Top 10 Cloud Risks That Will Keep You Awake at Night

Shankar Babu Chebrolu Ph.D., Vinay Bansal, Pankaj Telang

.. **Amazon EC2** (Cloud) to host Eng. Lab testing….

We want to use **SalesForce.com** to host our next Cisco customer application

Cisco Business User

.. **Facebook/MySpace** to collaborate with company's customer….

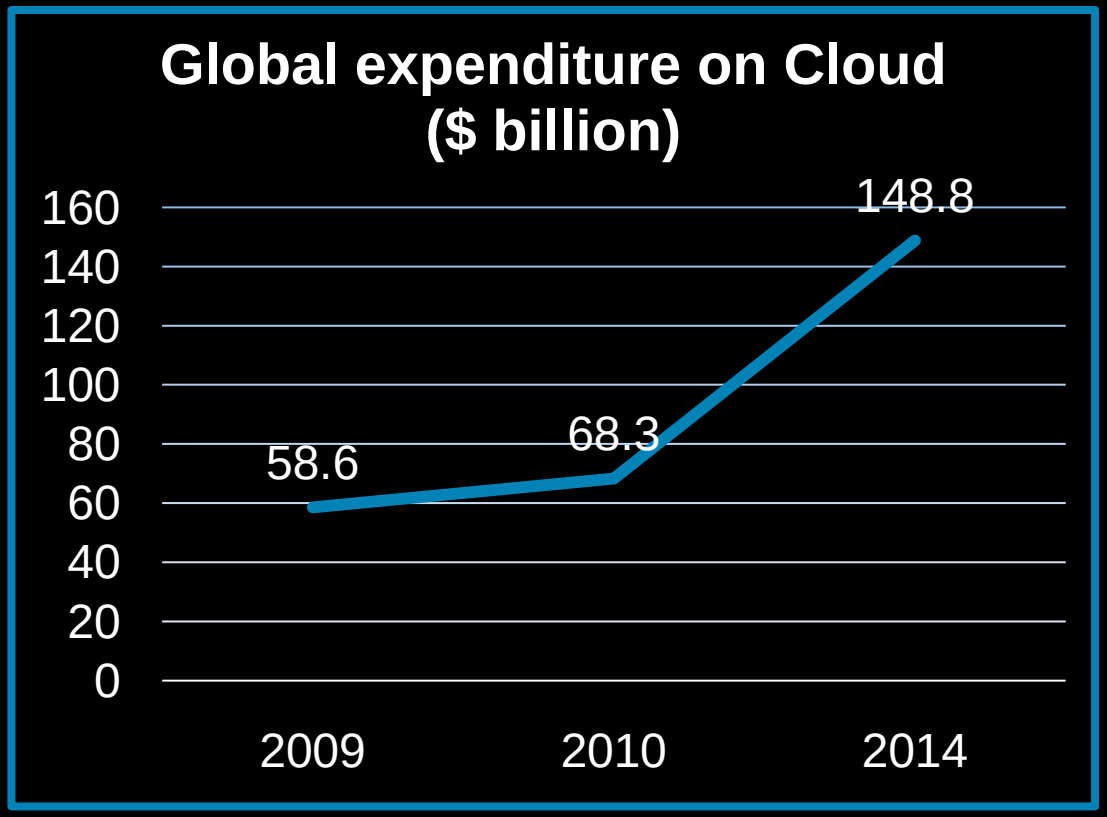
.. **Google docs** to share Cisco documents within team….

400+ ASPs (aka Cloud Providers) in use within Cisco

Outline

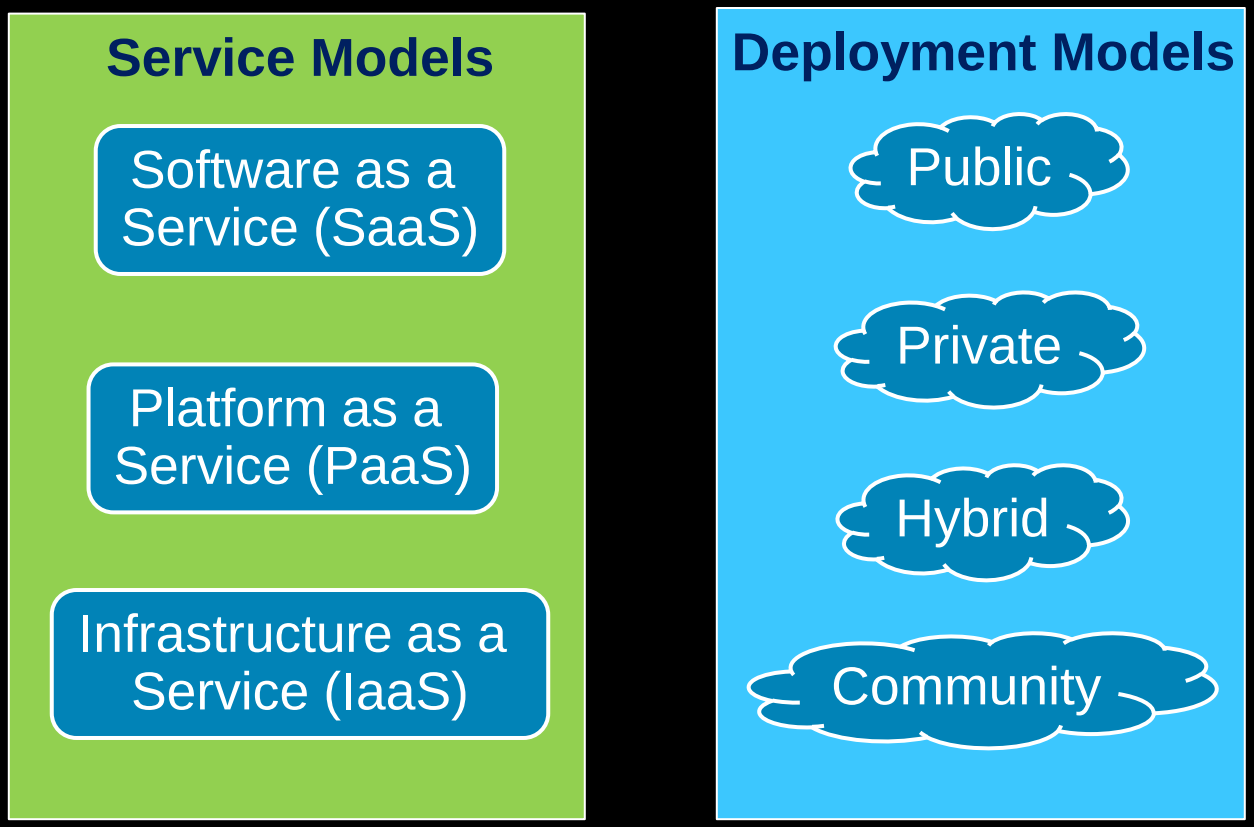
- Cloud – Industry Adoption Trend
- Cloud Taxonomy
- OWASP Cloud Top 10
- Cloud Security Risks
- Risk Mitigations
- Q & A

Cloud – Industry Adoption Trend



(Source Gartner)

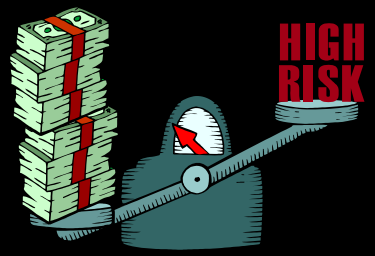
Cloud Taxonomy



Broad Network Access | Rapid Elasticity | Measured Service | On-Demand Self-Service | Resource Pooling

(Adapted from CSA Guide, originally from NIST)

Cloud Top 10 - Motivation



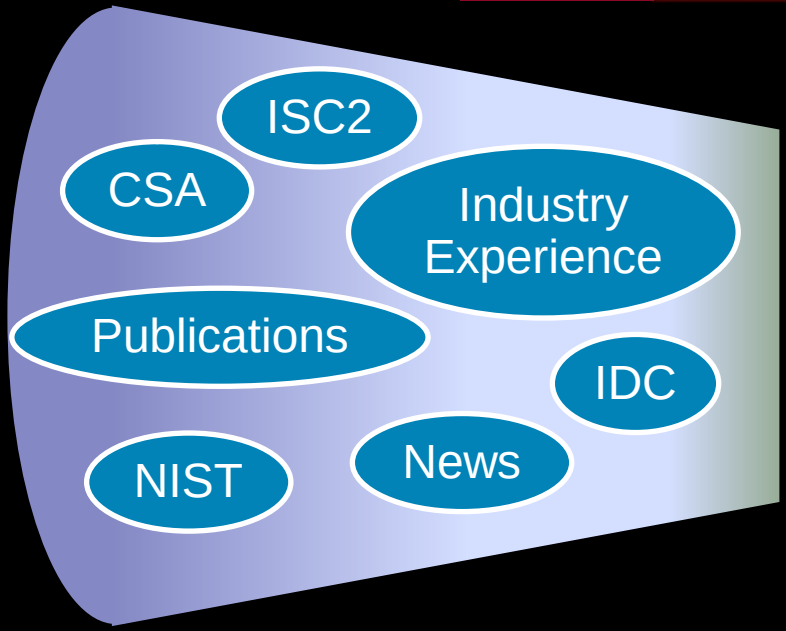
Develop and maintain top 10 risks with cloud

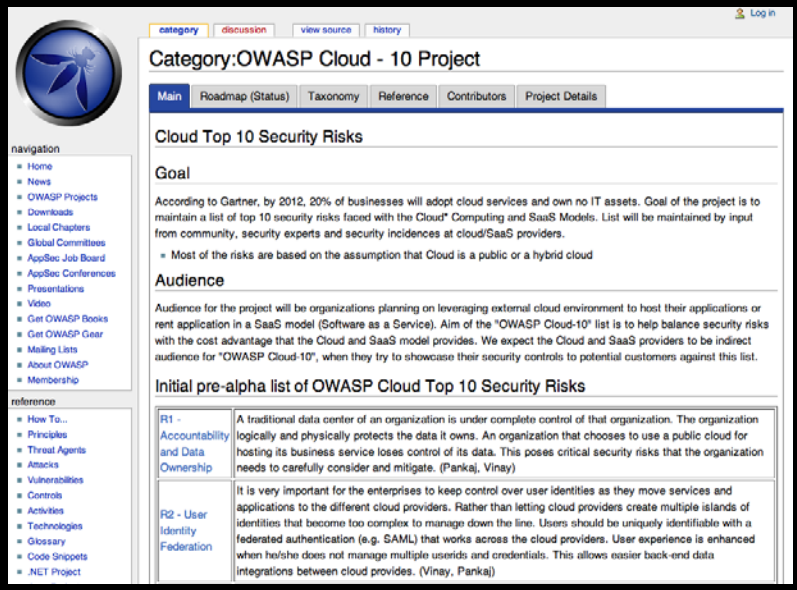
Serve as a quick list of top risks with cloud adoption

Provide guidelines on mitigating the risks

Cloud Top 10 - Approach

✓Easily Executable
✓Most Damaging
✓Incidence Frequency





OWASP Cloud Top 10

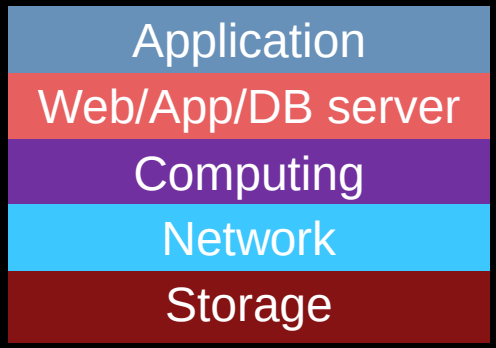
Cloud Top 10 Risks

- R1: Accountability & Data Risk
- R2: User Identity Federation
- R3: Regulatory Compliance
- R4: Business Continuity & Resiliency
- R5: User Privacy & Secondary Usage of Data
- R6: Service & Data Integration
- R7: Multi-tenancy & Physical Security
- R8: Incidence Analysis & Forensics
- R9: Infrastructure Security
- R10: Non-production Environment Exposure

R1: Accountability

In traditional data center, the owning organization is accountable for security at all layers

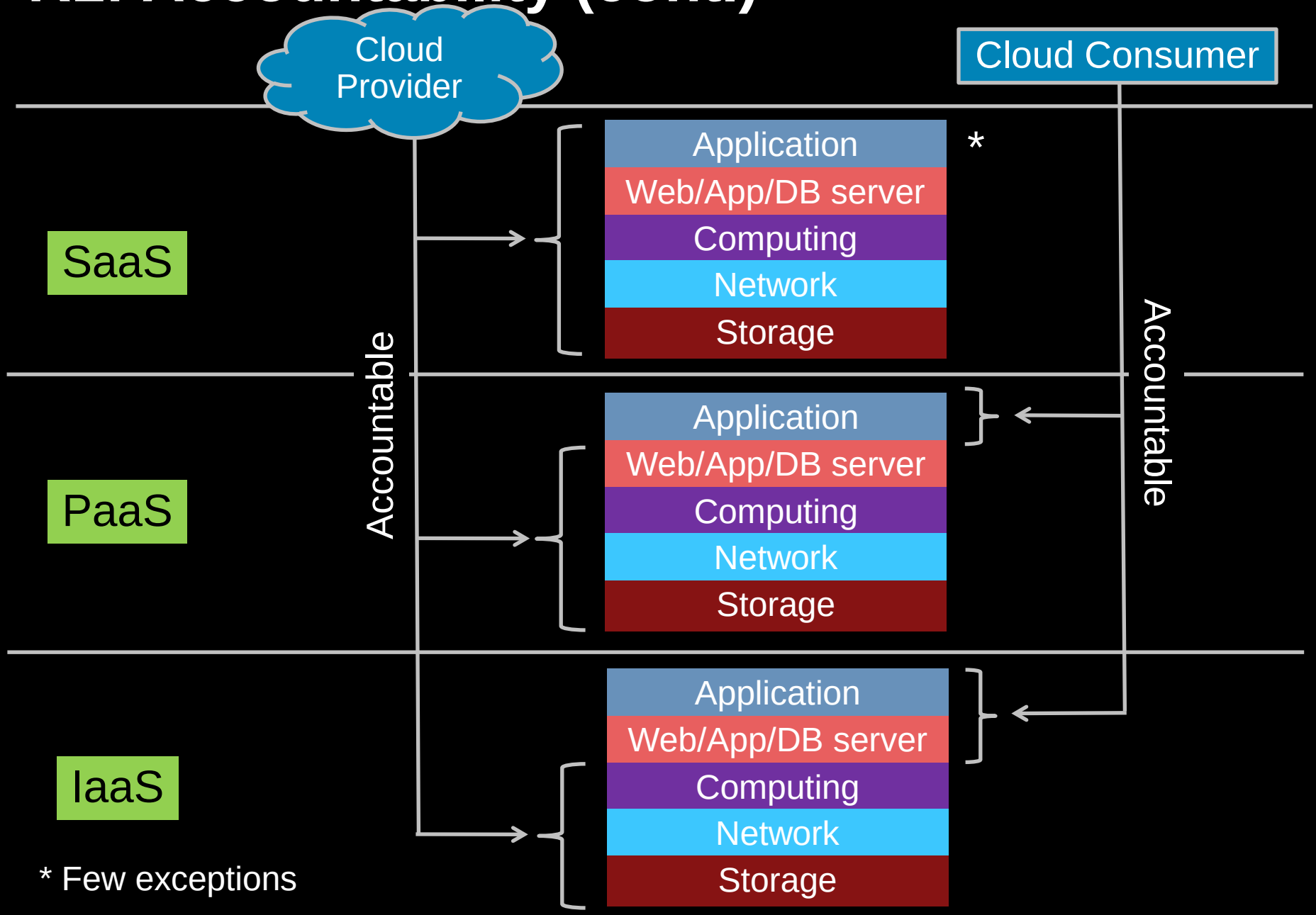
Organization fully accountable for security at all layers



You can outsource hosted services but you cannot outsource accountability

In a cloud, who is accountable for security at these layers?

R1: Accountability (cont.)



R1: Data Risk

How sensitive is the data?

Informal blogs
Twitter posts
Public news
Newsgroup messages

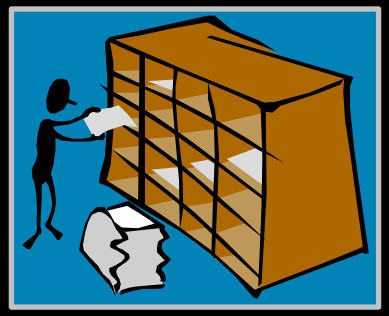
Health records
Criminal records
Credit history
Payroll

Who owns the data?

Data stored anywhere !!

Data encrypted? Single vs. multiple keys

R1: Accountability & Data Risk
Mitigation

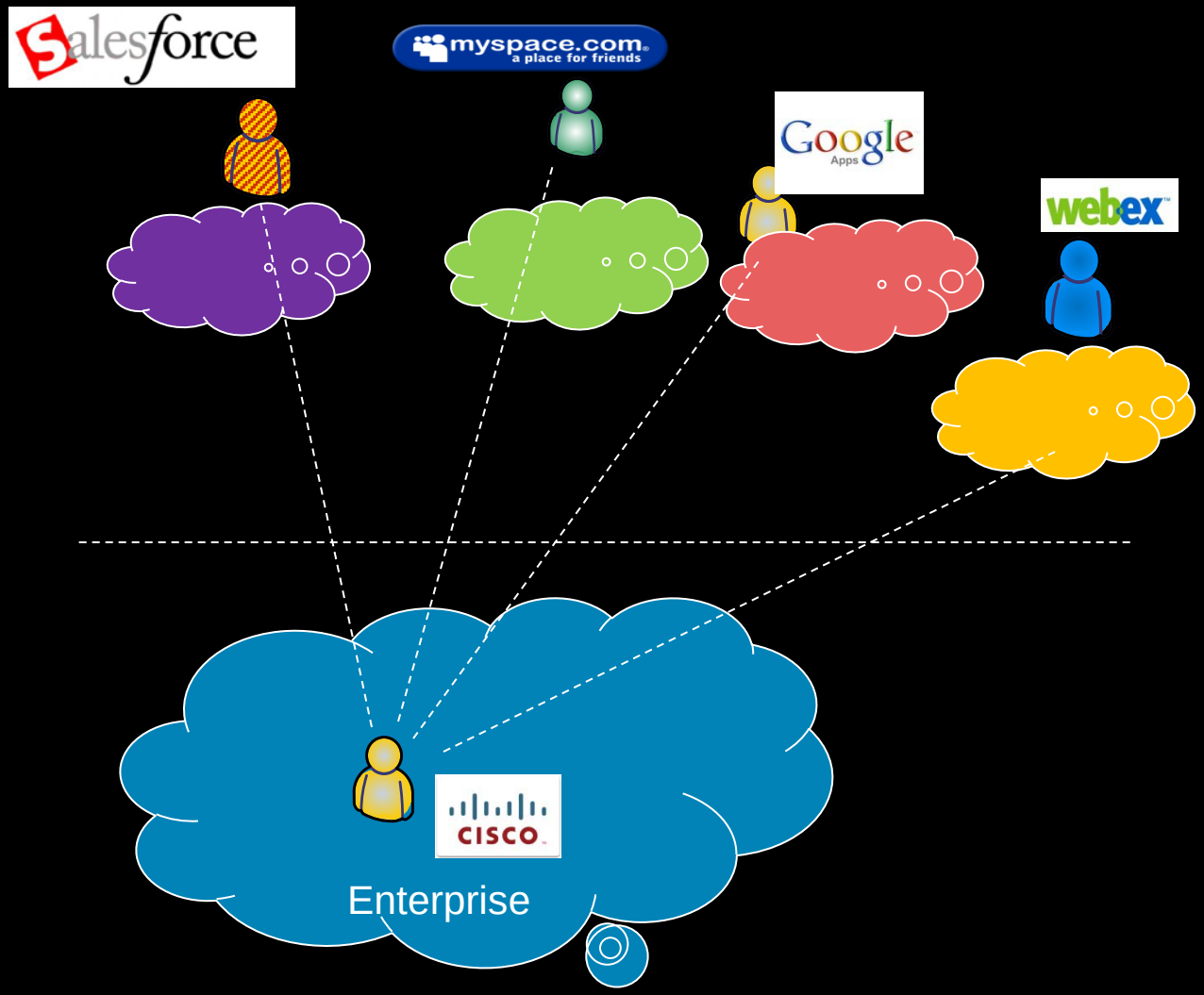


Logical isolation of the data of multiple consumers

Provider fully destroys deleted data

Multiple encryption keys

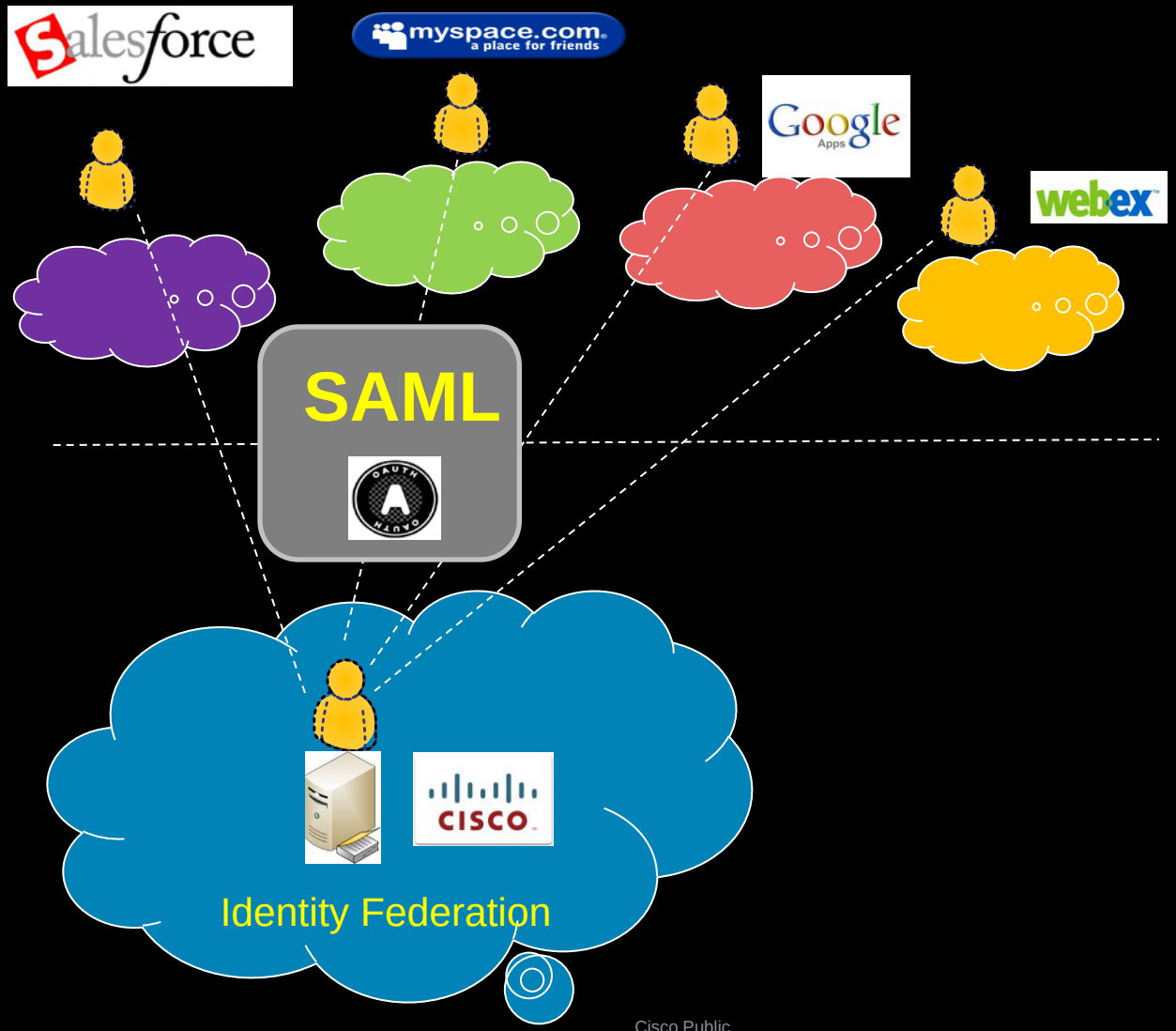
R2: Risks: Islands of User Identities



Security Risks

1. Managing Identities across multiple providers
2. Less control over user lifecycle (off-boarding)
3. User experience

R2: Mitigation: User Identity Federation

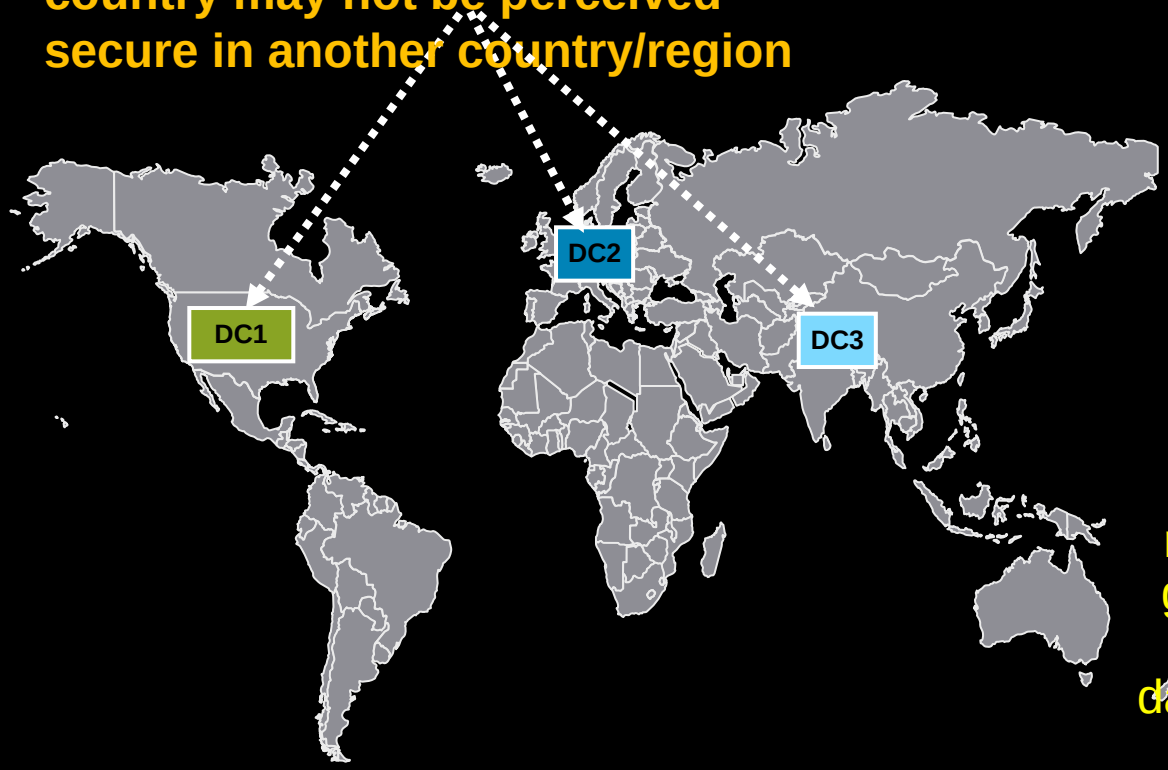


Mitigations

1. Federated Identity
2. OAuth for backend integrations
3. Tighter user provisioning controls

R3: Regulatory Compliance

Data that is perceived to be secure in one country may not be perceived secure in another country/region



Lack of transparency in the underlying implementations makes it difficult for data owners to demonstrate compliance(SOX/HIPAA etc.)

Lack of consistent standards and requirements for global regulatory compliance – data governance can no longer be viewed from a point-to-point data flow perspective but rather a multi-point to multi-point.

European Union (EU) has very strict privacy laws and hence data stored in US may not comply with those EU laws (*US Patriot Act allows federal agencies limitless powers to access any corporate data etc*)

R3: Regulatory Compliance – Mitigation Strategy

Apply risk management framework, case-by-case basis

Define data protection requirements and SLAs

Provider / Consumer agreement to a pre-defined RACI model

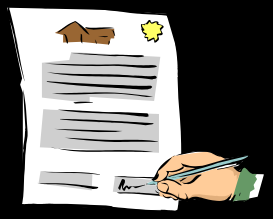
R4: Business Continuity & Resiliency

Lack of know-how and capabilities needed to ensure continuity & resiliency

Cloud provider may be acquired by a consumer's competitor

Monetary losses due to an outage

R4: Business Continuity & Resiliency
Mitigation

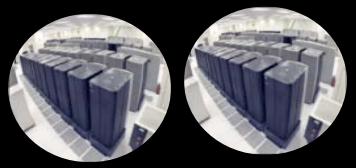


Contract defines Recovery Time Objectives, and monetary penalty for downtime

Cloud provider's Business Continuity program certified to standard such as BS 25999

R5: User Privacy & Secondary Usage of Data

Users vs. Providers (Priorities)



- Privacy of my data
  - Address, Email,.. (Personally Identifiable Information)
  - Health, personal financial info
  - Personal Details (email, IMs,….)

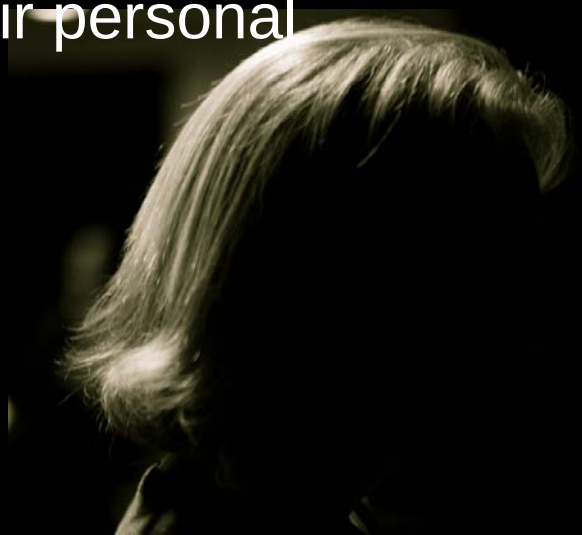
End Users

- **Keep Revenue Up/ Cost Down**
  - Push out the liabilities to user via Privacy and Acceptable Use Policy
  - Build Additional Services on users behavior (targeted advertisements) e.g. Google Email, banner adv.
  - Do minimal to achieve compliance
  - Keep their social applications more open (increased adoption)

Providers

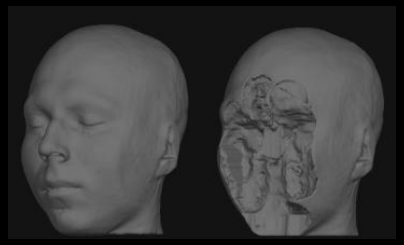
R5: Risks: User Privacy & Secondary Usage of Data

- User personal data mined or used (sold) without consent
  - Targeted Advertisements, third parties
- User Privacy data transferred across jurisdictional borders
- No opt out features for user (user can not delete data)
- Lack of individual control on ensuring appropriate usage, sharing and protection of their personal information.
- Law Obligation for providers
  - Key escrows to law agencies
  - Subpoena



R5: Mitigations: User Privacy & Secondary Usage of Data

Policy Enactment
- -Privacy and Acceptable Usage
- - Consent (Opt In / Opt Out)
- - Policy on Secondary Usage

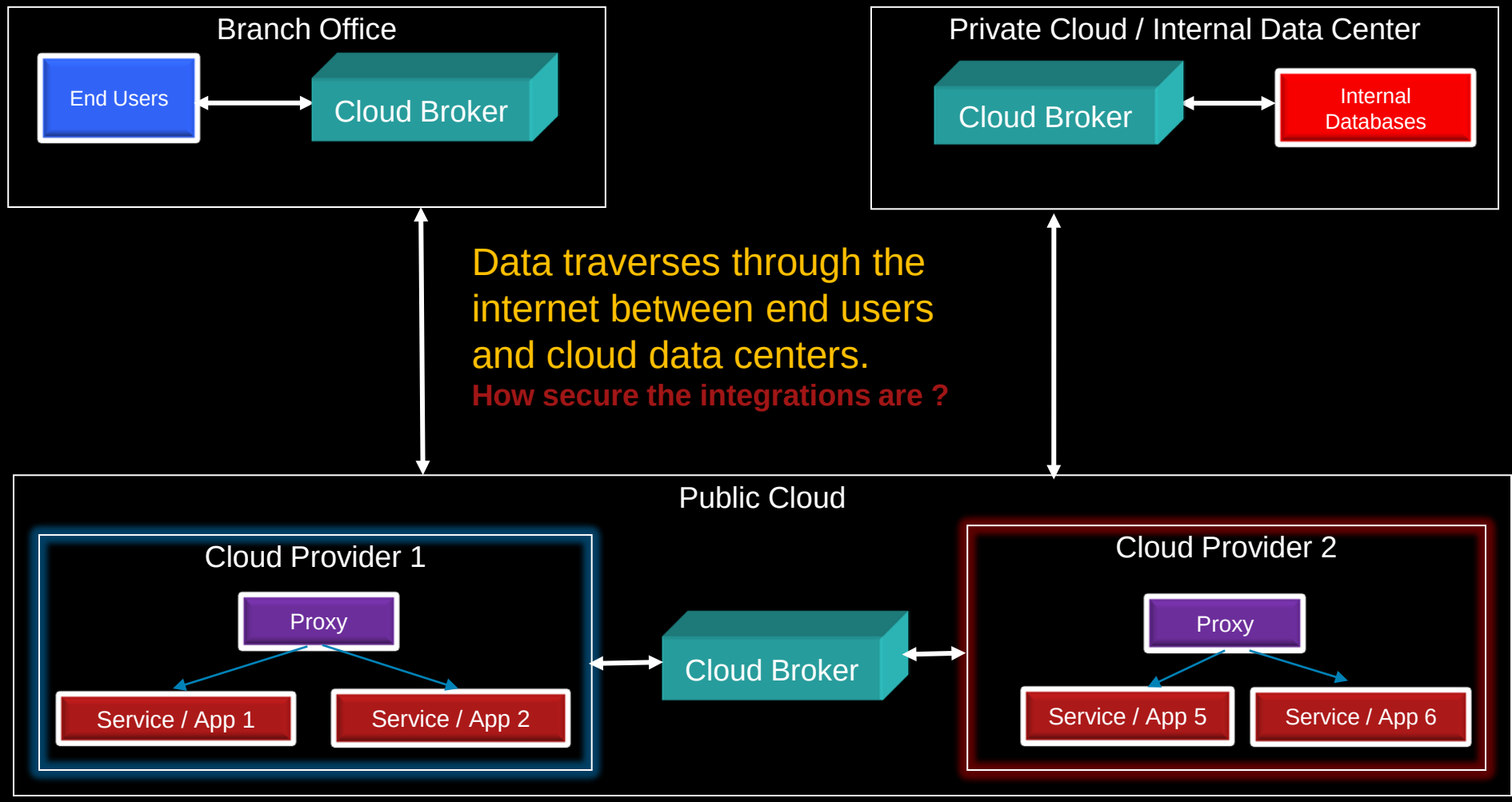


De-identification of personal Information

Encrypted storage

Terms of Service with providers
- Responsibility on compliance
- Geographical affinity

R6: Service & Data Integration



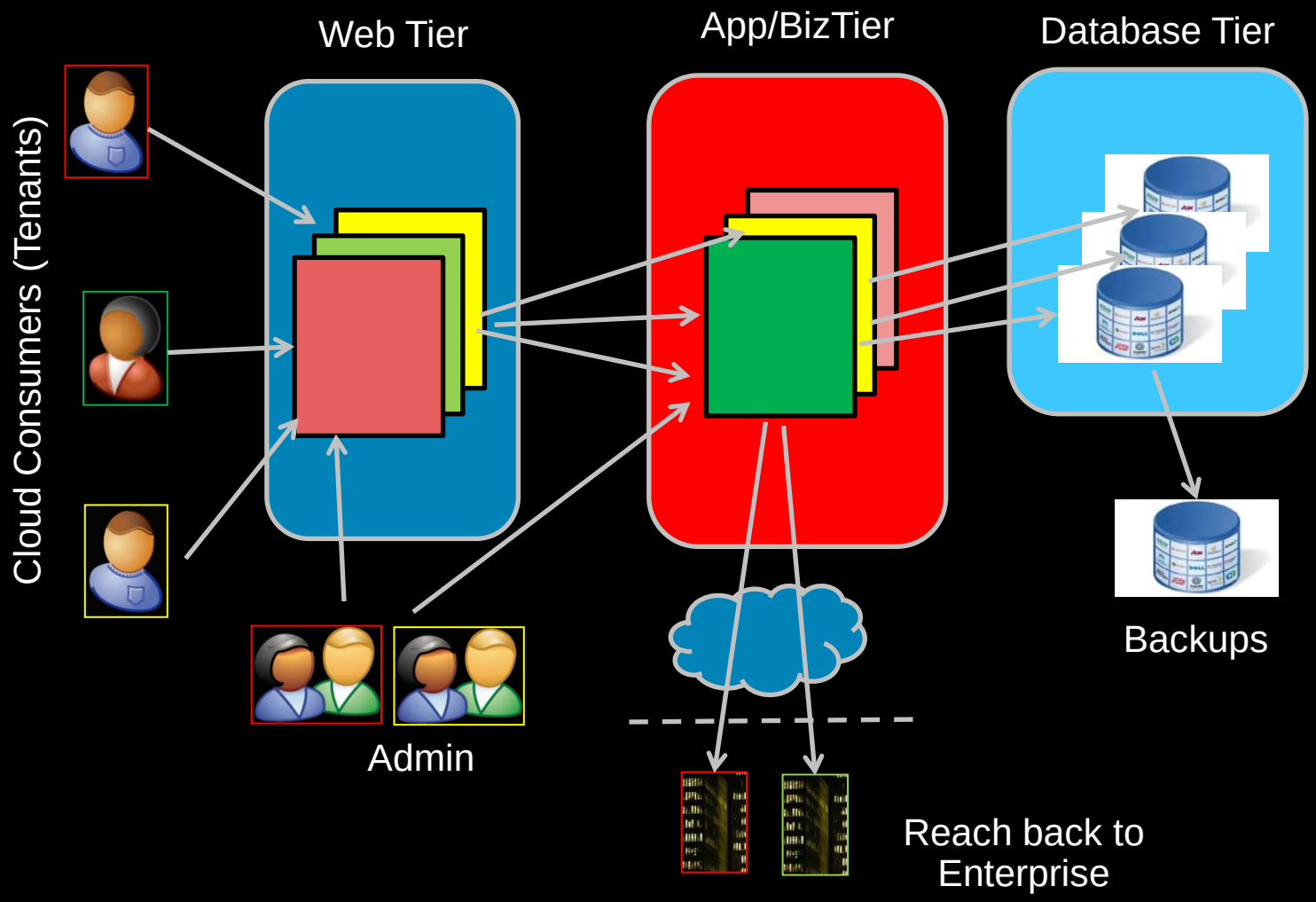
R6: Service & Data Integration – Mitigation Strategy

Data in Transit

Data at Rest

Encryption (keys, protocols etc)

R7: Risks: Multi-tenancy and Physical Security



Security Risks

1. Inadequate Logical Separations
2. Co-mingled Tenant Data
3. Malicious or Ignorant Tenants
4. Shared Service-single point of failures
5. Uncoordinated Change Controls and Misconfigs
6. Performance Risks

R7: Attacks and Incidences

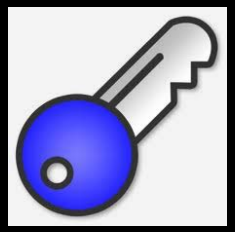
- MIT demonstrating cross-tenant attacks (Amazon EC2)*
  - Side channel Attacks
  - Scanning other tenants
  - DoS
- Wordpress Outage June 2010**
  - 100s of tenants (CNN,..) down in multi-tenant environment.
  - Uncoordinated Change in database

* http://chenxiwang.wordpress.com/2009/11/02/mit's-attack-on-amazon-ec2-an-academic-exercise/

** http://smoothspan.wordpress.com/2010/06/11/wordpress-and-the-dark-side-of-multitenancy/

R7: Mitigations: Multi-tenancy and Physical Security

Architecting for Multi-Tenancy



Data Encryption (per tenant key management)

Controlled and coordinated Change Management

Transparency/Audit-ability of Administrative Access

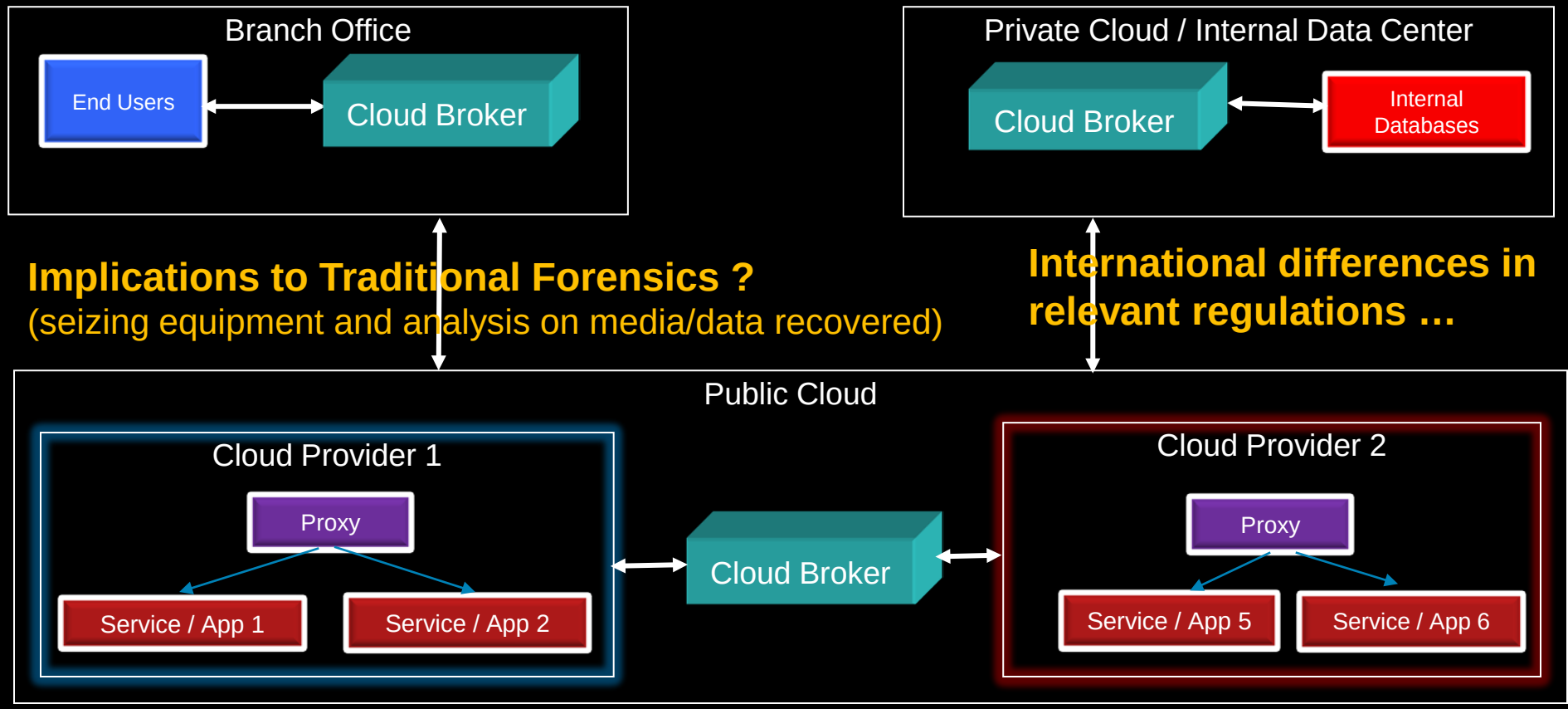
Regular Third Party Assessments

Virtual Private Cloud (VPC)

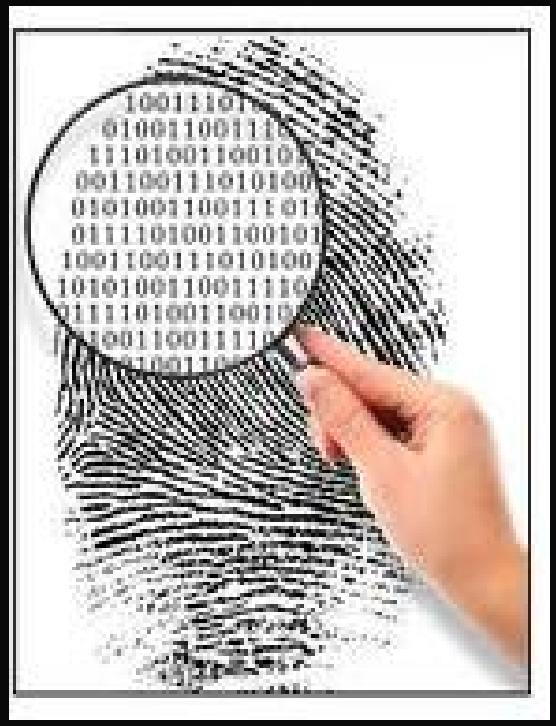
R8: Incidence Analysis & Forensic Support

Complex integration and dynamics in cloud computing present significant challenges to timely diagnosis and resolution of incidents such as:

- **Malware detection and**
- **Immediate intrusion response to mitigate the impact**



R8: Incidence Analysis & Forensic Support – Mitigation Strategy



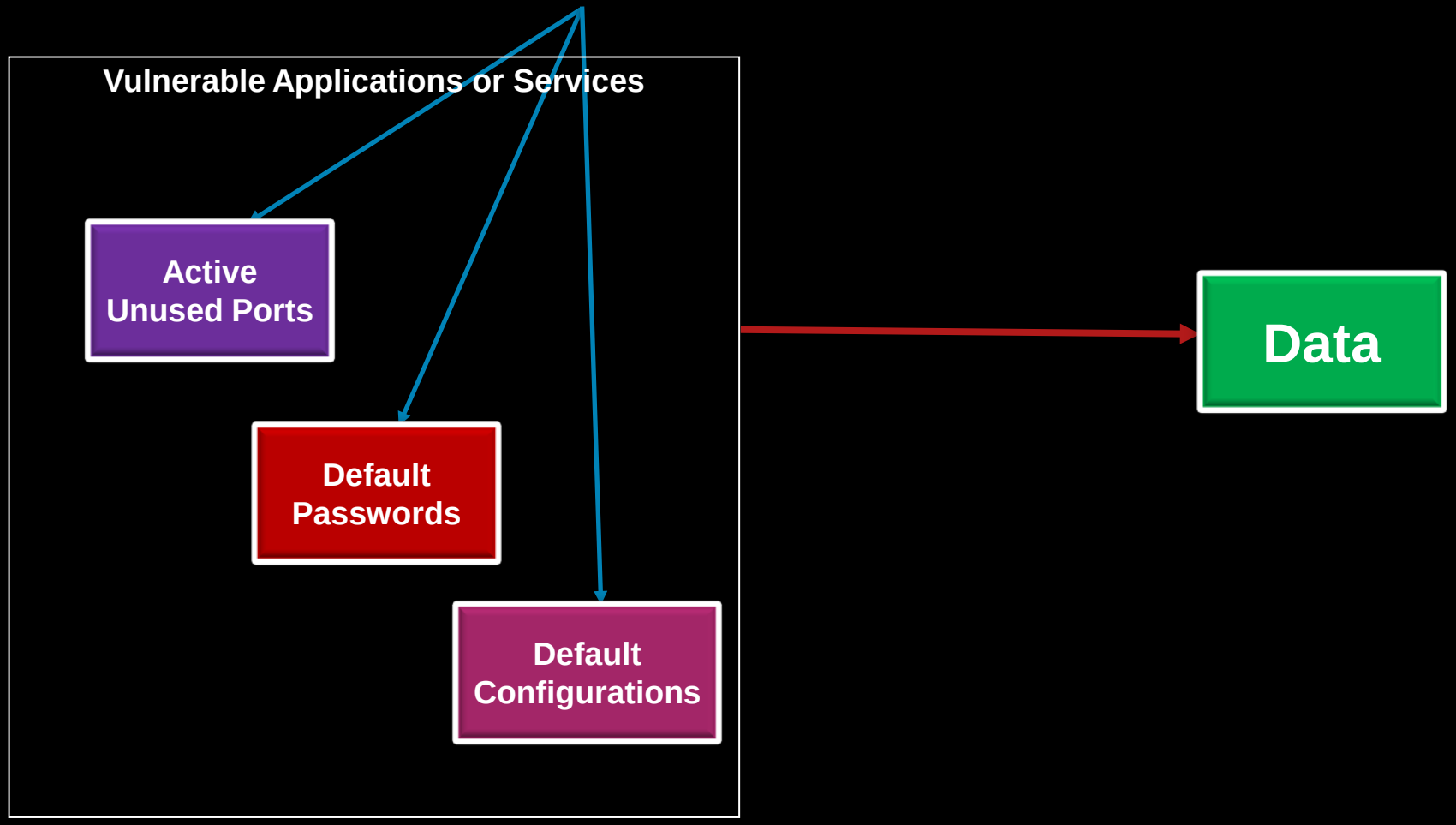
Dedicated Forensic VM Images

Comprehensive logging

Without compromising Performance

R9: Infrastructure Security

Malicious parties are actively scanning the internet for …



R9: Infrastructure Security - Mitigations

Segregation of duties and role based administrative privs

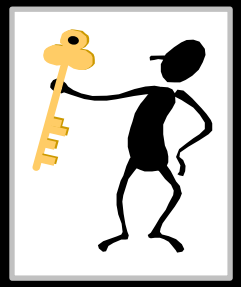
Third party audits and app vulnerability assessments

Tiered architecture with appropriate security controls between them

Hardening – Networks, OS, Apps

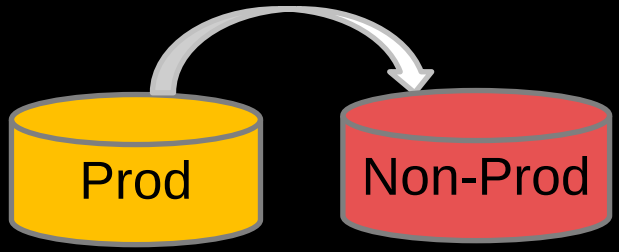
R10: Non-Production Environment Exposure

Non-Production Environments are …
used for design, development, and test activities internally within an organization

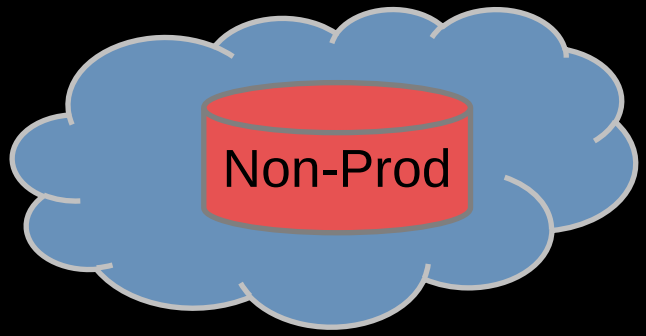


Typical non-prod environment use **generic** authentication credentials

Security flaws



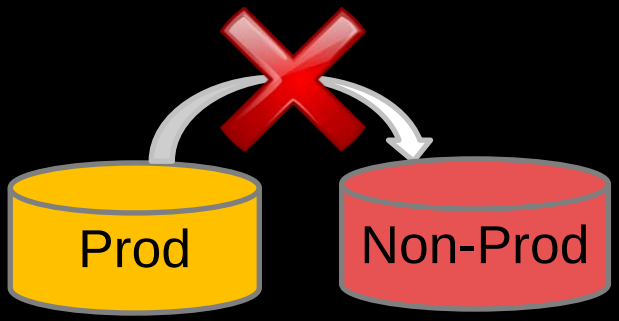
Data copied to non-prod from its production equivalent



High risk of an unauthorized user getting access to the non production environment

R10: Non-Production Environment Exposure
Mitigation

Use multi layers of authentication



Non-prod data is not identical to production

Don’t use cloud for developing a highly sensitive app in the cloud

Summary: Peaceful Sleep

- Photo - http://fineartamerica.com/featured/peaceful-sleep-ron-white.html

R5: Incidence: User Privacy & Secondary Usage of Data

Security

Google Fired Engineer for Privacy Violations

By: Brian Prince
2010-09-15
Article Rating: ★★★★★ / 4
Share This Article

Share 8 tweets retweet

There are 0 user comments on this Security story.

Google confirmed it fired an engineer for violating its privacy policies following a media report the employee had been let go for spying on the Google accounts of teenagers.

Rate This Article:
Poor ○ ○ ○ ○ ● Best
Rate

E-mail PDF Version
Print

Google confirmed today one of its engineers has been fired for violating the company's privacy rules.

The acknowledgment followed a media report that Google employee David Barksdale accessed the accounts of several teenagers in violation of Google policies. According to Gawker, Barksdale was let go in July for abusing his position as a site reliability engineer in Google's Kirkland, Wash., office by spying on the minors' Google accounts, including accessing Google Voice call logs records and Google Chat transcripts.

Barksdale was fired after Google received complaints about the situation, Gawker reported.

"Site reliability engineers [SREs] are responsible for a variety of tasks, including responding to technical problems across Google's product portfolio, and as such have unfettered access to users' accounts for the services they oversee," Gawker quoted a former Google SRE as saying.

In a statement, Bill Coughran, senior vice president of engineering at Google, said Barksdale had been fired for "breaking Google's strict internal privacy policies."

Consumer groups hammer Facebook privacy violations in federal complaint

FTC urged to overturn recent Facebook privacy changes

By Jon Brodkin, Network World
May 06, 2010 03:35 PM ET

Share/Email Tweet This Comment Print Newsletter Sign-Up

Facebook users were shocked to learn this week that private chats could have been viewed by their friends because of a security hole that was only recently closed, and also that new Facebook features can secretly add applications to your profile.

Facebook, Twitter becoming business tools, but CIOs remain wary

But those weren't the only privacy complaints Facebook faced this week. On Wednesday, the Electronic Privacy Information Center filed a 38-page complaint against the company with the Federal Trade Commission, demanding that Facebook cancel new features introduced in mid-April that compel users to share more information than before.

White Paper
FREE Download: Max server performance with Diskeeper Server: Download now

"Facebook now discloses personal information to third parties that Facebook users previously did not make available," EPIC said in its complaint. "These changes violate user expectations, diminish user privacy, and contradict Facebook's own representations. These business practices are Unfair and Deceptive Trade Practices."

Related Content
- Facebook security flaw makes private chats public
- Facebook Privacy Changes: 5 Can't-Miss Facts
- Facebook's $9.5M privacy settlement not good enough

In response to the FTC complaint, a Facebook spokesman said, "Our new features are providing beneficial new social experiences to people around the world that are transparent,