RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

CHANGE

Challenge today's security thinking

SESSION ID: PST-W10

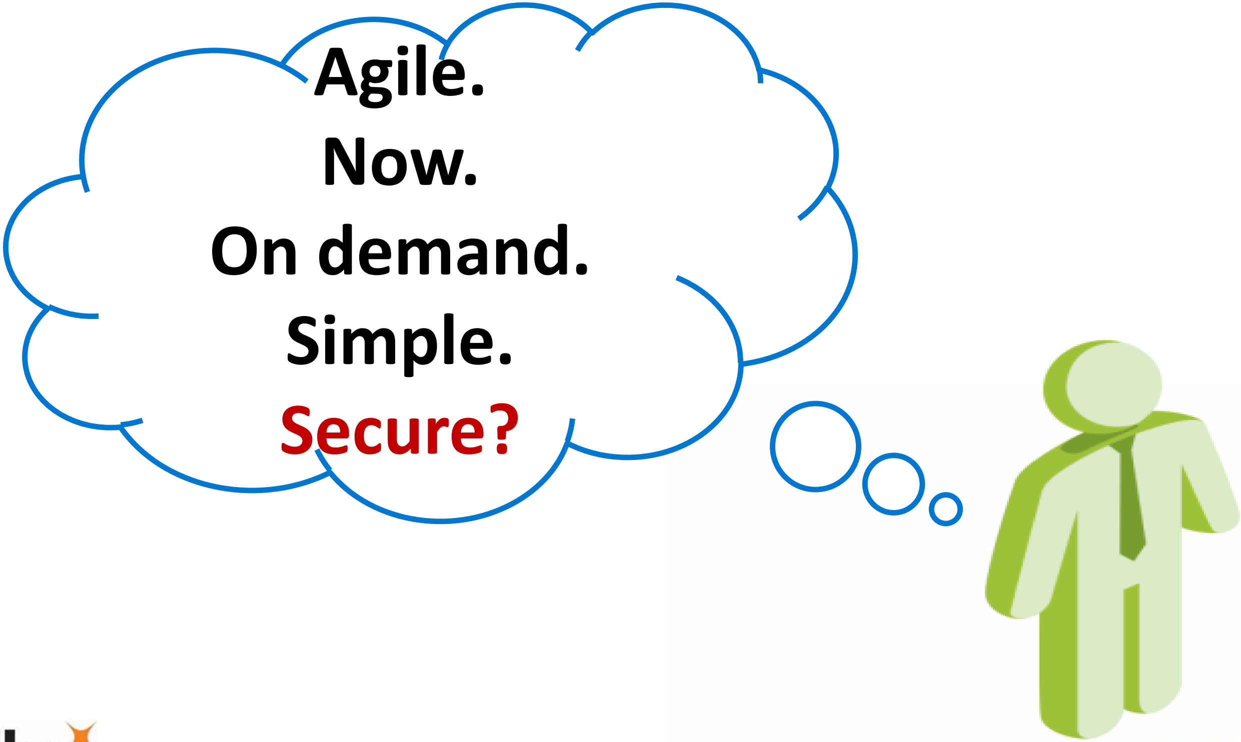
Whose Cloud Is It Anyway? Exploring Data Security, Ownership and Control

David Etue

VP, Business Development, Identity and Data Protection
Gemalto
@djetue

#RSAC

Cloud and Virtualization Are Changing the Way IT is Managed and Consumed



Agile.

Now.

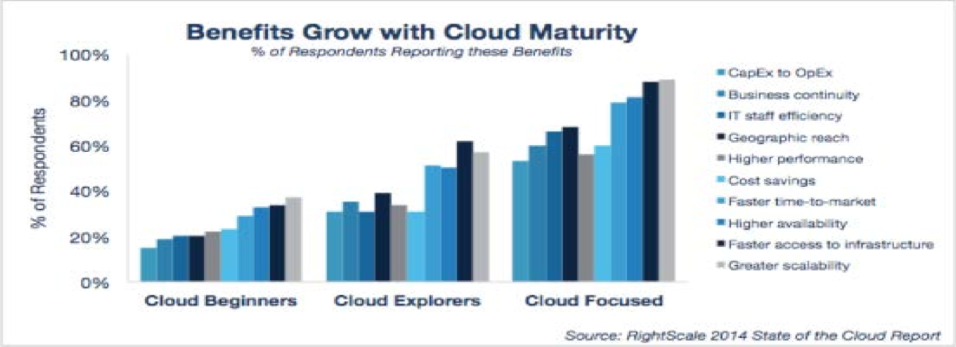
On demand.

Simple.

Secure?

Cloud Benefits Are Being Realized…

- 80% of mature cloud adopters are seeing:[1]
  - Faster access to infrastructure
  - Greater Scalability
  - Faster Time to Market for Applications
- 50% of cloud users report benefits including:[1]
  - Better application performance
  - Expanded geographic reach
  - Increased IT staff efficiency



Benefits Grow with Cloud Maturity

% of Respondents Reporting these Benefits

Source: RightScale 2014 State of the Cloud Report

RightScale 2014

STATE OF THE CLOUD REPORT

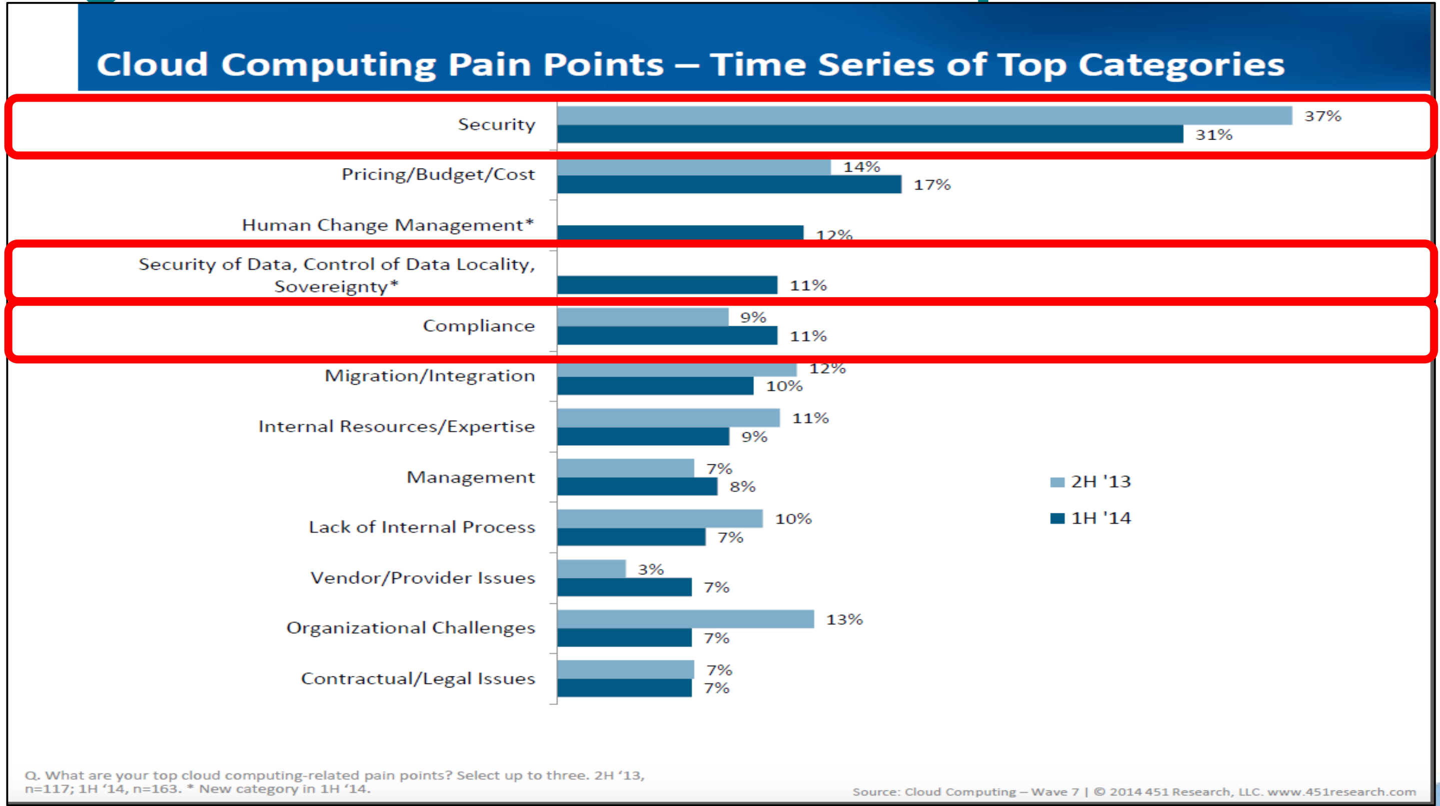
Public Cloud Adoption Nears 90 Percent on the Journey to Hybrid Cloud

[1]- *RightScale State of the Cloud Report 2014*

…But Cloud Benefits Are Driven by Sharing

And Security and Compliance Are Not the Biggest Fans of Sharing…

Leading Inhibitors to Cloud Adoption



Cloud Computing Pain Points – Time Series of Top Categories

Q. What are your top cloud computing-related pain points? Select up to three. 2H '13, n=117; 1H '14, n=163. * New category in 1H '14.

Source: Cloud Computing – Wave 7 | © 2014 451 Research, LLC. www.451research.com

451 Research - Cloud Computing Wave 7

Security and Compliance Concerns With Shared Clouds

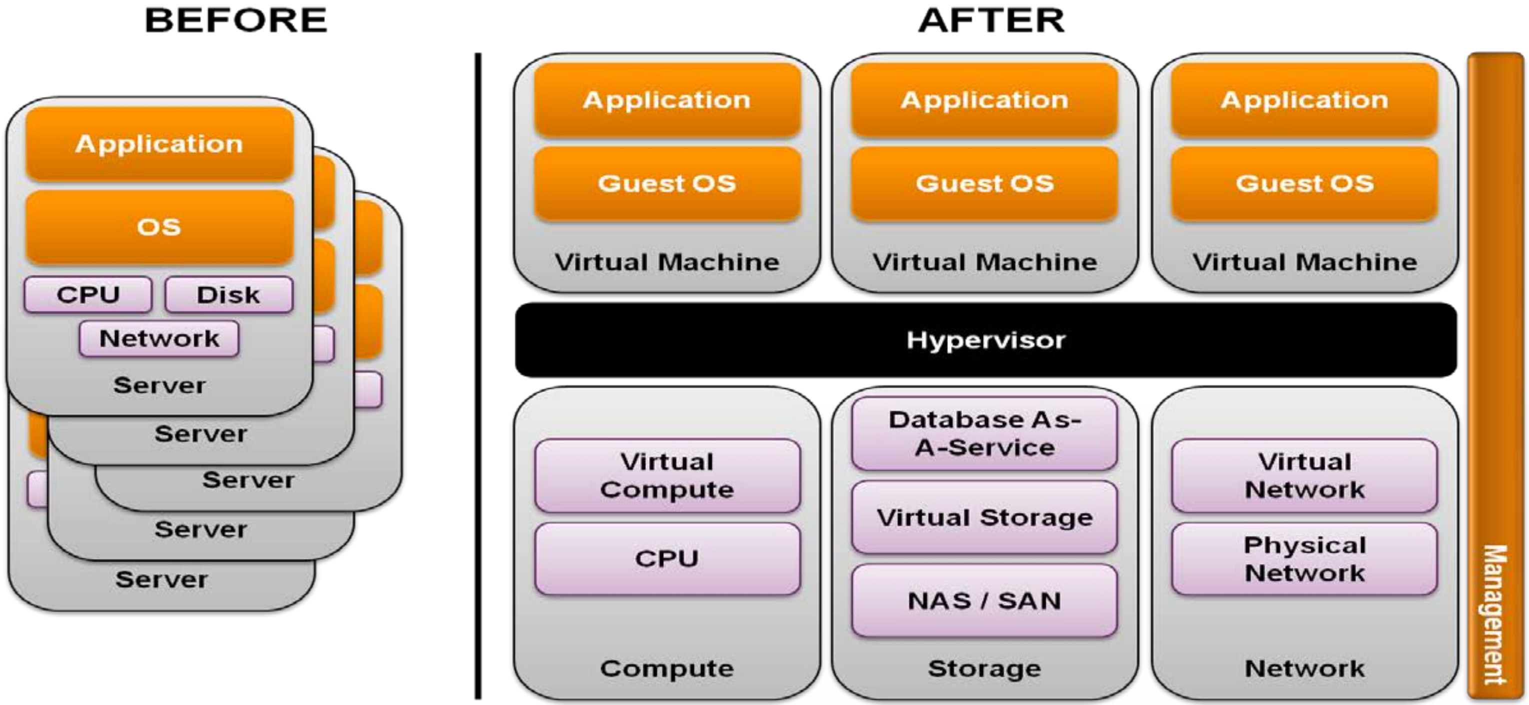
Data Governance Lack of Visibility	• Can you track all of my data instances? Backups? Snapshots? • Am I aware of government requests/discovery? • Do you new when data is copied?
Data Compliance Lack of Data Control	• Who is accessing my data? • Can I illustrate compliance with internal and external mandates? • Is there an audit trail of access to my data?
Data Protection Risk of Breach and Data Loss	• Are all my data instances secure? • Can I assure only authorized access to my data? • Can I "pull the plug" on data that's at risk of exposure or who's lifecycle has expired?

How Do You Maintain Ownership and Control Of Your Information In A Multi-Tenant Environment?

New Risks Driving Cloud Security Challenges

- Increased Attack Surface
- Privileged Users
- Ability to Apply Security Controls
- Control (or there lack of)

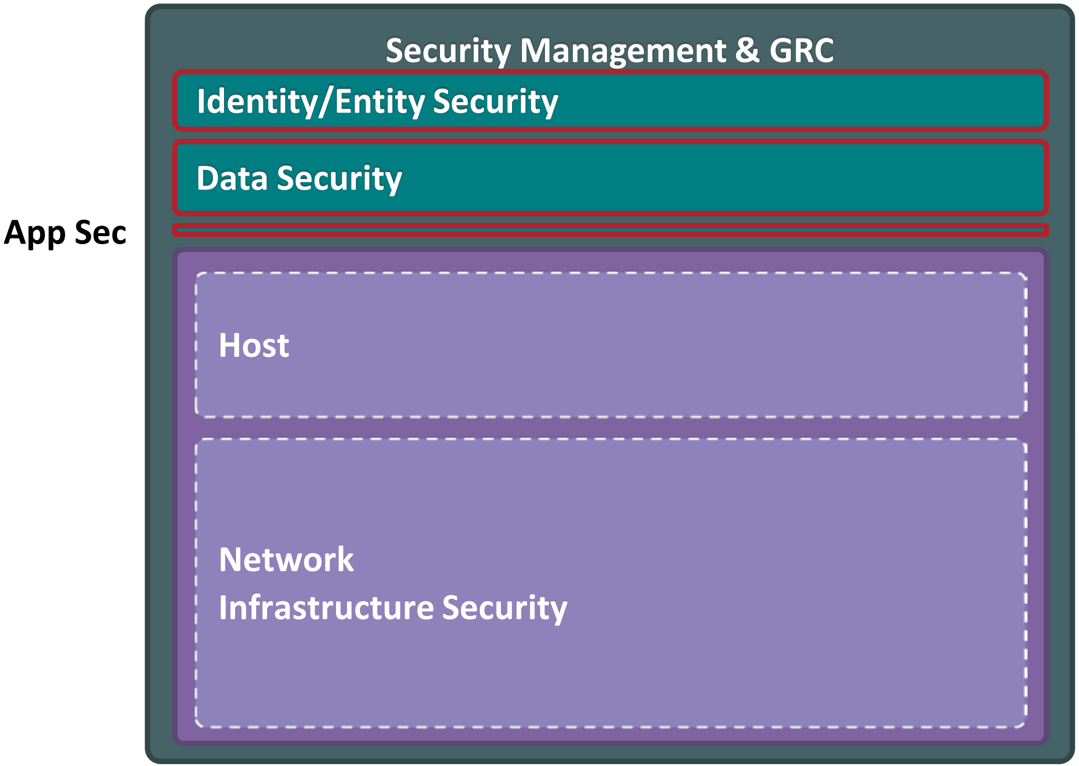
New Risk:
Increased Attack Surface



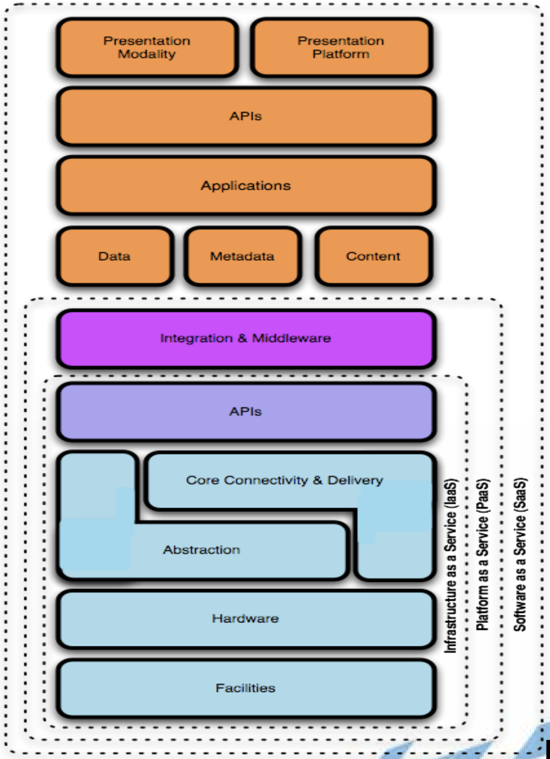
New Risk:
New Definition of Privilege

New Risk: Ability to Apply Security Controls

Security Controls Mapping and Sized by Budget

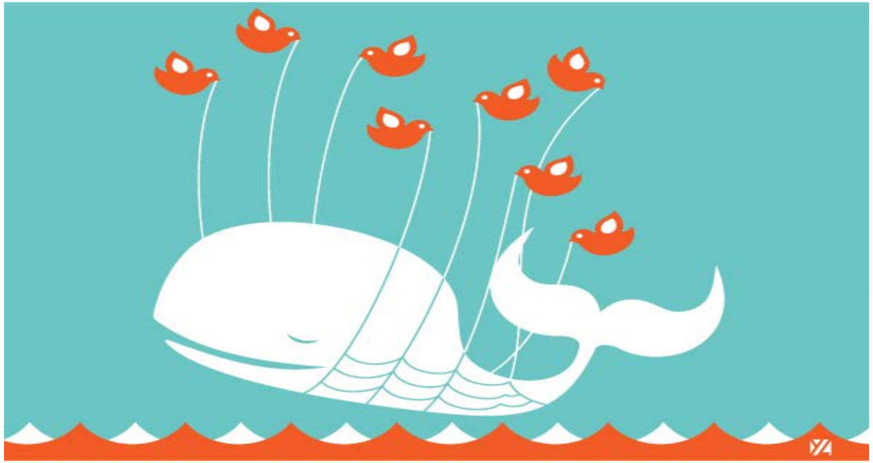


CSA Cloud Model



Source: Control Quotient: Adaptive Strategies For Gracefully Losing Control (RSA US 2013) by Josh Corman and David Etue.

New Risk: Ability to Apply Security Controls

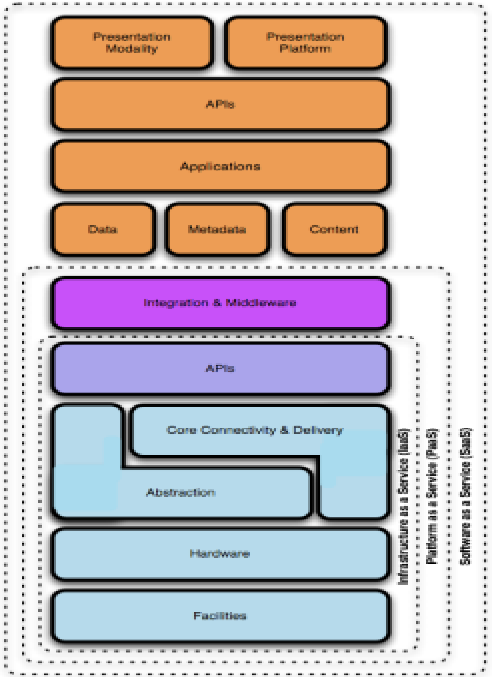


Most organizations are trying to deploy "traditional" security controls in cloud and virtual environments…but were the controls even effective then?

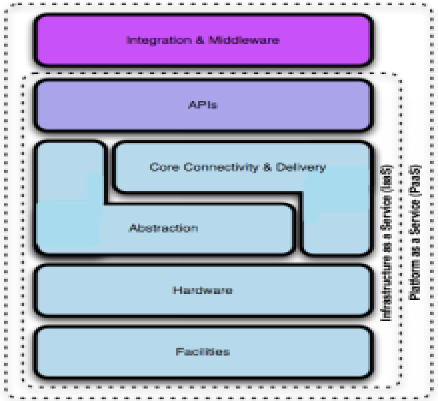
New Risk:
Control (or there lack of)

The lower down the stack the cloud provider stops, the more security **you** are tactically responsible for implementing & managing yourself.

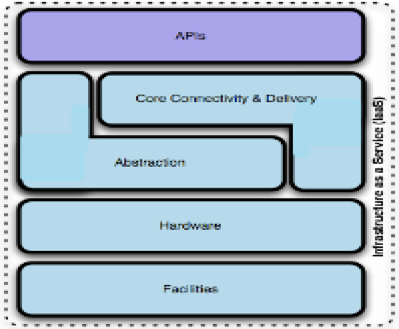
Salesforce - SaaS



Google AppEngine - PaaS

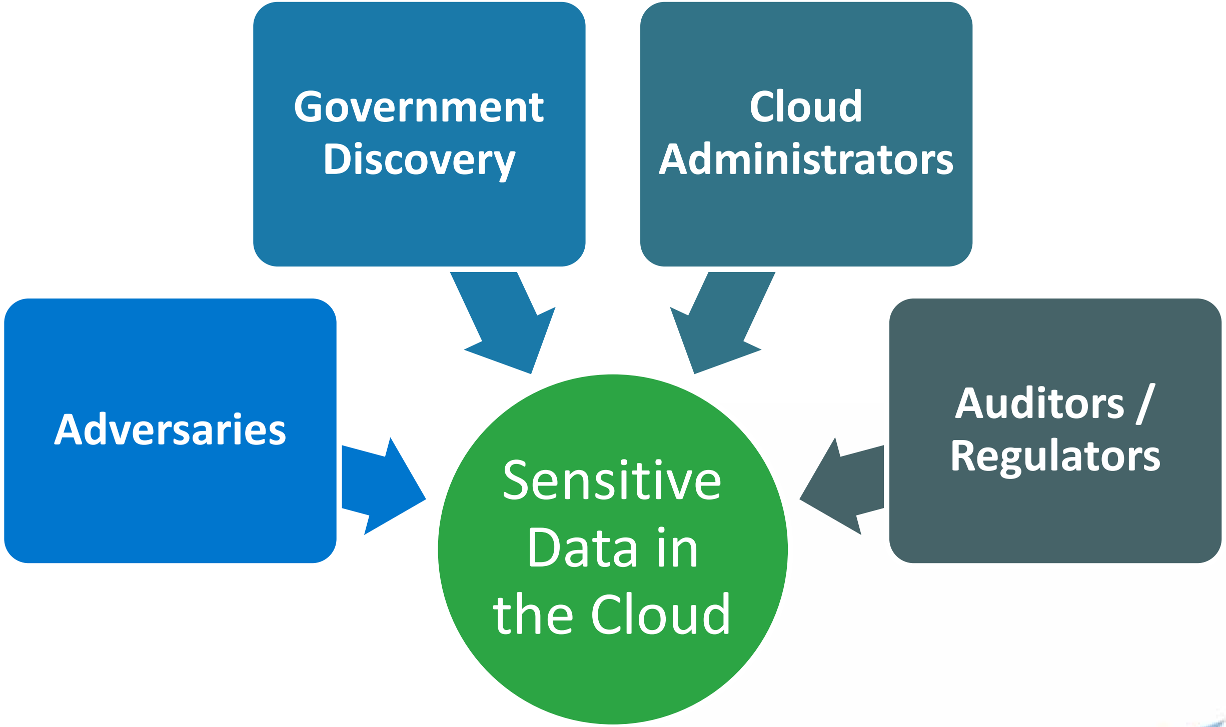

Integration & Middleware
APIs
Core Connectivity & Delivery
Abstraction
Hardware
Facilities
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)

Amazon EC2 - IaaS


APIs
Core Connectivity & Delivery
Abstraction
Hardware
Facilities
Infrastructure as a Service (IaaS)

Source: Control Quotient: Adaptive Strategies For Gracefully Losing Control (RSA US 2013) by Josh Corman and David Etue. "Stack" by Chris Hoff -> CSA

And Not Just The Traditional “Bad Guys"



Government Discovery

Cloud Administrators

Adversaries

Sensitive Data in the Cloud

Auditors / Regulators

So, Whose Cloud Is It Anyway?

Model	Private Cloud	IaaS in Hybrid / Community / Public Cloud	PaaS/SaaS
Whose Privilege Users?	Customer	**Provider**	**Provider**
Whose Infrastructure?	Customer	**Provider**	**Provider**
Whose VM / Instance?	Customer	Customer	**Provider**
Whose Application?	Customer	Customer	**Provider**
Government Discovery Contact?	Customer	**Provider**	**Provider**

Geographical Considerations?

Cloud Provider Headquaters
Cloud Region Location

- US Court Decision with Serious Implications: IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION, 13 Mag. 2814

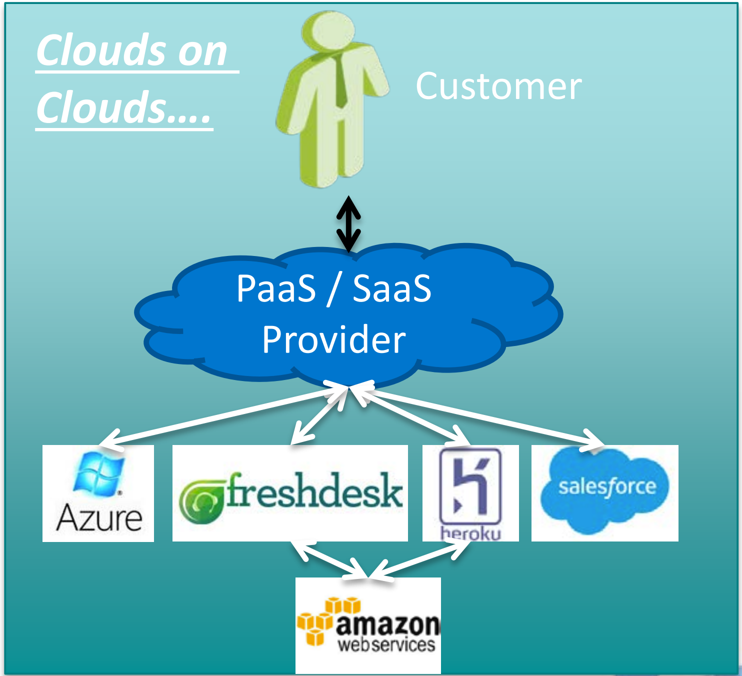
- A Sober Look at National Security Access to Data in the Cloud - A Hogan Lovells White Paper (covers US, EU, and EU member country legislation and case law)

- Safe Harbor is no longer… Microsoft: The Collapse of Safe Harbor

The Cloud "Supply Chain"

Two developers and a cloud account = SaaS company. Two developers, a cloud account and an Arduino board = IoT company. #security #cloud

- Many cloud providers, especially SaaS and PaaS built on top of other cloud providers
  - AWS Case Studies: Backupify, Freshdesk, Loggly, Sumo Logic
- MAY be discoverable in terms of service…
  - Heroku: "Heroku's physical infrastructure is hosted and managed within Amazon's secure data centers and utilize the Amazon Web Service (AWS) technology."
- May be more than one provider and more than one tier!

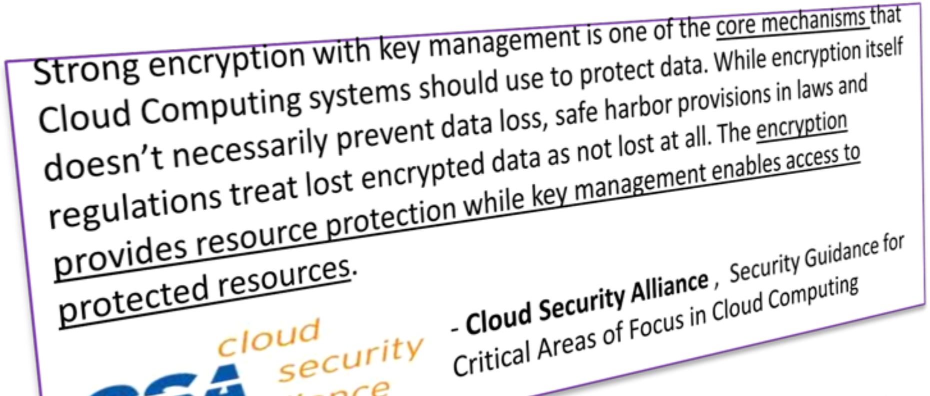


What is the trail created of your data—who and where?

Making it Your Cloud:
Key Enablers to Cloud Security

- Encryption (and Key Management)
- Identity and Access Management with Strong Authentication
- Segmentation
- Privilege User Management
- Detection and Response Capabilities
- System Hardening
- Asset, Configuration, and Change Management

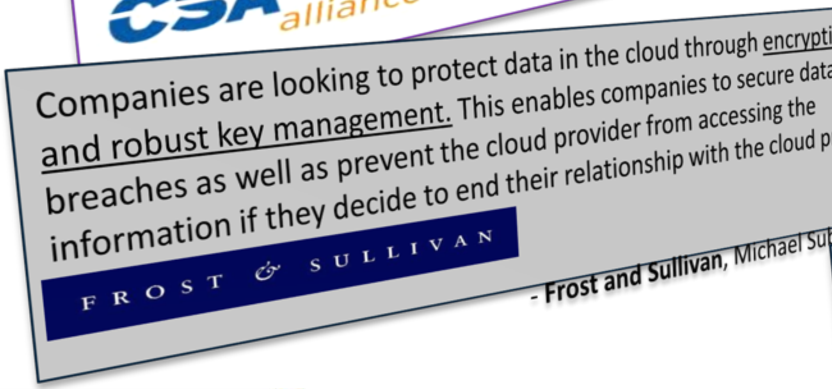
Encryption: Un-Sharing in a Shared Environment



Strong encryption with key management is one of the core mechanisms that Cloud Computing systems should use to protect data. While encryption itself doesn't necessarily prevent data loss, safe harbor provisions in laws and regulations treat lost encrypted data as not lost at all. The encryption provides resource protection while key management enables access to protected resources.

CSA cloud security alliance

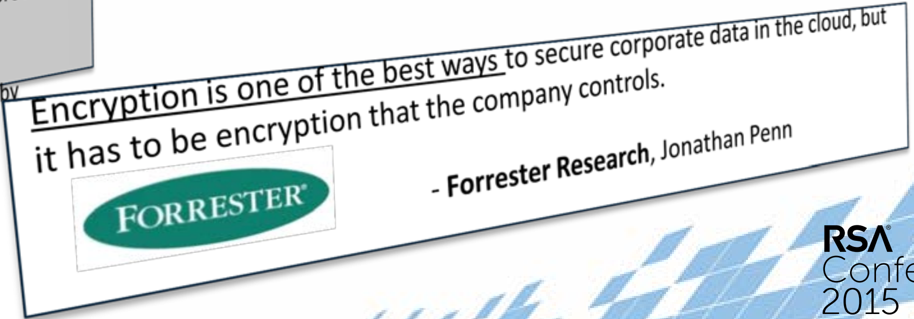
- **Cloud Security Alliance** , Security Guidance for Critical Areas of Focus in Cloud Computing



Companies are looking to protect data in the cloud through encryption keys and robust key management. This enables companies to secure data from breaches as well as prevent the cloud provider from accessing the information if they decide to end their relationship with the cloud provider.

FROST & SULLIVAN

- **Frost and Sullivan**, Michael Suby



Encryption is one of the best ways to secure corporate data in the cloud, but it has to be encryption that the company controls.

FORRESTER®

- **Forrester Research**, Jonathan Penn

Clouds Love Crypto!!!*

**with good key management…*

Cloud Encryption Models

Type of Encryption	Definition	Also Called:
Service Provider Encryption with Provider Managed Keys	Encryption performed by the cloud service provider using encryption keys owned and managed by the cloud service provider	- Server Side Encryption - SSE
Service Provider Encryption with Customer Managed Keys	Encryption performed by the cloud service provider using encryption keys owned and managed by the customer	- "Customer provided keys" - SSE-CPK
Customer Managed Encryption with Customer Managed Keys	Encryption performed by the customer using encryption keys owned and managed by the customer	- "Client side encryption" (for object storage and client-server environments)

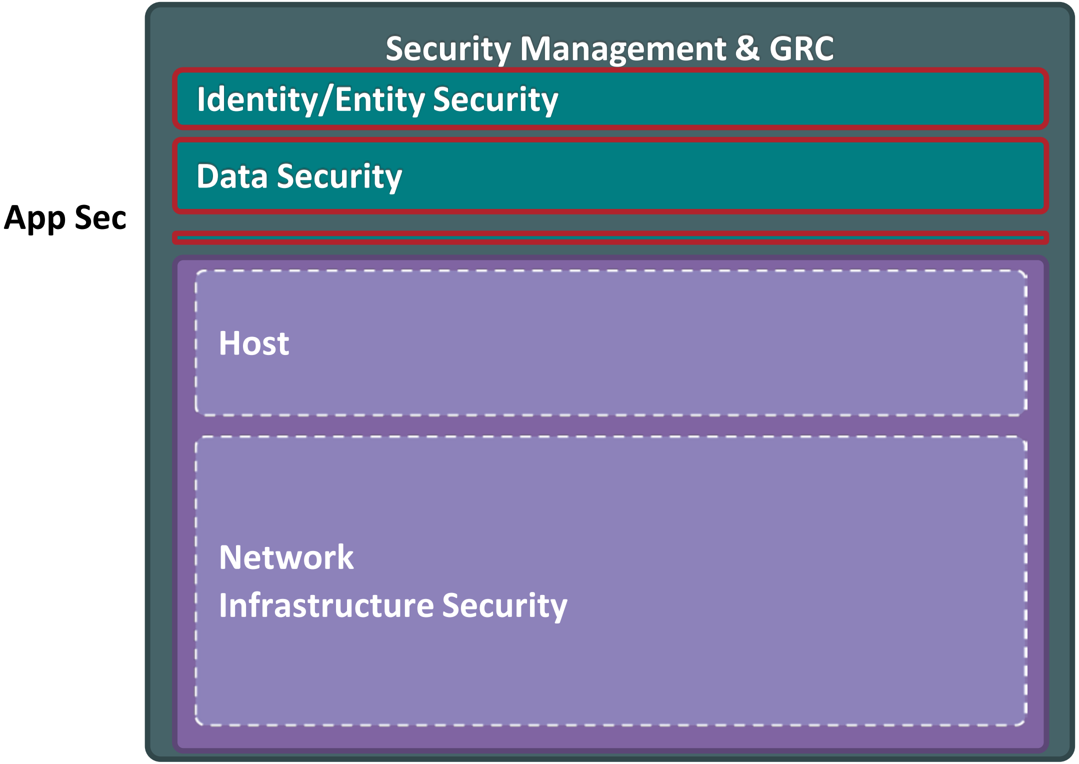
Remember: Encryption Data Can't Be Processed…

SaaS applications should be adding value to your data – what impact does encryption have? #security #RSAC

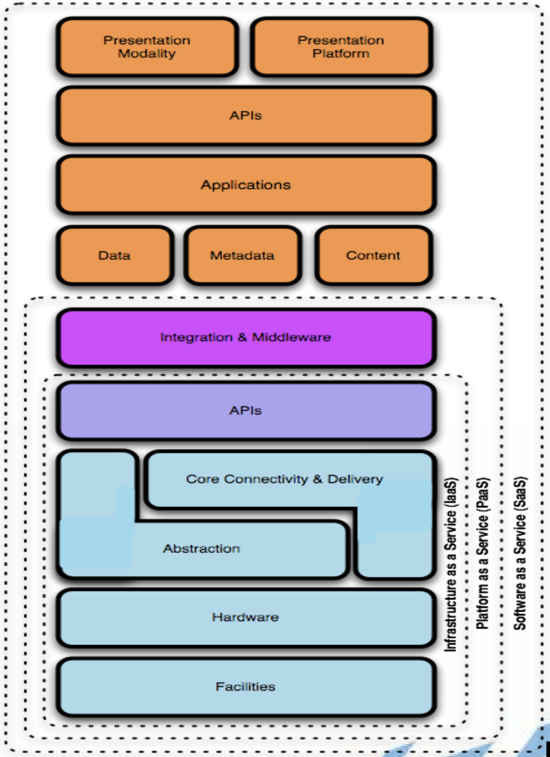
- Have to design encryption to enable data to be processed and accessed to support necessary business process
- An example: Cloud Encryption Gateways encrypt data before putting it in to SaaS applications
  - Provided by a Number of Vendors (CipherCloud, Perspecsys, Skyhigh, Vaultive, etc.)
  - Trade-off of security (encryption quality) and functionality…
  - Architectural implications
- Easy to minimize impact for IaaS and Storage, harder for PaaS and SaaS

How Do You Apply Security Controls?

Security Controls Mapping and Sized by Budget



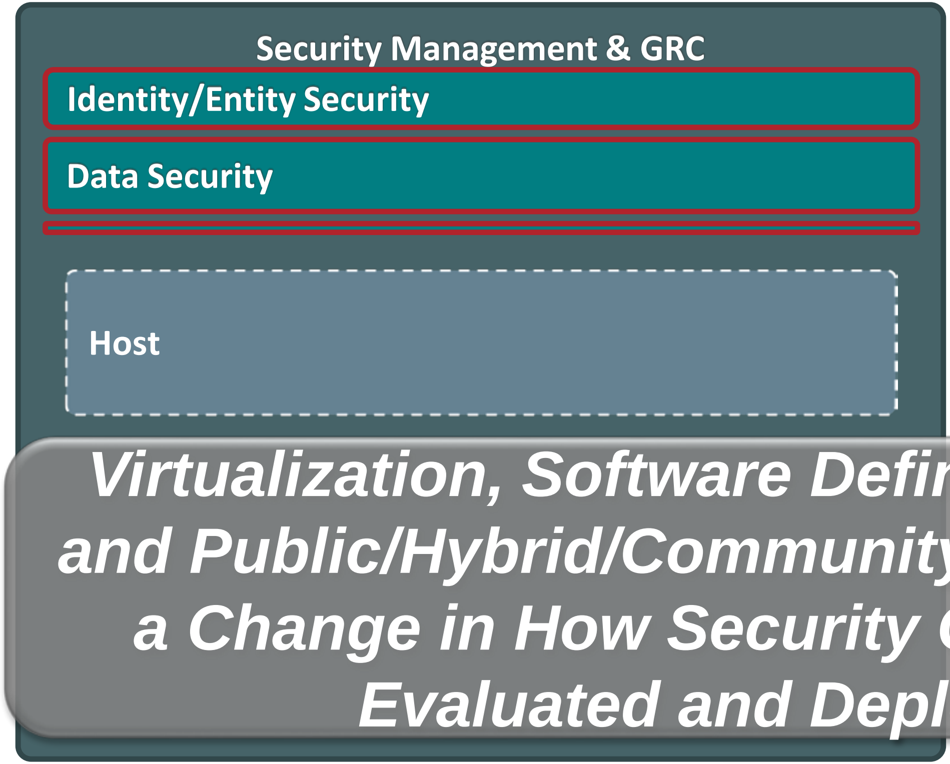
CSA Cloud Model



Source: Control Quotient: Adaptive Strategies For Gracefully Losing Control (RSA US 2013) by Josh Corman and David Etue.

Need to Focus "Up The Stack"

App Sec

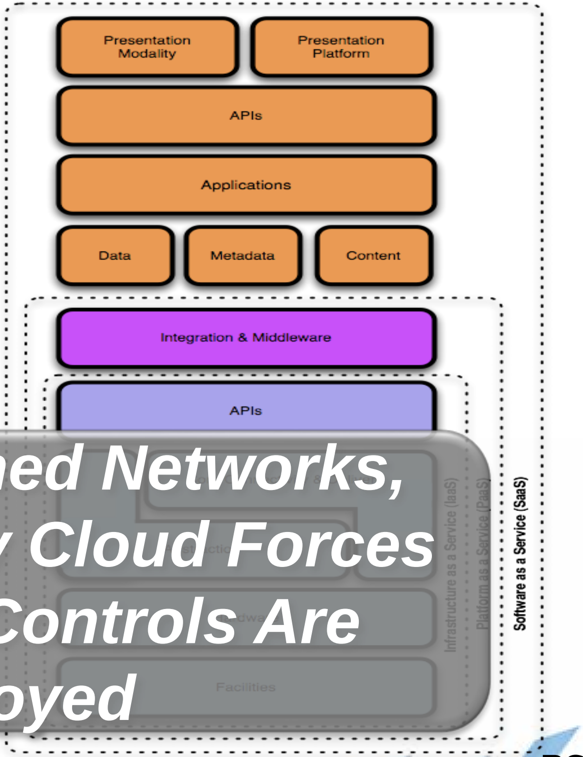

Security Management & GRC

Identity/Entity Security

Data Security

Host

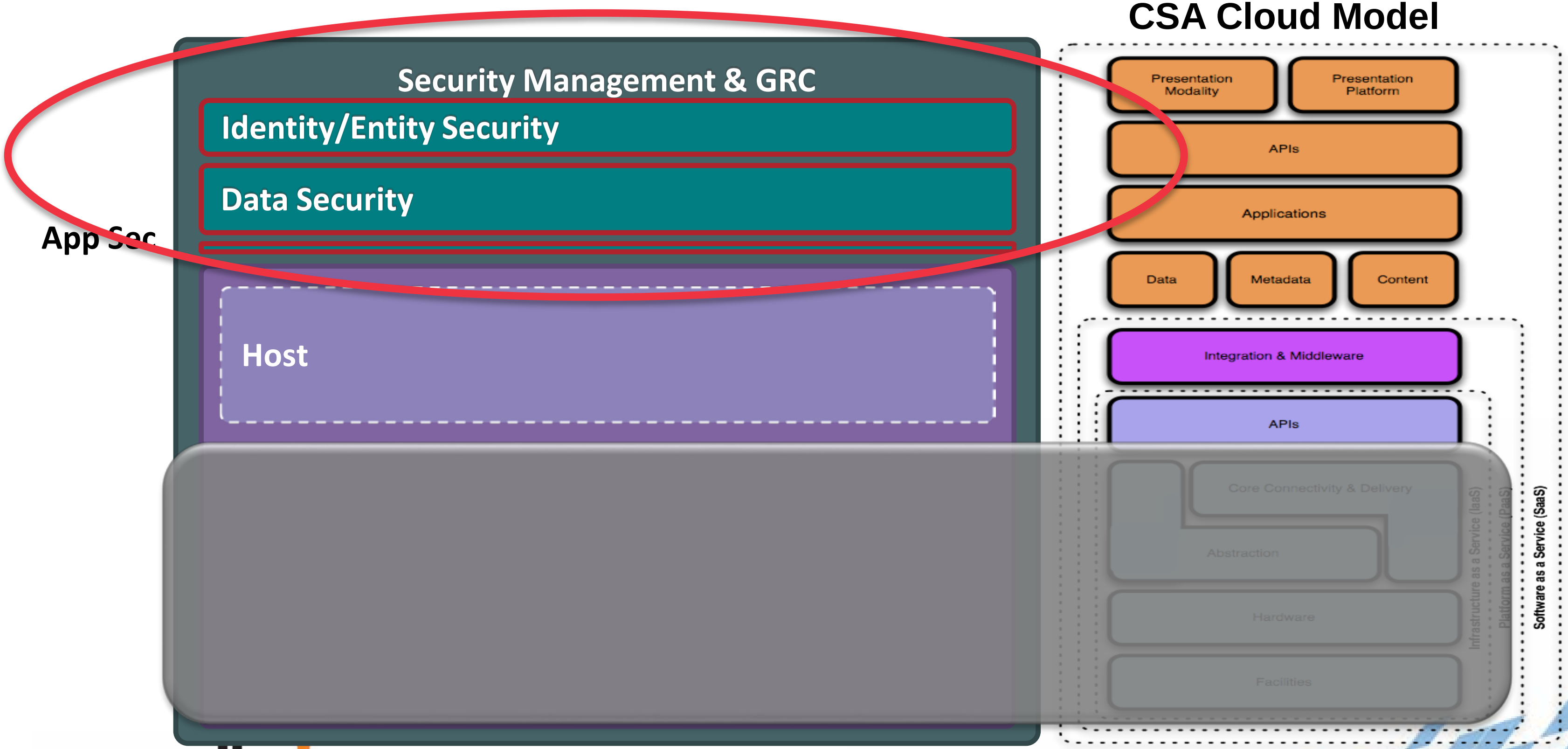
CSA Cloud Model



Virtualization, Software Defined Networks, and Public/Hybrid/Community Cloud Forces a Change in How Security Controls Are Evaluated and Deployed

Data Centric Security = Agility!

CSA Cloud Model



Security Management & GRC

Identity/Entity Security

Data Security

App Sec

Host

Presentation Modality

Presentation Platform

APIs

Applications

Data

Metadata

Content

Integration & Middleware

APIs

Core Connectivity & Delivery

Abstraction

Hardware

Facilities

Infrastructure as a Service (IaaS)

Platform as a Service (PaaS)

Software as a Service (SaaS)

Apply

- Be Part of the Solution—Don’t Be “Doctor No”
- Evaluate Security Solutions That are Cloud and/or SaaS delivered
  - Drive cost of security down
  - Gets direct experience using cloud
  - Illustrate to organization you can help use cloud securely
- Determine Your Teammates
  - Procurement, Legal, Finance, etc.
  - Understand Influence vs. Control
- Prepare
  - Get your policies ready for cloud (hopefully they are already)
  - Start adapting your toolkits “up the stack” toward data and identity