Everything You Need to Know About Cloud Security in 30 Minutes or Less

Rich Mogull
Securosis, L.L.C.

A long time ago...

You know, 2008

Securosis

In a galaxy far far away

You know, the Internet

(Where all the porn is)

Securosis

These guys...

Securosis

Securosis

Said, “Hey, we need the next big thing.”

securosis

So this guy

Securosis

Securosis

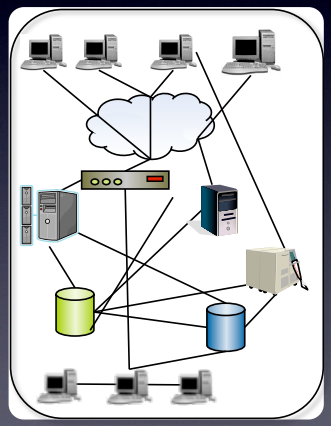
Said....

Securosis

“Hey, you know all those complicated diagram thingies customers are showing us?”

Securosis

Like this?



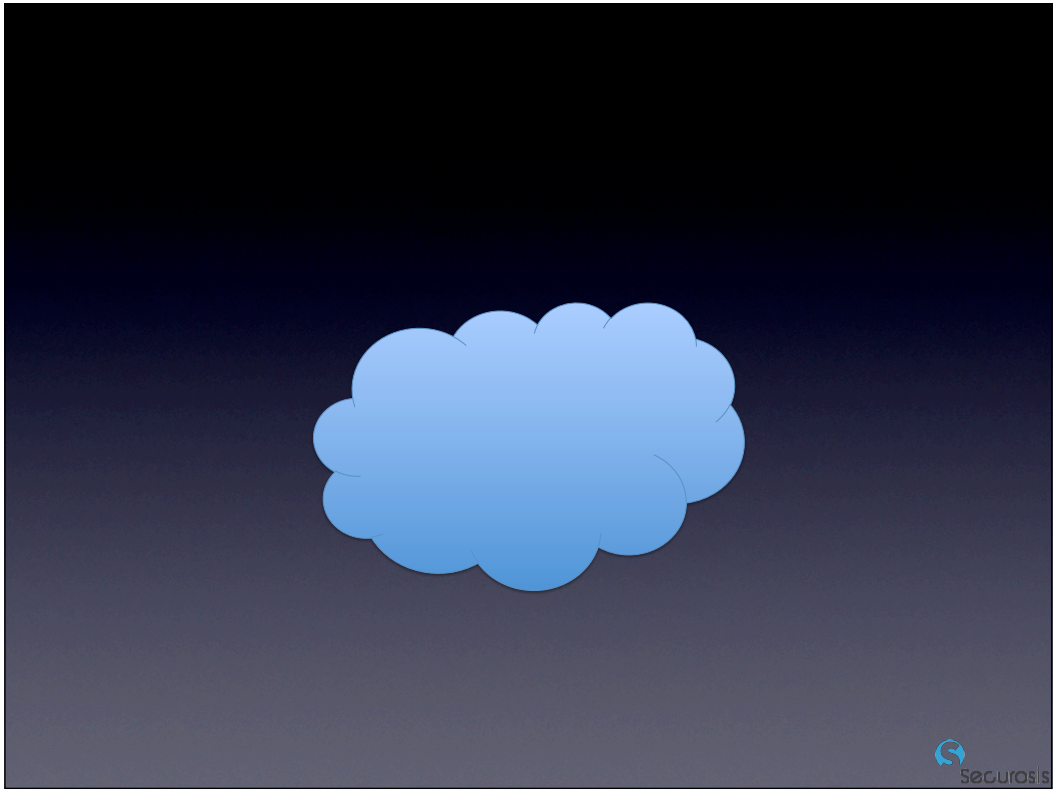
Securosis

Notice something?

Securosis

They all have one of these

Securosis


Securosis

And I've never seen a customer with one, so let's sell them *that*!

Securosis

Woah

Securosis

Securosis

We can totally sell that!

Securosis

Securosis

And thus THE CLOUD was born.

Securosis

And there was much rejoicing.

Securosis

Securosis

Unless, of course, you were in IT security.

Securosis

And your developers
told you they moved
everything to the cloud.

Securosis

Last week.

Securosis

In which case, it was more like this...

Securosis

Securosis

Why the cloud is a problem for security

- Poor understanding of cloud taxonomies and definitions.
- A generic term, frequently misused to refer to anything on the Internet.
- Lack of visibility into cloud deployments.
- Organic consumption.

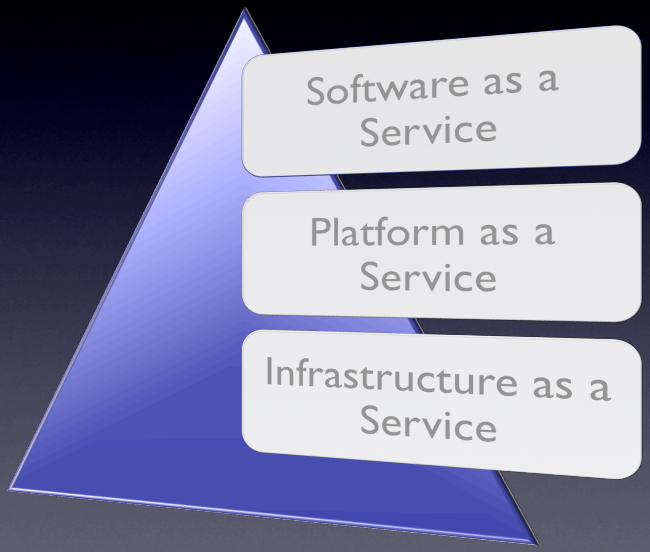
Securosis

The CSA 5 Principle Characteristics of the Cloud

- Abstraction of Infrastructure
- Resource Democratization
- Services Oriented Architecture
- Elasticity/Dynamism of Resources
- Utility model of Consumption & Allocation

Securosis

Three Delivery Models

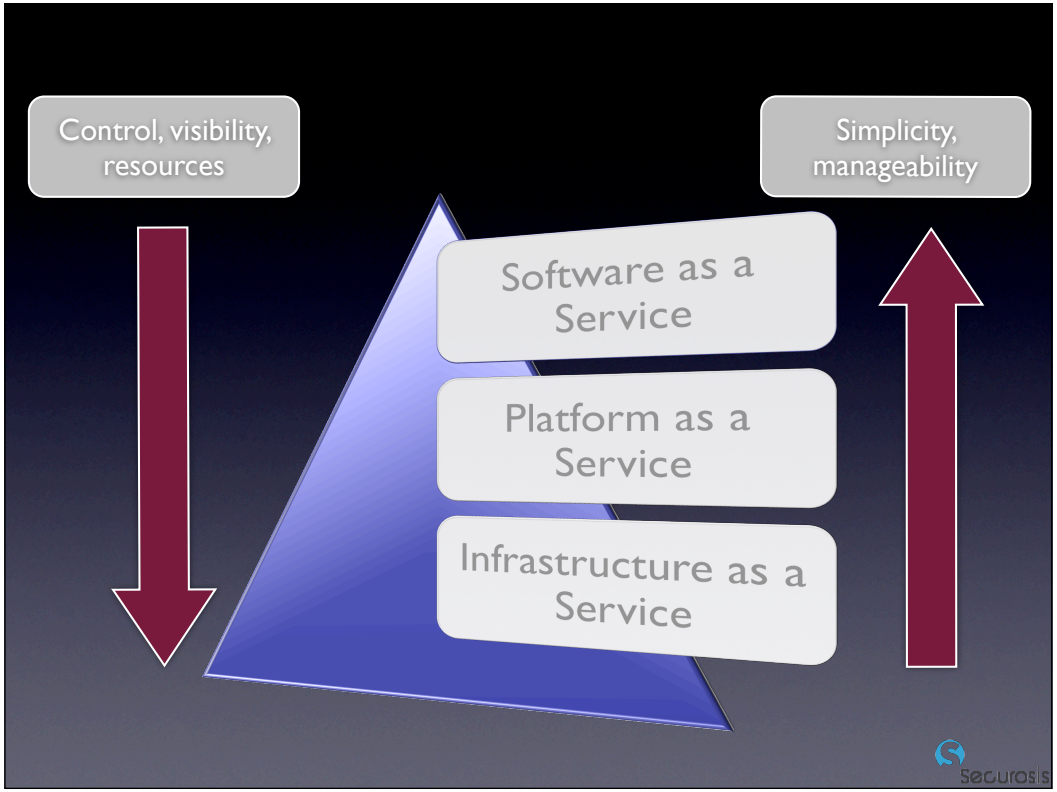


Securosis

Security Implications

- Variable control.
- Variable visibility.
- Variable simplicity.
- Variable resources.

Securosis


Control, visibility, resources
Simplicity, manageability
Software as a Service
Platform as a Service
Infrastructure as a Service
Securosis

But is the cloud more or less secure than we are now?

Securosis

It depends

Securosis

SaaS

- Most constrained.
- Most security managed by your provider.
- Least flexible.

Securosis

PaaS

- Less constrained.
- Security varies tremendously based on provider and application- shared responsibility.
- Security responsibility

Securosis

IaaS

- Most flexible.
- Most security managed by your developers.

Securosis

Specific issues

- Spillage and data security.
- Reliability/availability.
- Capability to apply traditional security controls in a dynamic environment.
- Lack of visibility into cloud usage.
- Changing development patterns/cycles.

Securosis

For example, where do you stick the WAF?

Securosis

Is vulnerability scanning your cloud legal?

Securosis

How do you use your static and dynamic analysis testing tools in the cloud?

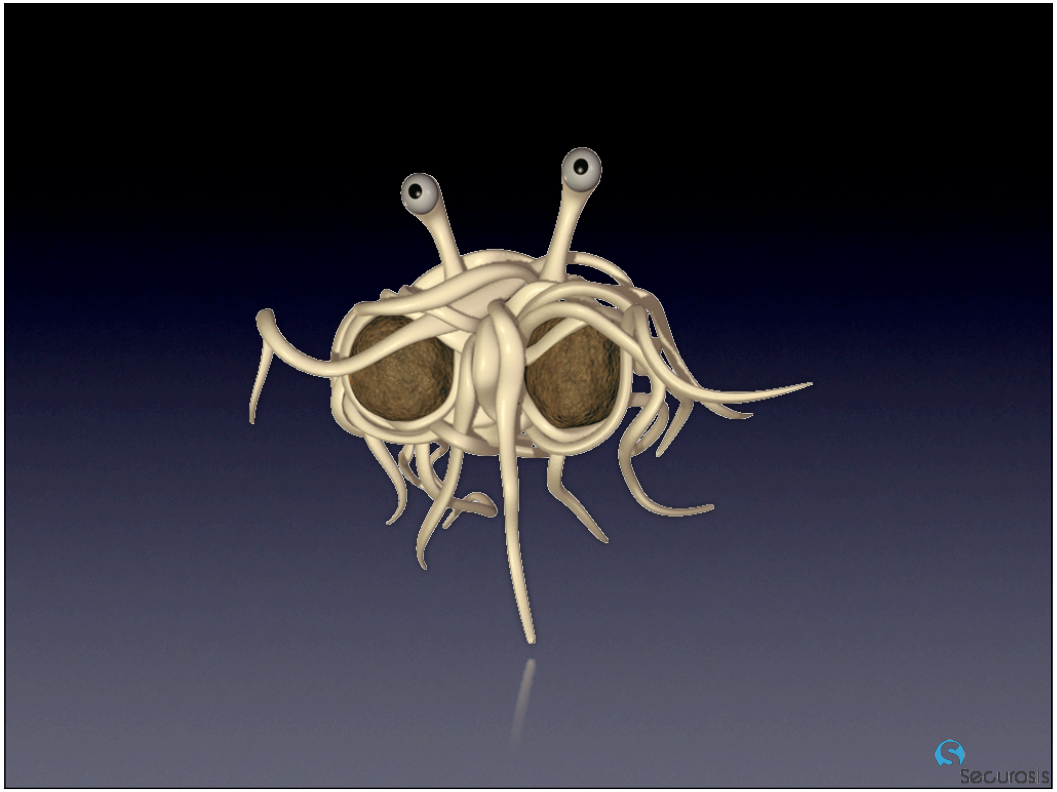
Securosis

Where do you roll the cloud when it fails?

Securosis

How most organizations secure their clouds today...

Securosis


Securosis

Your Top 2 Cloud Security Defenses

Service Level Agreements

Security Understanding

Securosis

Understand Your SLAs

- Are there security-specific SLAs?
- Can you audit against those SLAs?
- Are there contractual penalties for non-compliance?
- Do your SLAs meet your risk tolerance requirements?

Securosis

Suggested SLAs

- Availability.
- Security audits- including third party.
- Data security/encryption.
- Personnel security.
- Security controls (depend based on service).
- User account management.
- Infrastructure changes.

Securosis

Understand Your Cloud

- What security controls are in your cloud?
- How can you manage and integrate with the controls?
- What security documentation is available?
- What contingency plans are available?

Securosis

Cloud Security Controls to Look For

- Data encryption/security (key management).
- Perimeter defenses.
- Auditing/logging.
- Authentication
- Segregation.
- Compliance.

Securosis

Cloud Security Macro Layers

- Network
- Service
- User
- Transaction
- Data

Securosis

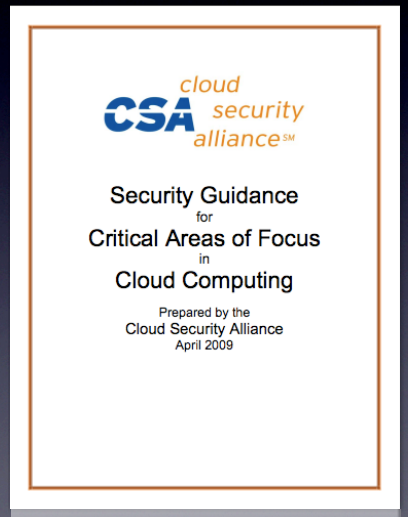
Don't Trust

- SAS70 Audits.
- Documentation without verification.
- Non-contractual SLAs.
- Anything not in writing, with penalties for non-compliance.
- Anything you don't understand.

Securosis

Resources

- Cloud Security Alliance
- Jericho Forum
- NIST



Securosis

What to Do

- Educate yourself.
- Engage with developers.
- Develop cloud security requirements.
- Understand risk/controls tradeoffs.
- Document and engage management.

Securosis

The 5 Stages of Cloud Computing Grief

- Denial: There is no cloud.
- Anger: Why the f&*k is this sales guy trying to sell me a cloud?
- Bargaining: Can you please just tell me what the f&^k your cloud is?
- Depression: The sales guy found my CIO. Now I have to by a cloud.
- Acceptance: There is no cloud.

Securosis

Securosis

Rich Mogull

Securosis, L.L.C.

securosis.com
rmogull@securosis.com
Twitter: rmogull
Skype: rmogull