Booz | Allen | Hamilton

Cloud Computing Security

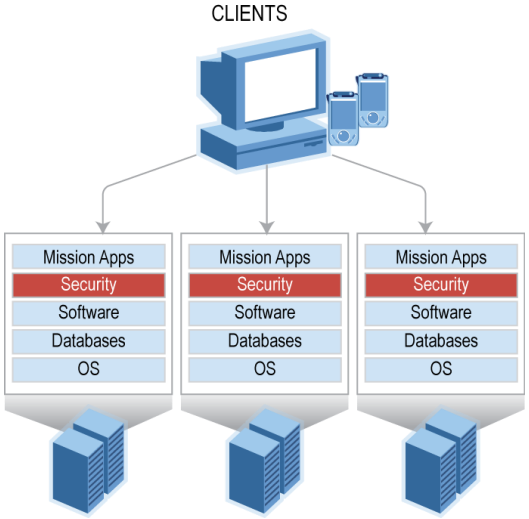
Stan Wisseman
December 9, 2009

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.**

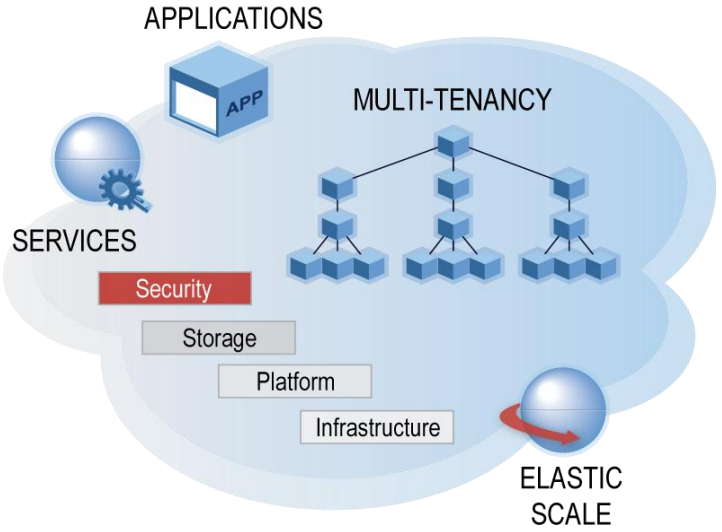
Traditional Computing

Barriers to Sharing, Duplicate Resources



Cloud Computing

Drives Culture of Sharing, Reduces Duplicate Resources Across All IT Functions



5 Essential Characteristics

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured Service

3 Service Models (What's being offered)

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

4 Deployment Models (How is it being offered)

- Public Cloud
- Private Cloud
- Community Cloud
- Hybrid Cloud

*Definitions are from NIST - http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

There are specific security challenges that organizations face when moving to a Cloud

Cloud Security Major Challenges

1 Data Protection

- Where do data physically reside, and does data's location have legal ramifications?
- Are data safely protected while stationary or in motion within and across a Cloud?
- How is availability of data assured in the Cloud?

2 Security Control

- What security controls need to be implemented by a Cloud provider and how are they implemented?
- How are assurance levels effectively and efficiently managed and assessed in Cloud?

3 Compliance

- Is my Cloud complying with the necessary guidance?
- Can the Cloud provider substantiate claims that security controls are implemented sufficiently?

4 Multi-Tenancy

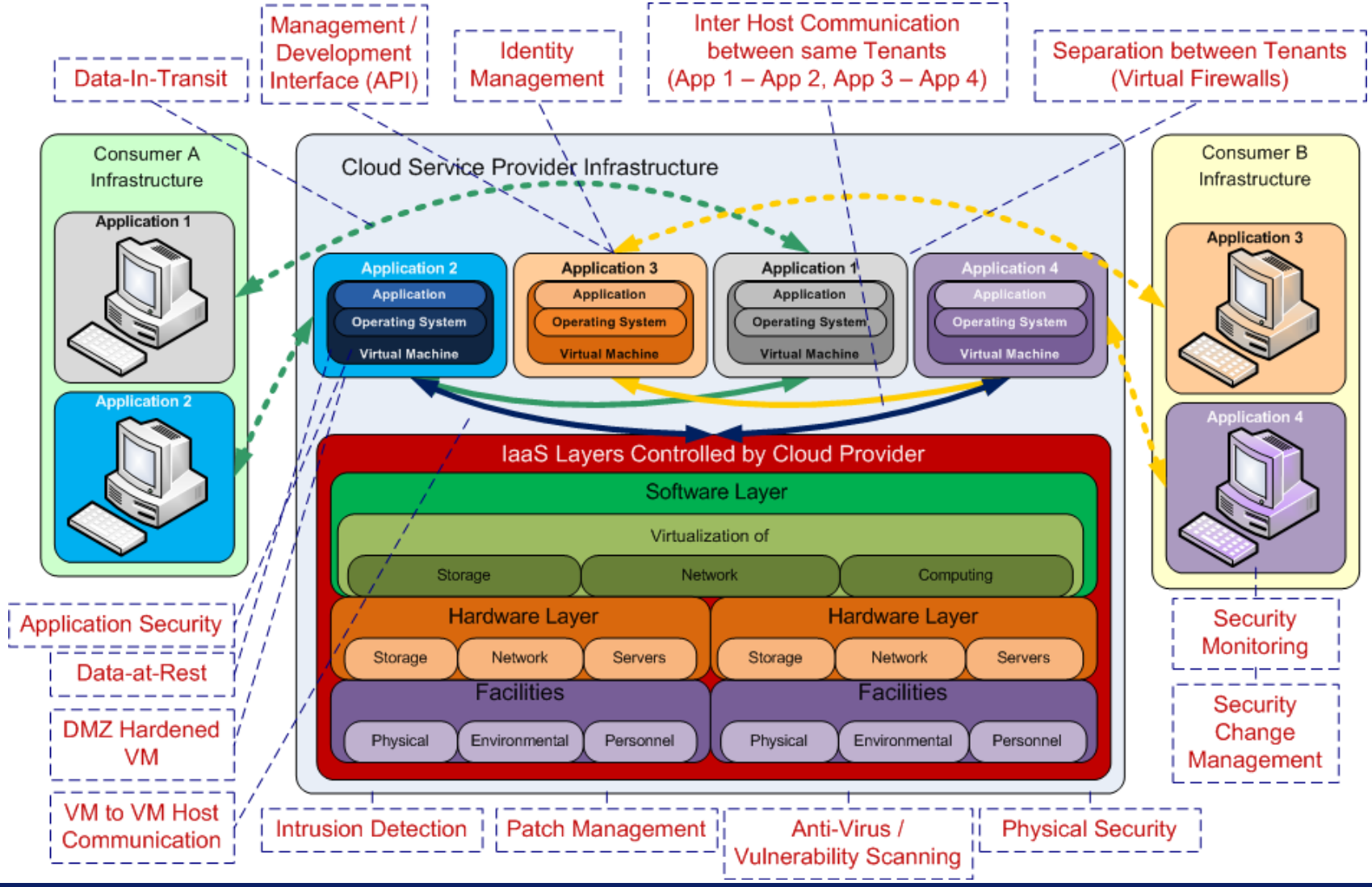
- Are my assets vulnerable if another consumer is exploited by an attack?
- How does the cloud provider keep different consumers' data separated and inaccessible by other consumers?

5 Security Governance

- Who owns / accesses / deletes / replicates my data in the cloud?
- How do you ensure policy enforcement?
- How do I measure and track service/network performance?

To Resolve These Issues, Clients Must First Focus On Addressing Underlying Strategic Considerations. These questions identify the key fundamental issues that agencies (working with cloud providers) must address in order to resolve the overall security hurdles. In some cases, these strategic considerations represent the root cause of each challenge.

Infrastructure as a Service Notional Security Model



If there is a Data Spill, what do you need to do about it?

- Data leakage/loss - The accidental leaking of sensitive information
- "Data Spills" - a security accident that results in the transfer of classified or sensitive information to unaccredited and unauthorized information systems, applications or media.
- Requirements for cleanup of a spill vary with the classification of the data spilled and the data owner.
- Using 3x block overwrite of data and slack space is typically acceptable for DoD and Intel data spills.
- **However** - The Govt client (data owner) makes the final determination as to how we must clean a spill. This may require confiscation, degaussing, or wiping of equipment.

Data Spill Cleanup – Standard Operating Procedures

- Only persons with the appropriate level clearance may clean the spill
- All instances of the data in question must be identified
- Use a software tool (i.e. Secure Clean from White Canyon) to erase spilled file(s)
- Use a software tool (i.e. Secure Clean from White Canyon) to perform a 3x overwrite of the slack space on the disks that contained the contaminated data
- Any users that had possession of the data that are not appropriately cleared must sign a non-disclosure statement
- All users that had possession of the data must complete and sign an Incident Certification Form (this is a statement identifying what was done with the data in question i.e. printed, faxed, saved on home computer, downloaded to blackberry etc.)

Objectives of Cloud Computing Pilot

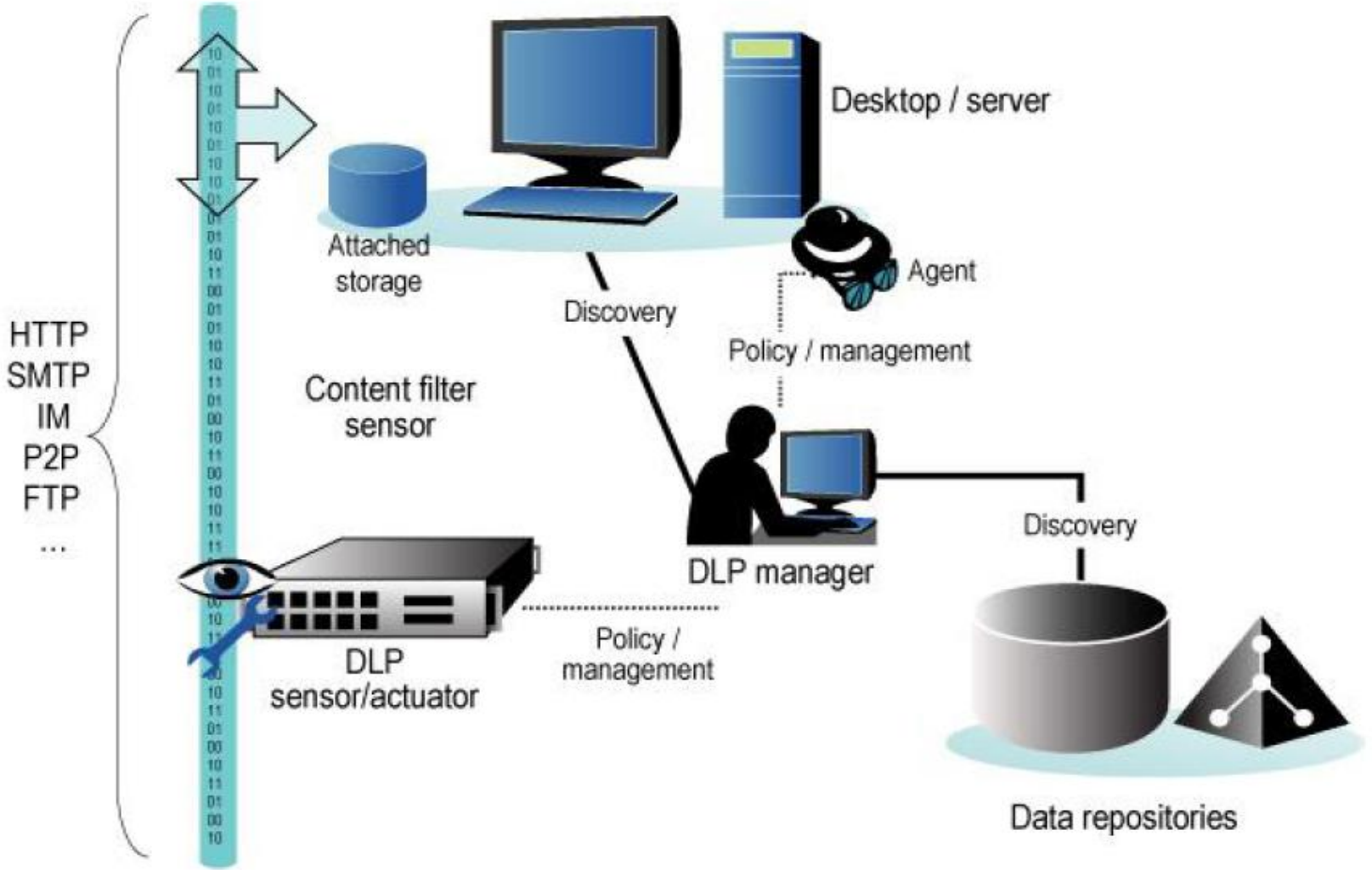
The objective of the Cloud Pilot is to prototype the transition, implementation, and hosting of an Enterprise Application in a Public IaaS Cloud, in order to identify the challenges, risks, and costs involved with transitioning applications to Cloud Infrastructures

Pilot will result in:

- Technical engineering and planning to host an Enterprise Application in the Cloud
- Security analysis and assessment of the viability of protecting proprietary corporate and Government data in the Cloud and in transit to/from the Cloud
- Evaluation and refinement of organization's Cloud Computing cost models, specifically in the areas of Transition

Data spills remediation part of pilot's scope

Data Loss Protection & Data Spill Prevention



Data Spill Cleanup

- **Data sanitization methods requiring logical access**
  – Virtual Servers configured with Elastic Block Storage (EBS) support utilities executing 3x block overwrite of data and slack space (aka SDelete and Secure Clean)
  - We have successfully tested SDelete and Secure Clean (utilities used in the organization's Data Spill Cleanup SOP) in the Amazon Cloud
- **Data sanitization methods requiring physical access**
  - Amazon does not allow clients physical entry/access to their data centers.
  - If the data owner requires confiscation, degaussing, or wiping of equipment, these methods are NOT supported with the Amazon Cloud.
  - Supporting the possible confiscation, degaussing, or wiping of equipment will require a Cloud Provider other than Amazon.

Risk management for data spills and data leaks

- **Data Spill Sanitization - Virtual Servers configured with Amazon's Elastic Block Storage (EBS) support utilities executing 3x block overwrite of data and slack space (aka SDelete and Secure Clean)**
- **Side Channel Vulnerability Protection – Limit of One Virtual Machine per Physical server - (Single Tenant)**
- **Use of CA DLP to monitor data information flows**
- **Security Hardening – Harden all Virtual images via STIGs**
- **Storage Release – Execute SecureClean 3x block overwrite of data and slack space on all storage volumes prior to the release of the storage device.**
  - Ensures that all data is properly overwritten in the event that notification of a data spill occurs after storage has been released and is no longer accessible.

Do you have questions?

- **Additional Information/Resources**
  - For more detailed information, please contact:

Stan Wisseman
Senior Associate

Booz | Allen | Hamilton

Booz Allen Hamilton, Inc.
8283 Greensboro Drive
McLean, VA 22102, USA
Tel (703) 403-8549
Wisseman_stan@bah.com