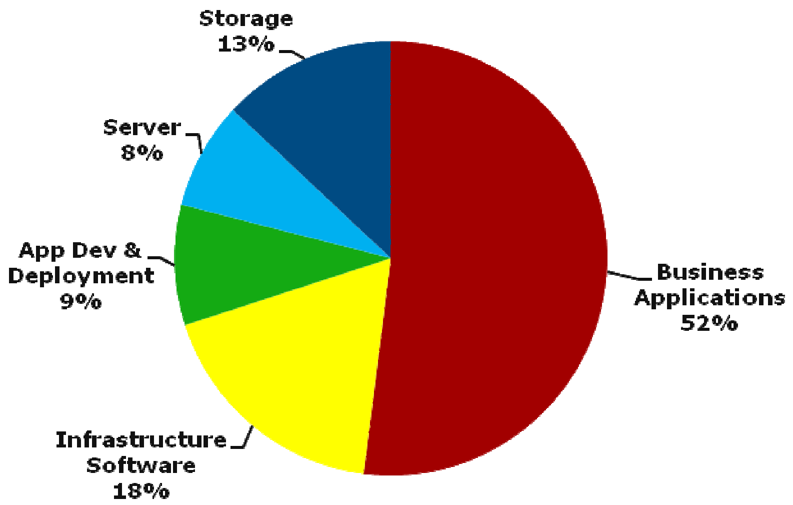


* Includes enterprise IT spending on Business Applications, Systems Infrastructure Software, Application Development & Deployment Software, Servers and Storage

Source: IDC, October 2008

IDC eXchange, IT Cloud Services Forecast - 2008, 2012: A Key Driver of New Growth, http://blogs.idc.com/ie/?p=224, October 8, 2008.

Worldwide IT Cloud Services Spending* by Product/Service Type
2012



$42.3 Billion

*** Includes enterprise IT spending on Business Applications, Systems Infrastructure Software, Application Development & Deployment Software, Servers and Storage**

Source: IDC, October 2008

IDC eXchange, IT Cloud Services Forecast - 2008, 2012: A Key Driver of New Growth, http://blogs.idc.com/ie/?p=224, October 8, 2008.

Why Cloud? What's the Customer Value?

Cost Reduction

- Potentially lower infrastructure (capital) costs
- Potentially lower maintenance and energy costs

Elasticity / Scalability

- Capacity only when you need it
- Ability to handle expected or unexpected changes in load
- Achieve high business agility

Speed to Market

- Reduction of time to pilot and test projects
- Faster availability to customers

High Performance Computing

- Increased capacity from your current physical infrastructure
- Avoid provisioning (and paying) for the peak
- "Infinite" computing capacity on demand

Why Cloud? What's the Vendor Value?

Cost Reduction

- Limited Platform support = Limited testing
- Controlled environment = Higher quality
- Better ROI for customers and Vendors

Elasticity / Scalability

- Repeatable processes allows for maximum use of hardware
- Ability to satisfy the needs of many customers
- Ability to load balance between customers

Speed to Market

- Reduction of time to pilot and test projects
- Faster availability to customers
- Ability to enhance software in iterations

High Performance Computing

- Take advantage of specialized Hardware to reduce costs
- Take advantage of new models (Storage in the cloud) to reduce costs
- Utilize Virtualization to gain performance and scale

The challenging economy is the driver for renewed interest

> The interest level in cloud has increased dramatically in the last 9 months

> Enterprises and Governments are looking at the details to determine myth or reality

> At CA we look at the cloud in 3 Models

- 1) Provide our customers the infrastructure and security necessary to utilize cloud based applications.
  - Extensions to their existing heterogeneous environments
- 2) Provide the service providers with applications that can be hosted in the cloud
- 3) Provide hosted applications (Clarity on Demand)

An Example of Infrastructure as a Service: Amazon Elastic Compute Cloud (Amazon EC2)

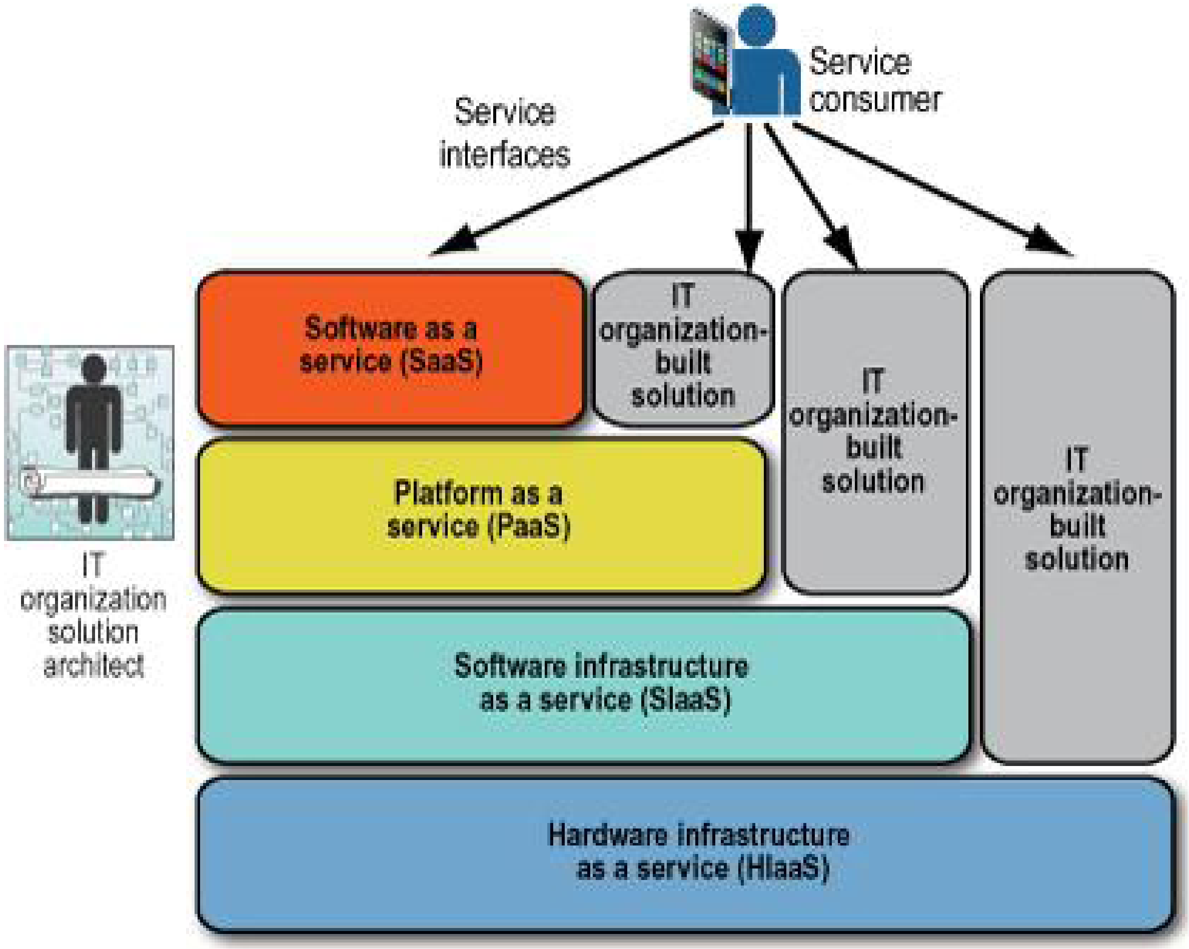
- Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud.
  - Designed to make web-scale computing easier for developers.
- Applications are packaged as “Amazon Machine Instances” (AMI)
- Tightly coupled Storage service (Amazon S3)
- Amazon EC2 web services control the environment
- Infrastructure internally (Amazon) developed

The Surge

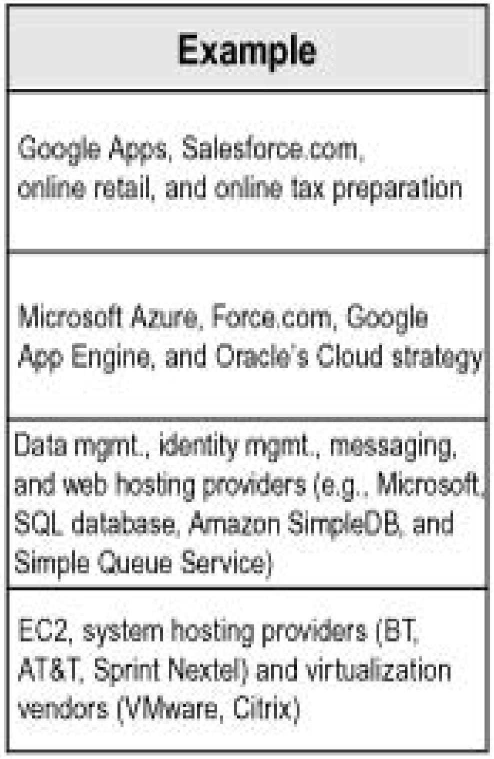
FOR A PREVIEW CLICK HERE

- Early in the Spring they had about 5000 sign up per day
- In mid-April, Facebook users found it and 750,000 people signed up in three days.
- At the peak, almost 25,000 people tried Animoto in a single hour.
- Animoto had worked with RightScale, a cloud services firm in Santa Barbara, Calif., to design their application for Amazon’s cloud.
- During the three-day surge, Animoto did not buy or configure a single new server.
- It added capacity on Amazon, for about 10 cents a server per hour
- When the surge subsided, they shed capacity

Four Forms of Cloud Services



Service consumer
Service interfaces
IT organization solution architect
Software as a service (SaaS)
IT organization-built solution
Platform as a service (PaaS)
IT organization-built solution
Software infrastructure as a service (SIaaS)
IT organization-built solution
Hardware infrastructure as a service (HIaaS)



Example
Google Apps, Salesforce.com, online retail, and online tax preparation
Microsoft Azure, Force.com, Google App Engine, and Oracle's Cloud strategy
Data mgmt., identity mgmt., messaging, and web hosting providers (e.g., Microsoft, SQL database, Amazon SimpleDB, and Simple Queue Service)
EC2, system hosting providers (BT, AT&T, Sprint Nextel) and virtualization vendors (VMware, Citrix)

Source: Burton Group 2009
“Cloud Computing Security in the Enterprise,” July 15, 2009
By Dan Blum

Cloud Computing Models

> Internal Cloud
  - Utilize Cloud infrastructure inside the Enterprise
  - Full organizational control
  - Lower Risk

> Private Cloud
  - Group determines security requirements
  - More organizational control
  - Medium Risk

> Public Cloud
  - High volume limited customization
  - Limited organization control
  - Higher Risk

> Hybrid Model consisting of a combination of models

Security and Privacy Concerns Exist in All Models (Public, Private, Internal)

> Security and Privacy can be implemented in a cloud model but:

- It needs to be cost effective for the customer and vendor
- Need to balance cost and risk
- Managed Security Service is good example

> Changing from an existing model creates risk

> New models need new controls and processes

> Public, Private and Hybrid model can have

- Loss of control
- Loss of visibility
- Data Privacy and Data Sharing
- Inability to achieve Internal and regulatory compliance
- Additional risk of data loss, breach, brand and reputation
- Additional layers which effect Service Level Agreements

Loss of Control Does Not Equal Additional Risk

> In some environments it is easier to mange risk externally
  - Loss of control =
    - More contractual control
    - More SLA control
    - More accountability
    - More security and less Risk

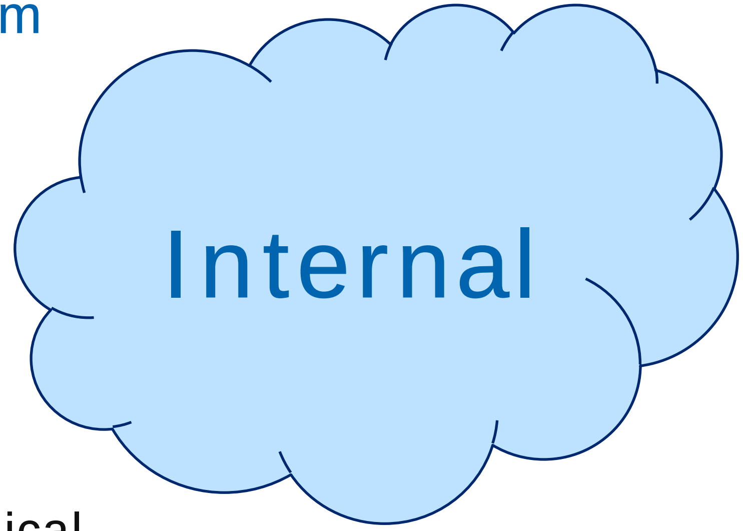
> In other environments loss of control equals greater risk
  - Loss of control =
    - Changes in processes and procedures
    - Changes in applications and data models
    - Changes in visibility

> As Cloud application usage grows technical issues may be overtaken by contractual issues

The Internal Cloud

> Offers new implementation paradigm

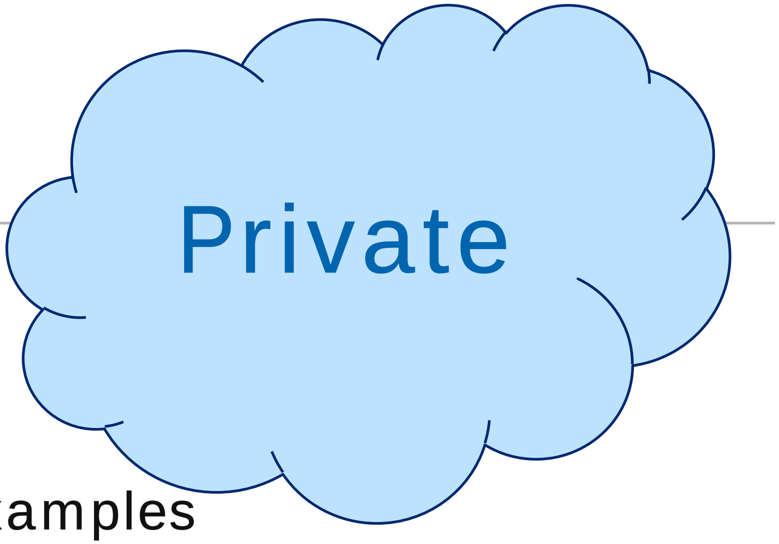
- Highly scalable
- Redundant
- Standards based
- Controlled by the Enterprise



> As you consider internal clouds

- Overall design and planning is critical
- Evaluation of existing applications and their ability to exist in a cloud environment
  - What does muti-tenancy really mean?
- New models even if fully under an Enterprise Control creates new vectors of risk
- Do not take the movement to the cloud lightly

The Private Cloud



- > Cloud applications defined for specialized purpose
  - Covisint, SAFE Biopharma are examples
- > Control of cloud is within the scope of the members
- > Members drive
  - Overall characteristics
  - Risk Tolerance
  - Audit requirements
  - Regulatory requirements
  - Service level agreements

As you consider Private Clouds

> Review the cloud offering carefully. Work with members to define requirements

> Review all applications within the offering

> Do not compromise on your risk tolerance

> Understand the limitations.

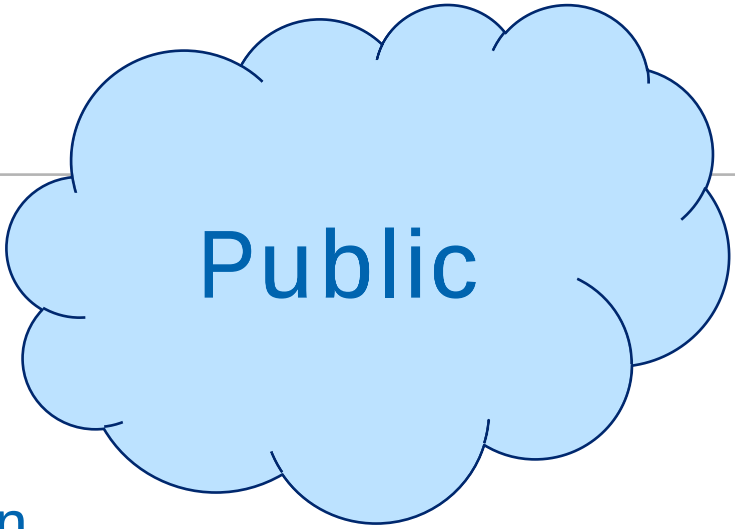
  - Just because the risk level is acceptable in other organizations doesn’t mean it fits yours

> Verify the contracts and also the technology

> If possible utilize your existing identity, access control and auditing systems

> Constantly monitor and test the environment to insure it meets your requirements

The Public Cloud

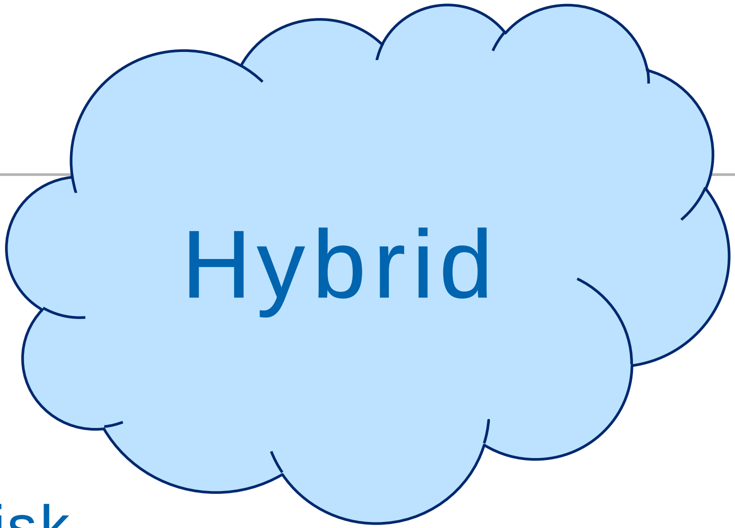


- Public Cloud offerings
  - Salesforce.com
  - Amazon EC2, S3
- High volume – Low customization
- Some applications work very well in this model
- Inability for Vendor to customize can mean that solutions do not fit within a given enterprises risk tolerance
- Data storage and Audit requirements, transparency requirements, data separation requirements, Legal and Regulatory requirements, and contractual obligations

As you consider Public Cloud Applications

- Carefully review the contracts and the technology
- Assess the risk and importance of your data and applications. Public Cloud Applications can not adjust to your needs.
  - Do not compromise on your risk tolerance
- Understand what control and visibility you are giving up
- When possible utilize your existing identity systems, policies and audit mechanisms
- Create programs to regularly test and verify the implementations

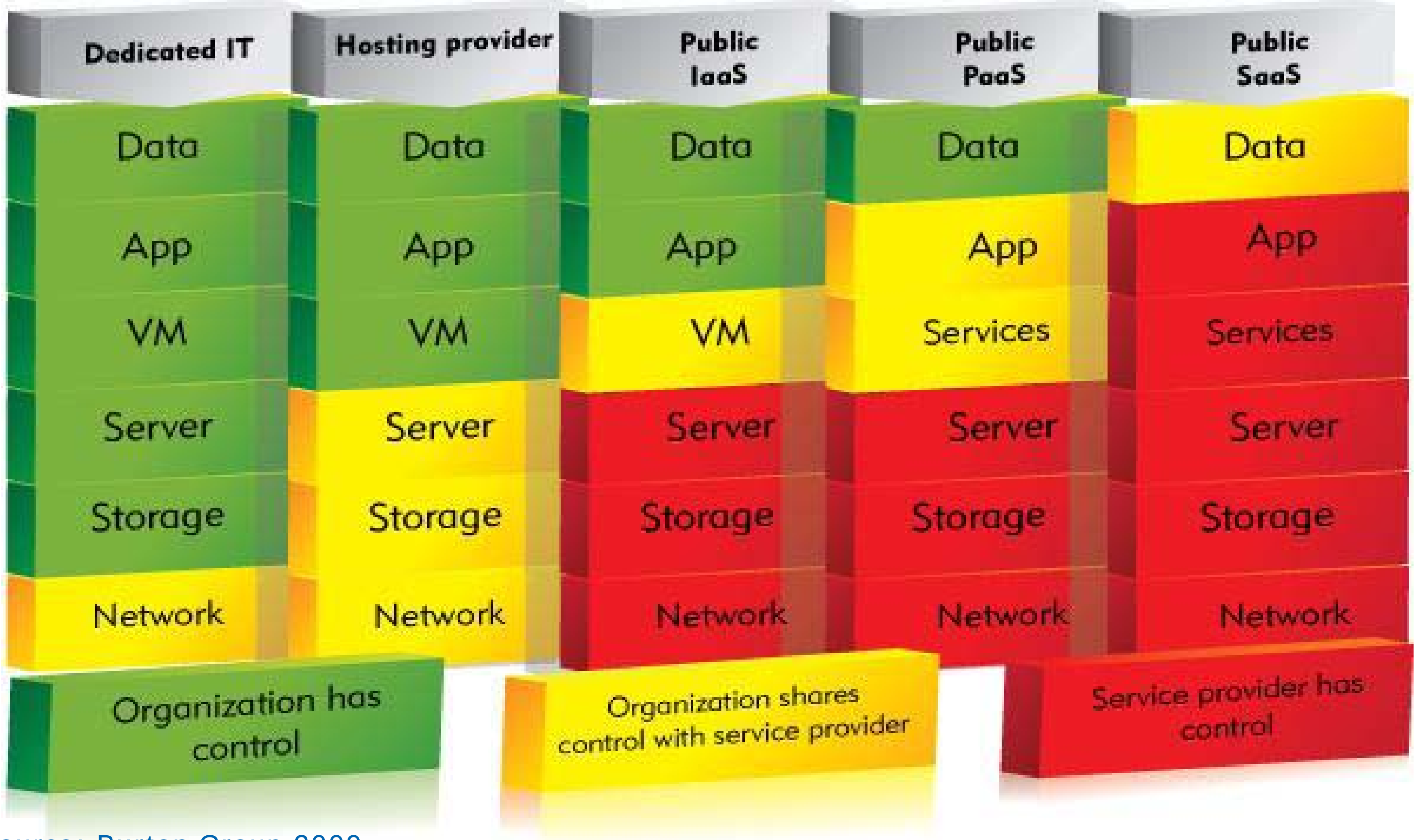
The Hybrid Model



Hybrid

- A combination of Internal, Private and Public Cloud models
- Allows the Enterprise to adjust risk posture for applications and data
- Can be more complicated and require well thought out design and implementation planning
- This model will be the primary model within the Enterprise

Control within the Cloud



Dedicated IT	Hosting provider	Public IaaS	Public PaaS	Public SaaS
🟩 Data	🟩 Data	🟩 Data	🟩 Data	🟨 Data
🟩 App	🟩 App	🟩 App	🟨 App	🟥 App
🟩 VM	🟩 VM	🟨 VM	🟨 Services	🟥 Services
🟩 Server	🟨 Server	🟥 Server	🟥 Server	🟥 Server
🟩 Storage	🟨 Storage	🟥 Storage	🟥 Storage	🟥 Storage
🟨 Network	🟨 Network	🟥 Network	🟥 Network	🟥 Network

🟩 Organization has control

🟨 Organization shares control with service provider

🟥 Service provider has control

Source: Burton Group 2009
“Cloud Computing Security in the Enterprise,” July 15, 2009
By Dan Blum

In Conclusion

- Look for products, technology and processes that work together
- Take a defense in depth approach all members of the cloud play an important role in Security
- Don’t under estimate the role of planning and design. This is a new paradigm with new risks and rewards
- Look at risk and manage appropriately
- After reviewing the contracts and implementing the technology, it is critical to initiate a plan to trust but verify all appropriate controls and functions are working properly