

# *Cloudification*

*Indiscriminate Information Intercourse Involving Internet Infrastructure*

# ::Agenda

- Cloud Defined ::  
*Talking Heads & Shark Jumping*
- Heart Of Darkness ::  
*Corrosive (t)Rust*
- Cloudifornication ::  
*Stacked Turtles & Pwnage*

# ::Setting Some Context

*Cloud Computing is a natural,  
disruptively innovative and timely  
opportunistic response to a converging  
set of socio-economic, political, cultural  
and technological stimuli\**

\*It's also a really good marketing job...

# ::Setting Some Context

Cloud is an adaptive **operational model**, not a particular technology and there are lots of different Clouds.

This talk focuses on Public Clouds



## ::Setting Some Context

These Clouds are often operated via  
**mega datacenters** interconnected  
using **shared utilities**, logically  
provided & **operated by other**  
**providers** & in many cases using the  
Internet

# ::Setting Some Context

*The Internet is a remarkably frail operating platform, loosely hinged on luck, politeness, ad hoc peering & transit, handshake relationships and the IP Protocol\**

\*It's up more than it's down because even the bad guys need it up to operate...

## *::Setting Some Context*

*At the end of the day, we're adding  
layers of abstraction/indirection to  
40 year old technologies and  
practices & wondering why we still  
have issues*

*:: Context*

*The Internet assumes a fictional  
trusted core but is in fact an  
untrusted, unreliable & hostile  
platform.*

*So then, is Cloud.*

IF It All Comes Down To Trust...



What are we going to differently about who  
we trust, how and why?

*Cloud Defined ::*

*Talking Heads & Shark Jumping*



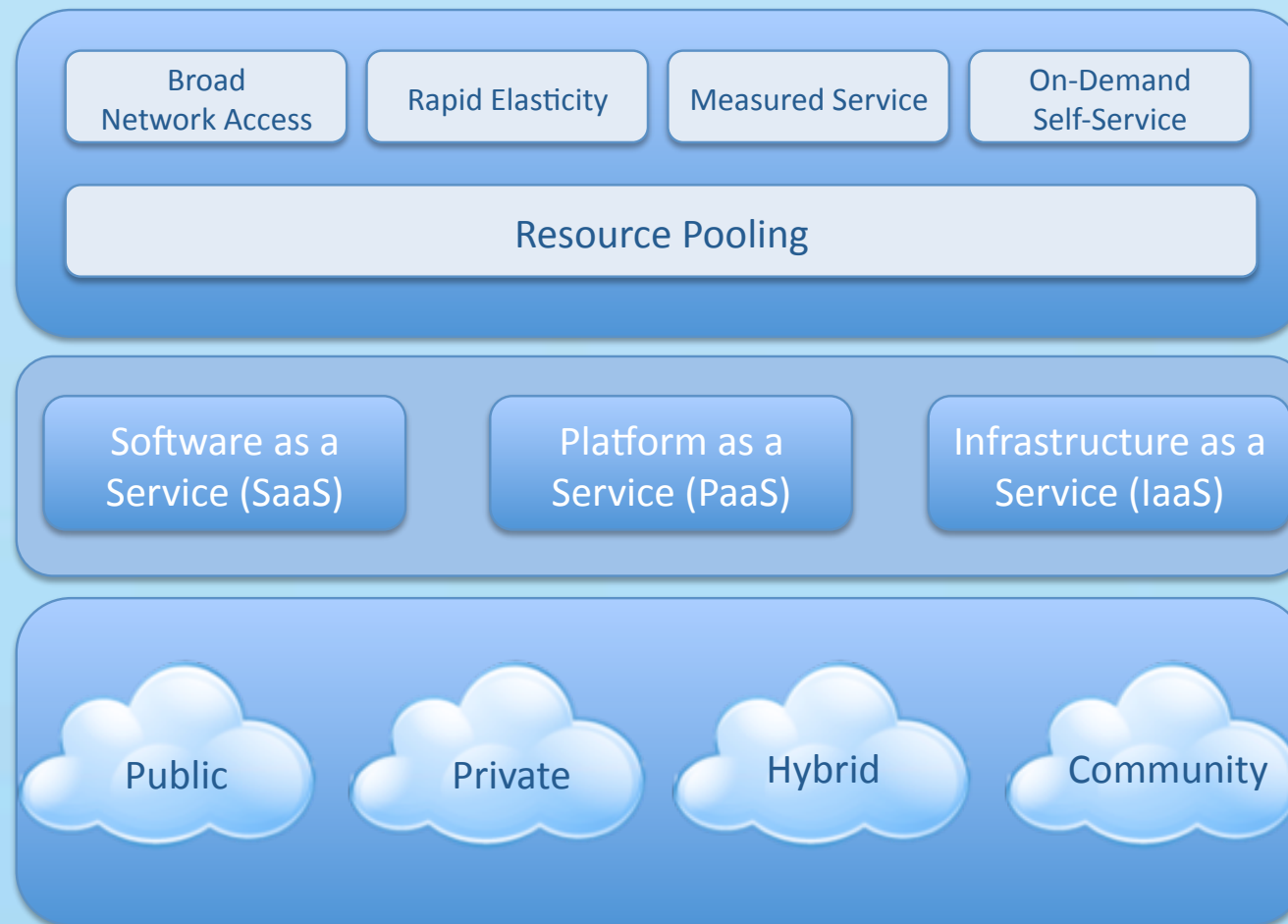
*What the !@#%& IS Cloud Computing?*



# Provider's/Technician's View

Visual Model Of NIST Working Definition Of Cloud Computing

<http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html>



**Abstraction of Infrastructure**

**Resource Democratization**

**Services Oriented**

**Self-Service, On-Demand  
Elasticity/Dynamism**

**Utility Model Of Consumption  
& Allocation**





# *Key Ingredients In Cloud Definition*

- *Abstraction of Infrastructure*
- *Resource Democratization*
- *Services Oriented*
- *Self-Service, On-Demand Elasticity/  
Dynamism*
- *Utility Model Of Consumption & Allocation*

*From the Consumer's Perspective...*



Everything Is Cloud...



*CloudWow! You'll Say "HOW?" Every Time...*



# *The Journey to the InterCloud*



*Begins With a Single Slide, It Does...*

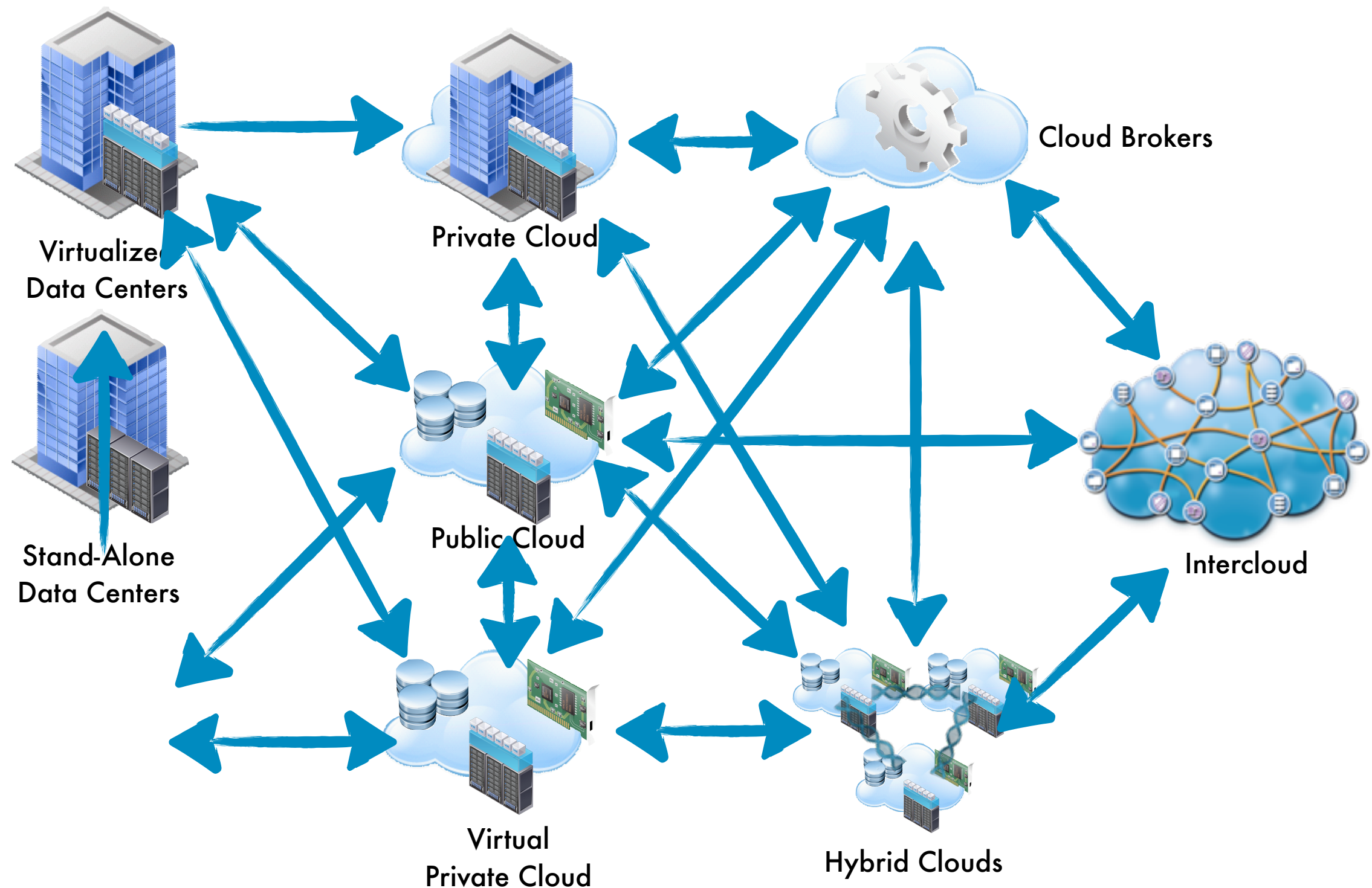
*...It Ends With One, Too...*



*...and Here It Comes...*

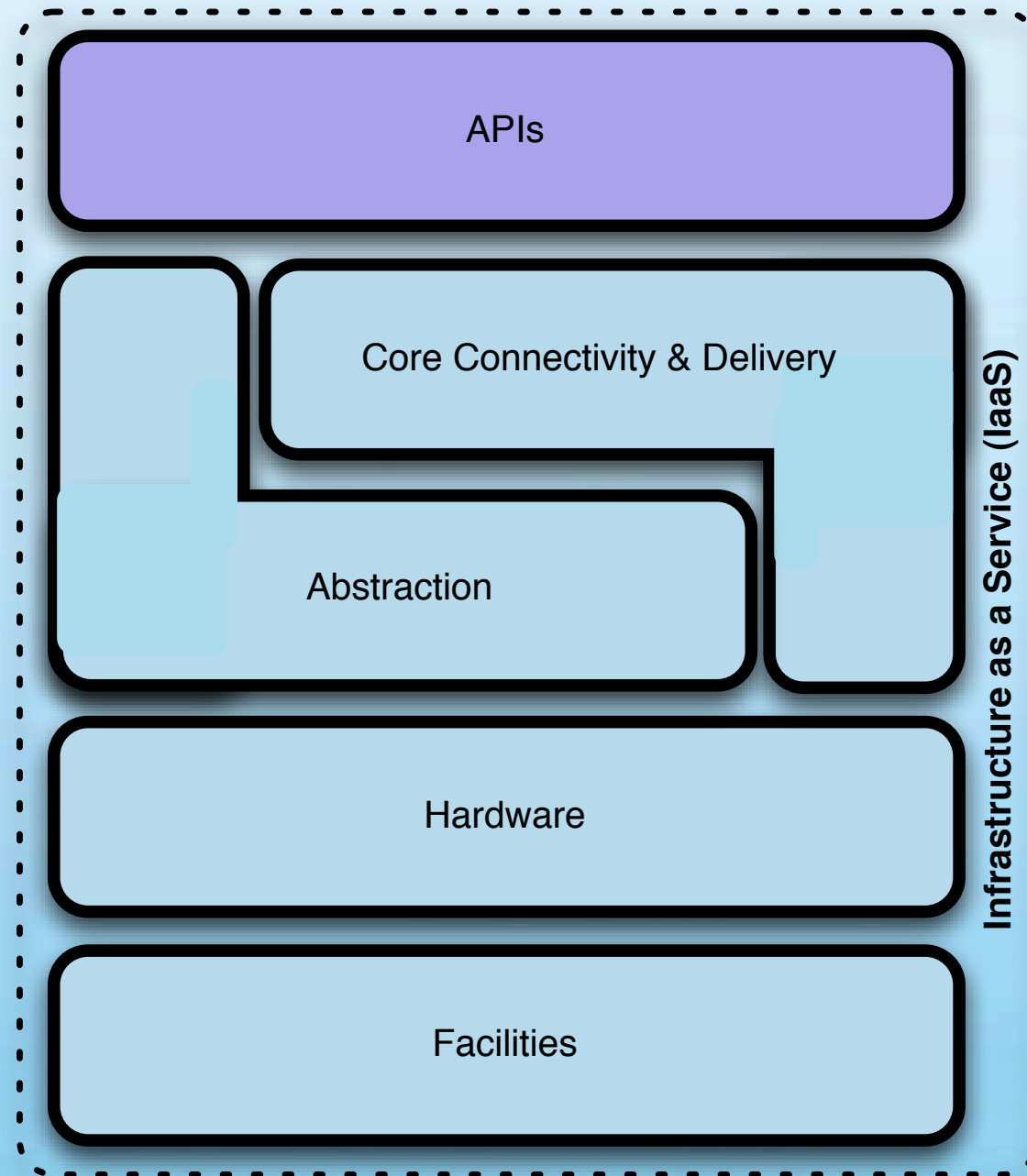


# Journey To The Intercloud Made Simple

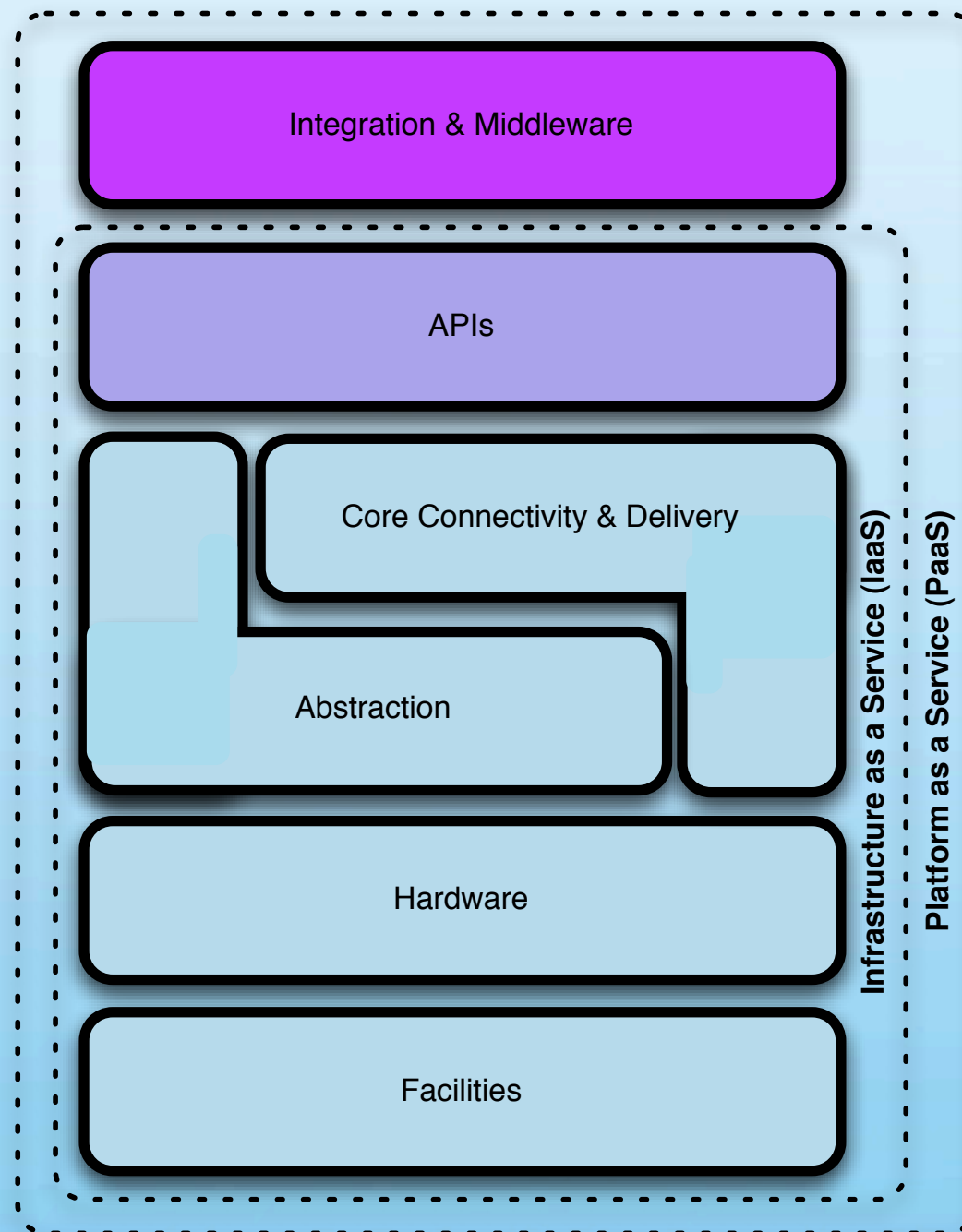


Federation / Workload Portability / Interoperability

# Cloud Model :: Infrastructure as a Service (IaaS)

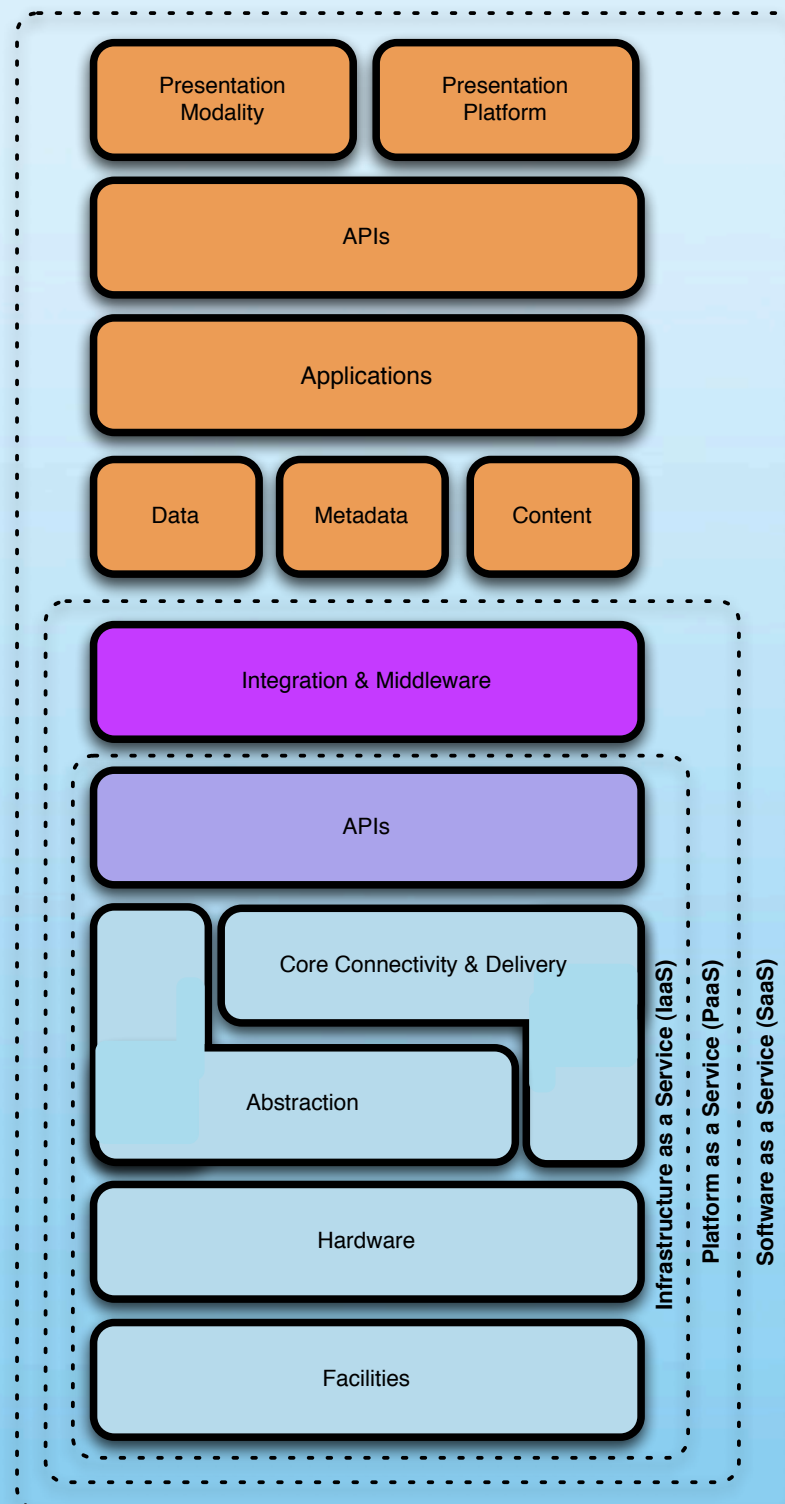


# Cloud Model :: Platform as a Service (PaaS)





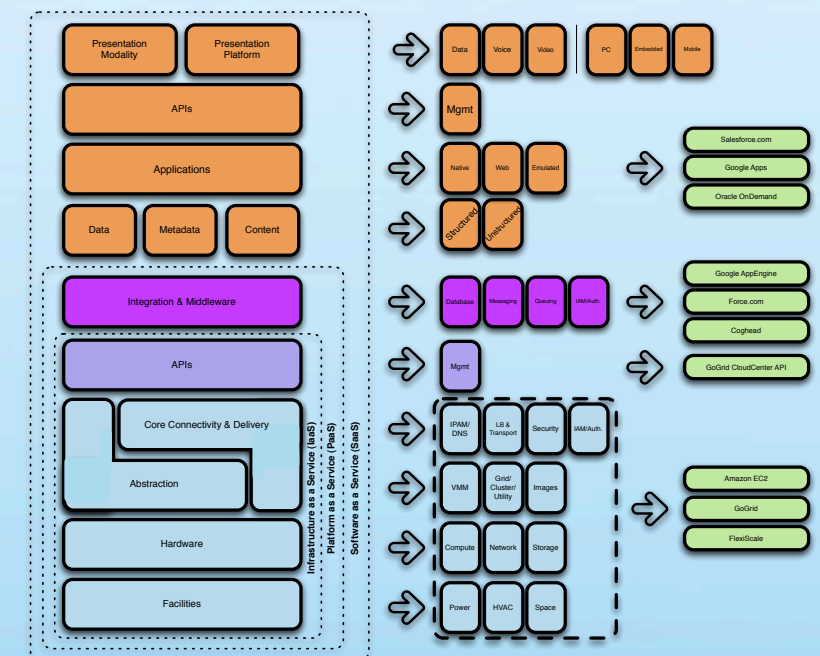
# Cloud Model :: Software as a Service (SaaS)



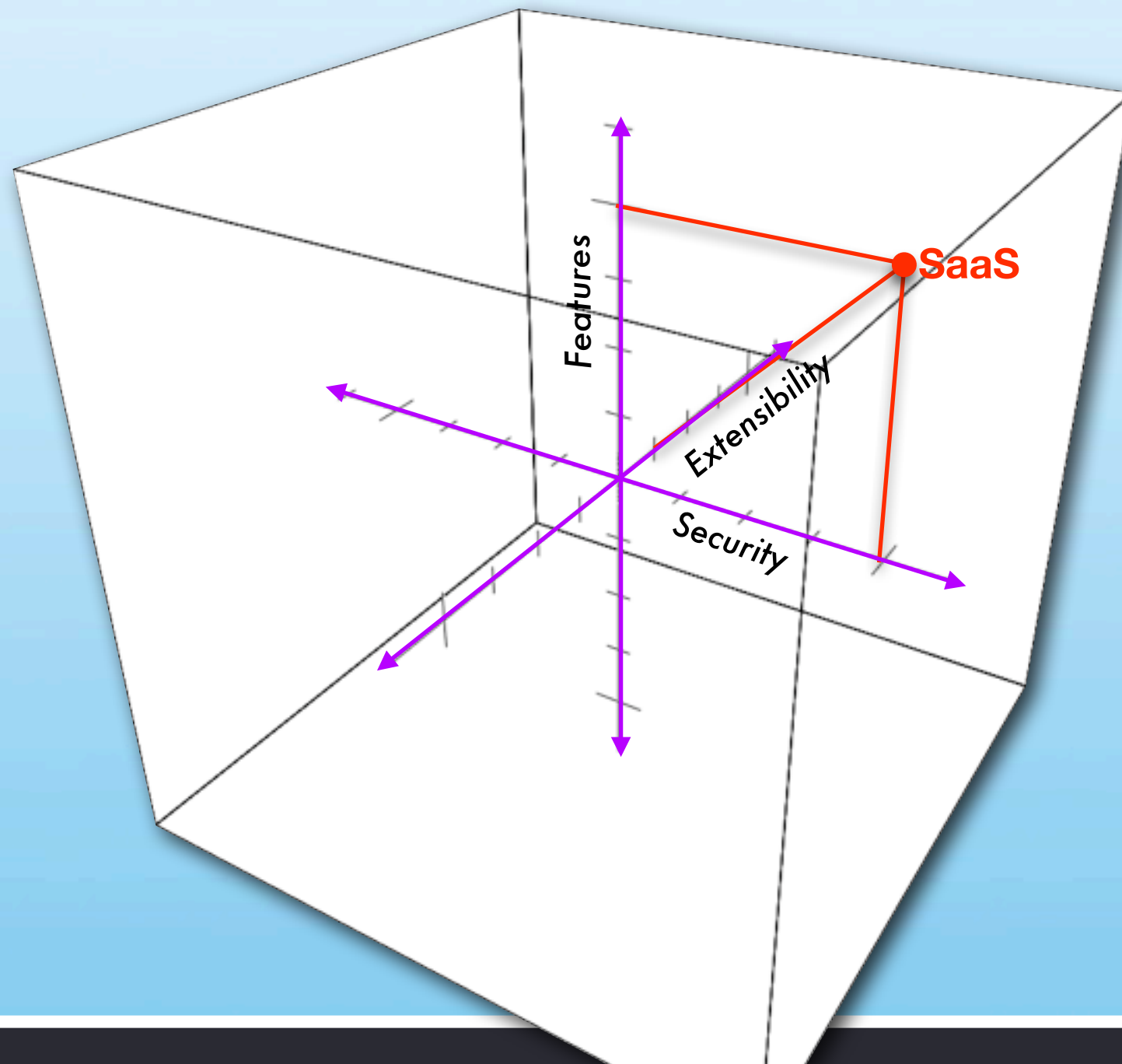
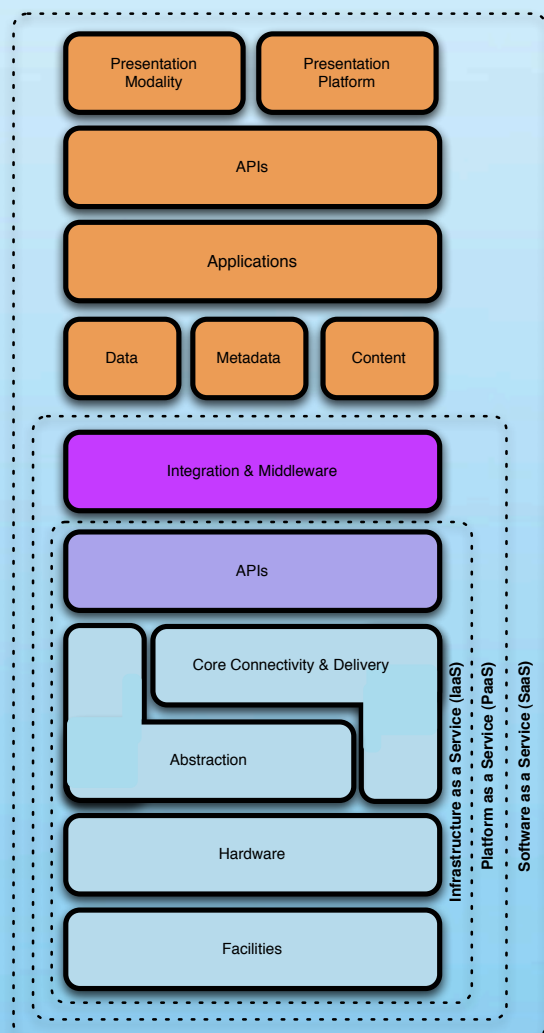
# Lots Of \*aaSes...Variations On a Theme

Packaging these up in combination yields lots of \*aaS(es):

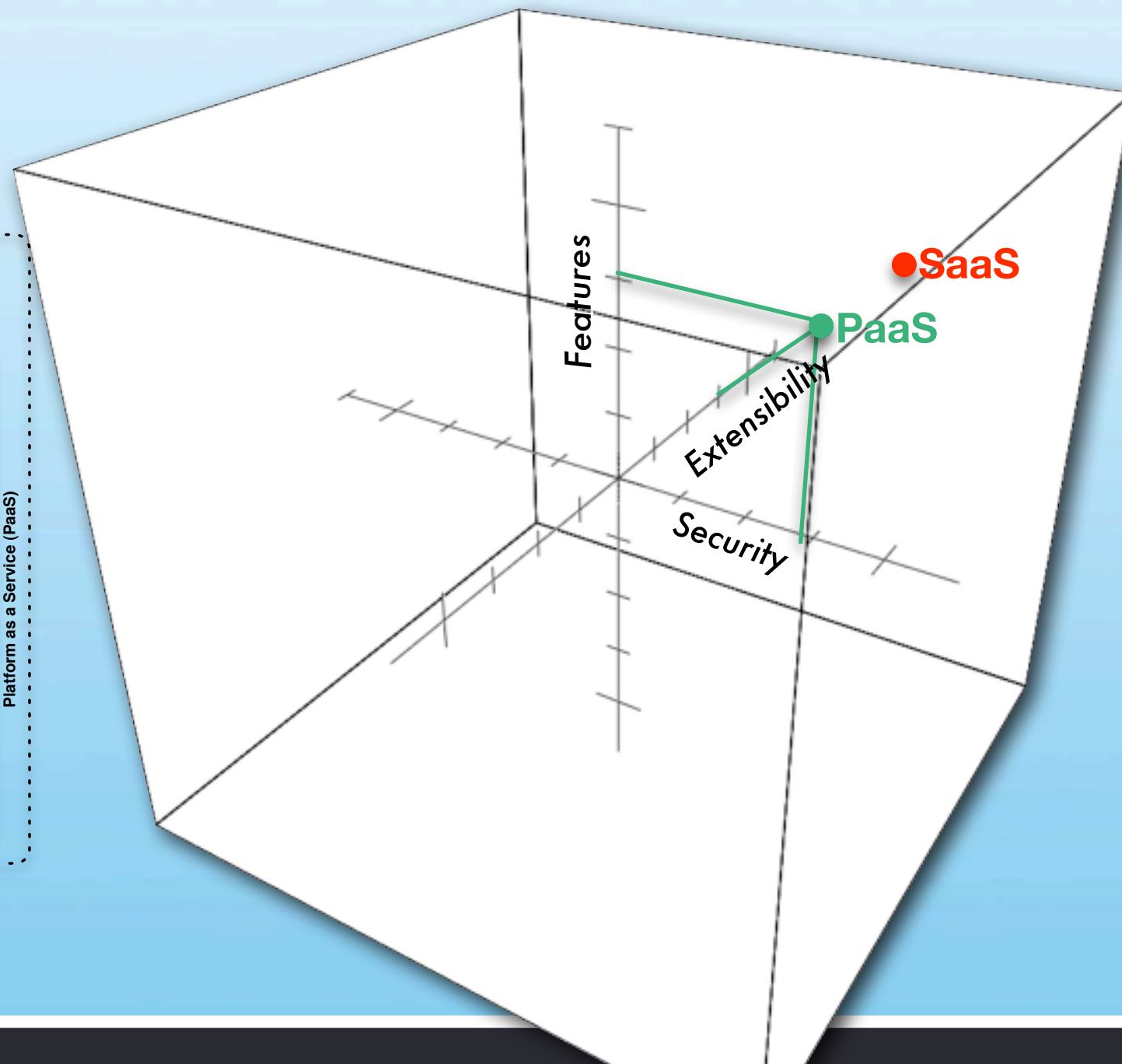
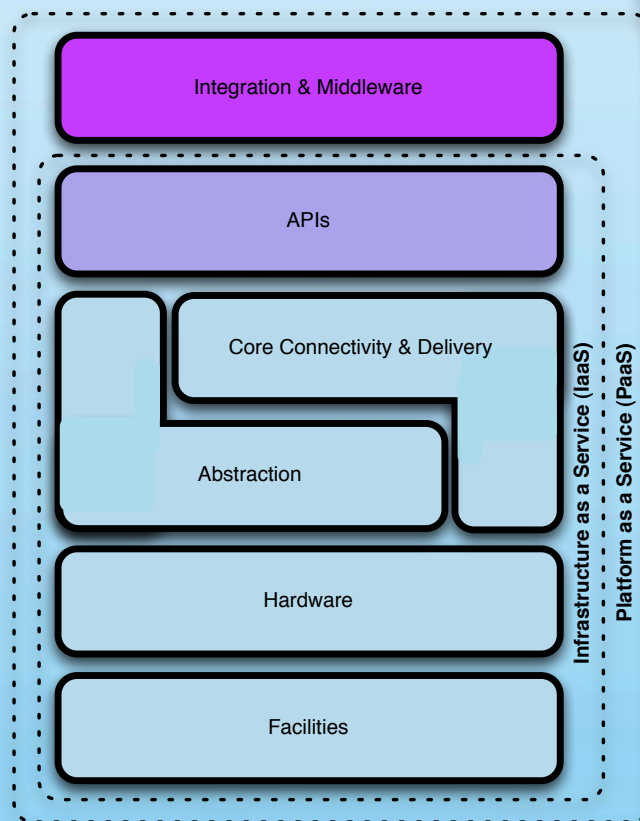
- Storage as a Service
- Database as a Service
- Information as a Service
- Process as a Service
- Integration as a Service
- Security as a Service
- Management as a Service
- Testing as a Service...



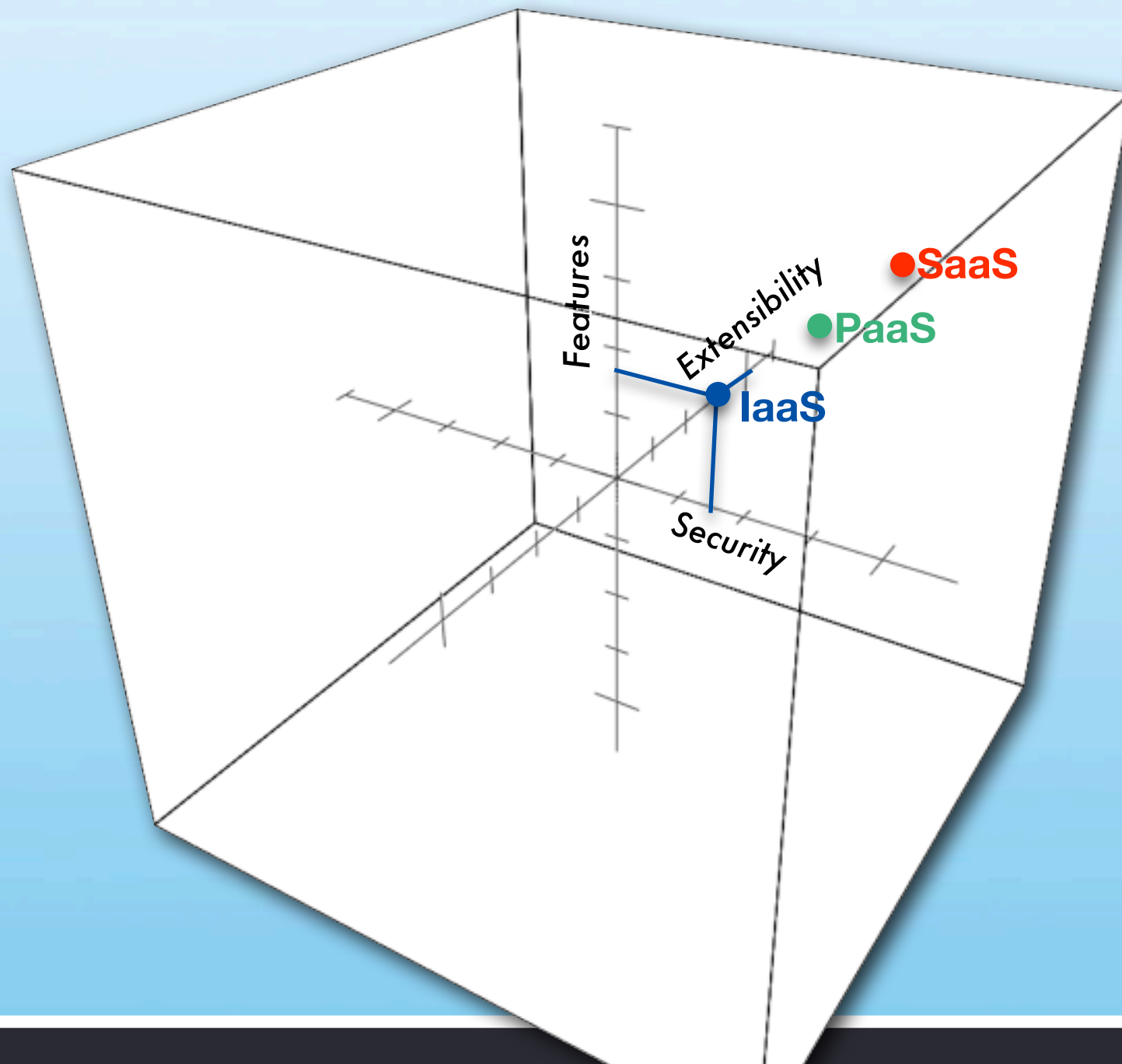
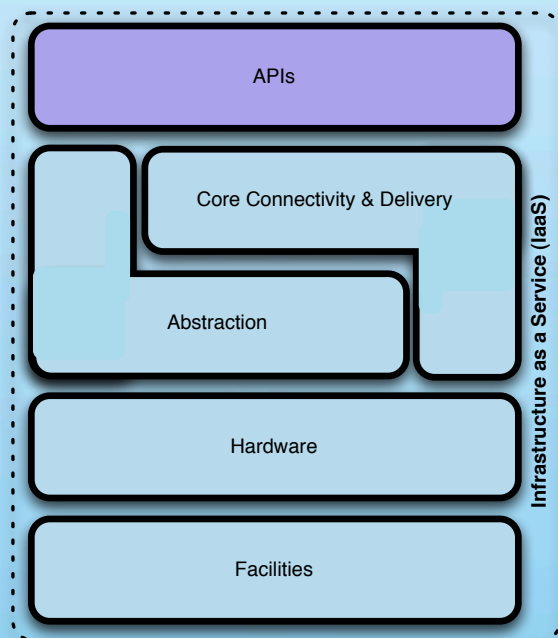
# The Many Dimensions Of Cloud :: SaaS



# The Many Dimensions Of Cloud :: PaaS



# The Many Dimensions Of Cloud :: IaaS



# *:: The Cloud Journey & It's Impact On Security and Vice-Versa*



# The SPI Cloud Model

Three delivery models that people talk about about when they say "Cloud":

Software as a Service  
(SaaS)

Platform as a Service  
(PaaS)

Infrastructure as a Service  
(IaaS)

End Users

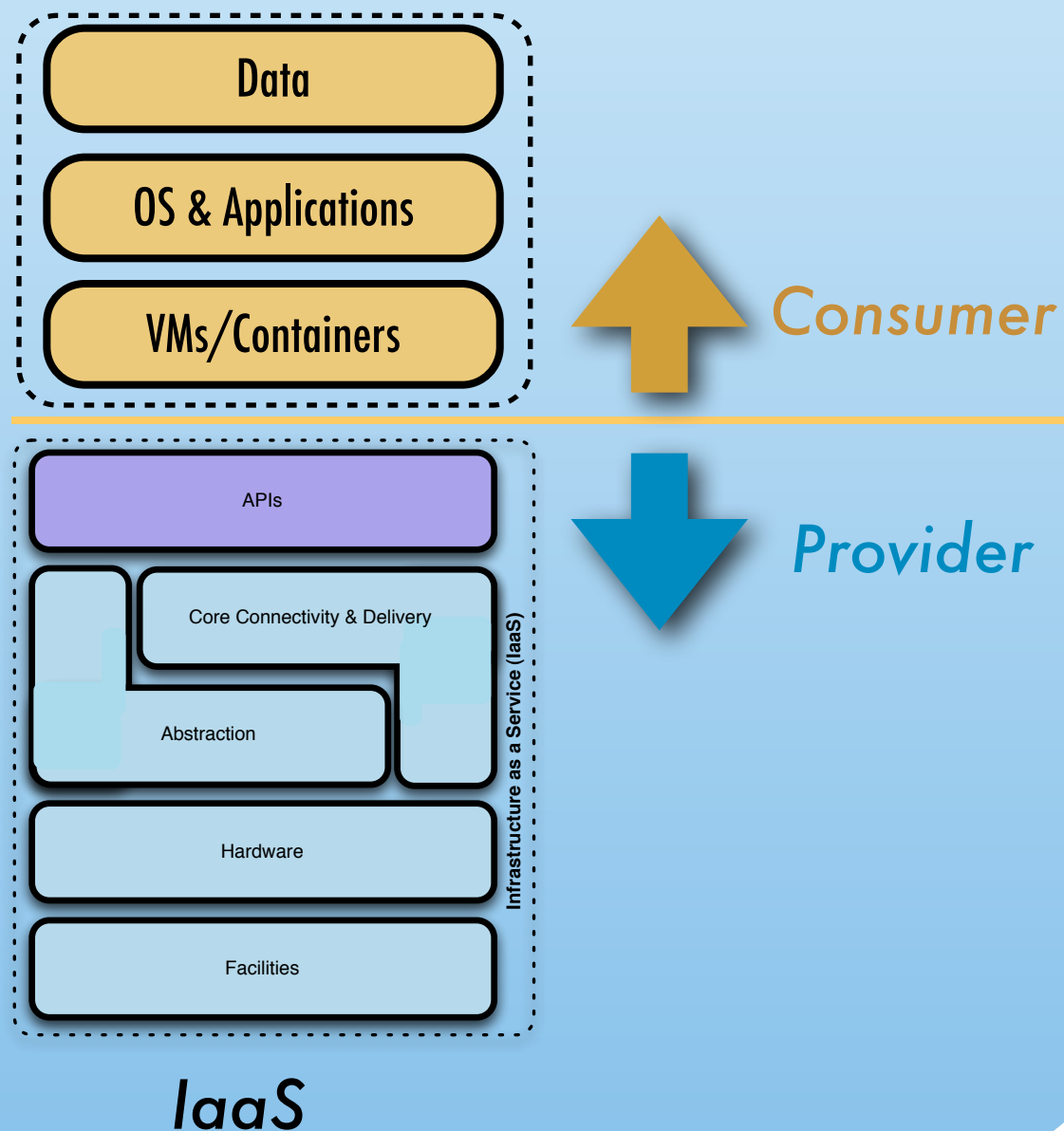
Developers

SysAdmins

What Do These  
Look Like?



# IaaS Security :: Guest/Host-Based



- Provider secures "their" infrastructure to maximize availability & multi-tenancy
- Remainder of the stack (and confidentiality, integrity) is your problem
- General focus is on VM's & Guest-Based



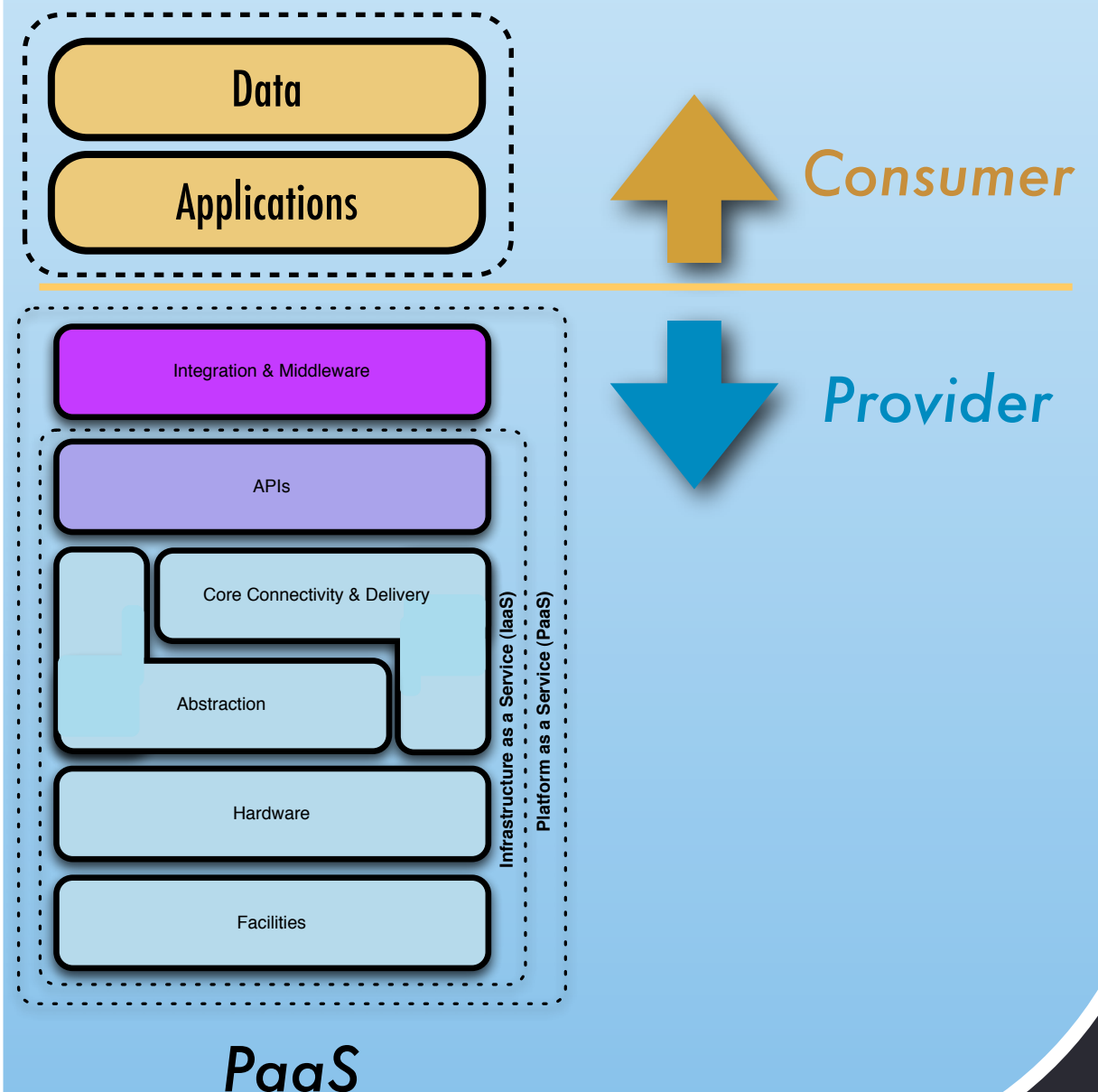
*All You, Baby...*

7.2. Security. We strive to keep Your Content secure, but cannot guarantee that we will be successful at doing so, given the nature of the Internet...you acknowledge that **you bear sole responsibility for adequate security, protection and backup of Your Content and Applications...**We will have no liability to you for any unauthorized access or use, corruption, deletion, destruction or loss of any of Your Content or Applications.



# PaaS Security :: Programmatic

- Provider owns the compute, network, storage layers & programmatic interface security
- The consumer creates the applications based upon supported development environment
- Writing secure applications and ensuring your data is safe is on you

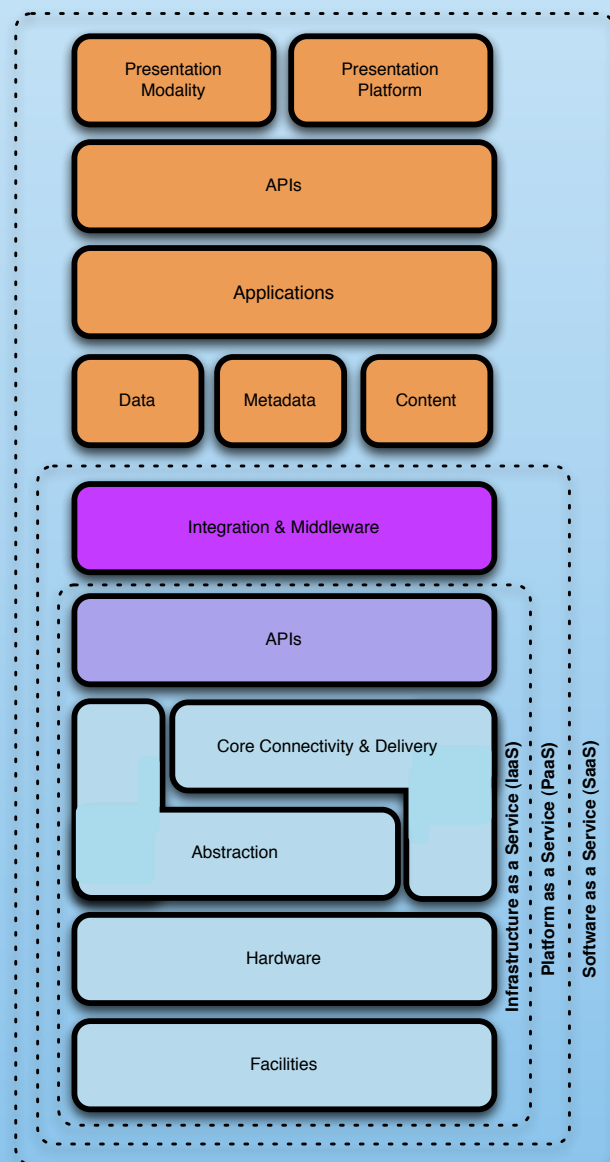


## *Oh, Passwords?*



2.1. You must provide accurate and complete registration information any time you register to use the Service. **You are responsible for the security of your passwords and for any use of your account.** If you become aware of any unauthorized use of your password or of your account, you agree to notify Google immediately.

# SaaS Security :: All or Nuthin'



*Provider*

**SaaS**

- The provider owns the entire stack
- Security (C, I and A) becomes a contract negotiation
- Traditional security and compliance functions are more administrative & policy-focused

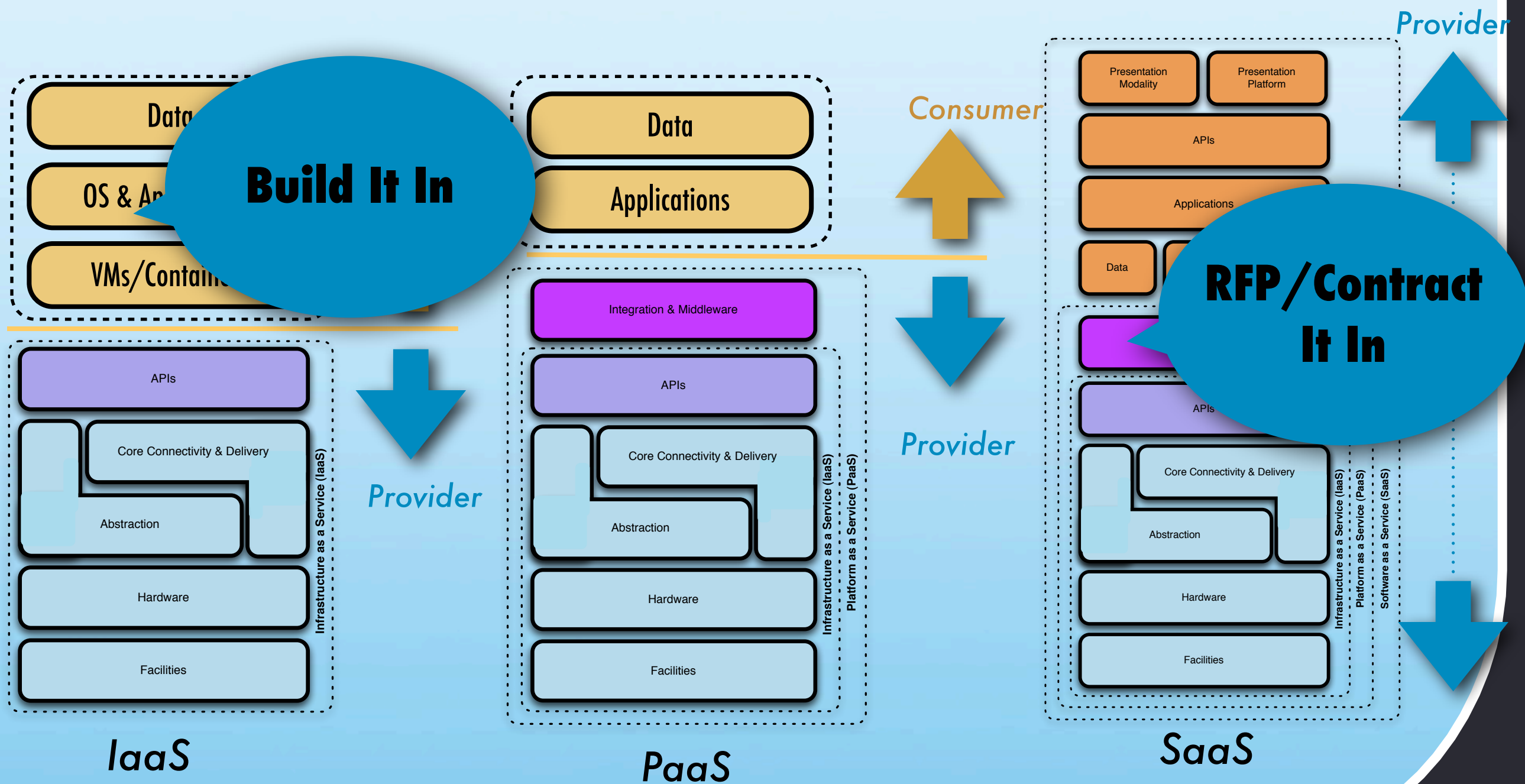
## Good As Good Gets...

8.3. Protection of Your Data. Without limiting the above, **We shall maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Your Data.** We shall not (a) modify Your Data, (b) disclose Your Data except as compelled by law in accordance with Section 7.5 (Compelled Disclosure) or as expressly permitted in writing by You, or (c) access Your Data except to provide the Services or prevent or address service or technical problems, or at your request in connection with customer support matters.

The image shows a vertical strip of white paper with a torn, ragged edge, set against a light blue background. On the paper, the text "salesforce.com" is written in a black, sans-serif font. To the left of the ".com" part, there is a red logo consisting of a stylized "S" shape, followed by the text "Success On Demand." in a smaller, red, sans-serif font.

salesforce.com  
Success On Demand.

# What This Means To Security





## ::So What Does That Really Mean?

- Depending upon the Cloud delivery model, many options for compensating controls are abstracted to “good enough” or are simply unavailable
- The provider abstracts away the compute, storage and network which “simplifies” things but eliminates entire classes of capability, limiting visibility and options
- Even with the potential for API’s and open interface standards, when it comes to Cloud we’re at the mercy of what is provided and...



# Cloud Computing



It All Comes Down To *Trust...*



Heart Of Darkness ::  
Corrosive (t) Rust

# *:: Heart Of Darkness Corrosive (t)Rust*

Virtualization & Cloud's Operational Integrity, confidentiality and availability are based on faith and:

- Trust in providers
- Trust in protocols
- Trust in hardware
- Trust in software
- Trust in operations & people



## :: Trust < > Control



- Cloud is all about gracefully losing control
- Control is often an emotional issue we are often unprepared to deal with
- Transparency & visibility can easily make up for things that are out of your direct control

## *Cloudifornication: Stacked Turtles (Er, Frogs)*

- “Stacking Clouds on Clouds” and building levels of abstraction adds complexity and staggering interdependencies
- We’re building on a very shaky foundation/weak base of frogs; one goes, they all go





# *Air Deccan : Simplifying the Cloud*

There is an ancient Hindi proverb that says:

*"...just because you can,  
doesn't mean you  
should..."*

*...use duct tape to secure  
the wing of a Airbus 320  
that flies at 36,000 feet..."*

<http://blog.mobissimo.com/archives/392-Air-Deccan-Finds-New-Uses-For-Tape-Airplane-Wing-Repair.html>



## *Rules Of the Road*

*The only thing keeping you alive are some painted yellow lines, a general agreement that everyone wants to arrive at their final destination & the trust that each will keep to their side of the road...*





## *Rules Of the Road*

The only thing keeping you alive are some painted yellow lines, a general agreement that everyone wants to arrive at their final destination & the trust that each will keep to their side of the road...





## *What Have Cloud & Virtualization Providers Done To Earn Our Trust?*

- Hypervisor vulnerabilities
- Lack of TCB implementations
- Lack of Standards
- Introduction of monocultures
- Information Leakage
- Substantial Downtime
- Security By Obscurity



# Web3.0/Infrastructure 2.0?/Security 1.3a?

Achtung! Divergent Models

Das Cloud

Mainframes

Web2.0

Client/Server

Web1.0

	Developers	Security
1995	CGI, PERL	Network firewalls, SSL
1997	ASP, JSP	Network firewalls, SSL
1998	EJB, J2EE, DCOM	Network firewalls, SSL
1999	SOAP, XML	Network firewalls, SSL
2001	Rest, SOA	Network firewalls, SSL
2003	Web 2.0	Network firewalls, SSL

Display

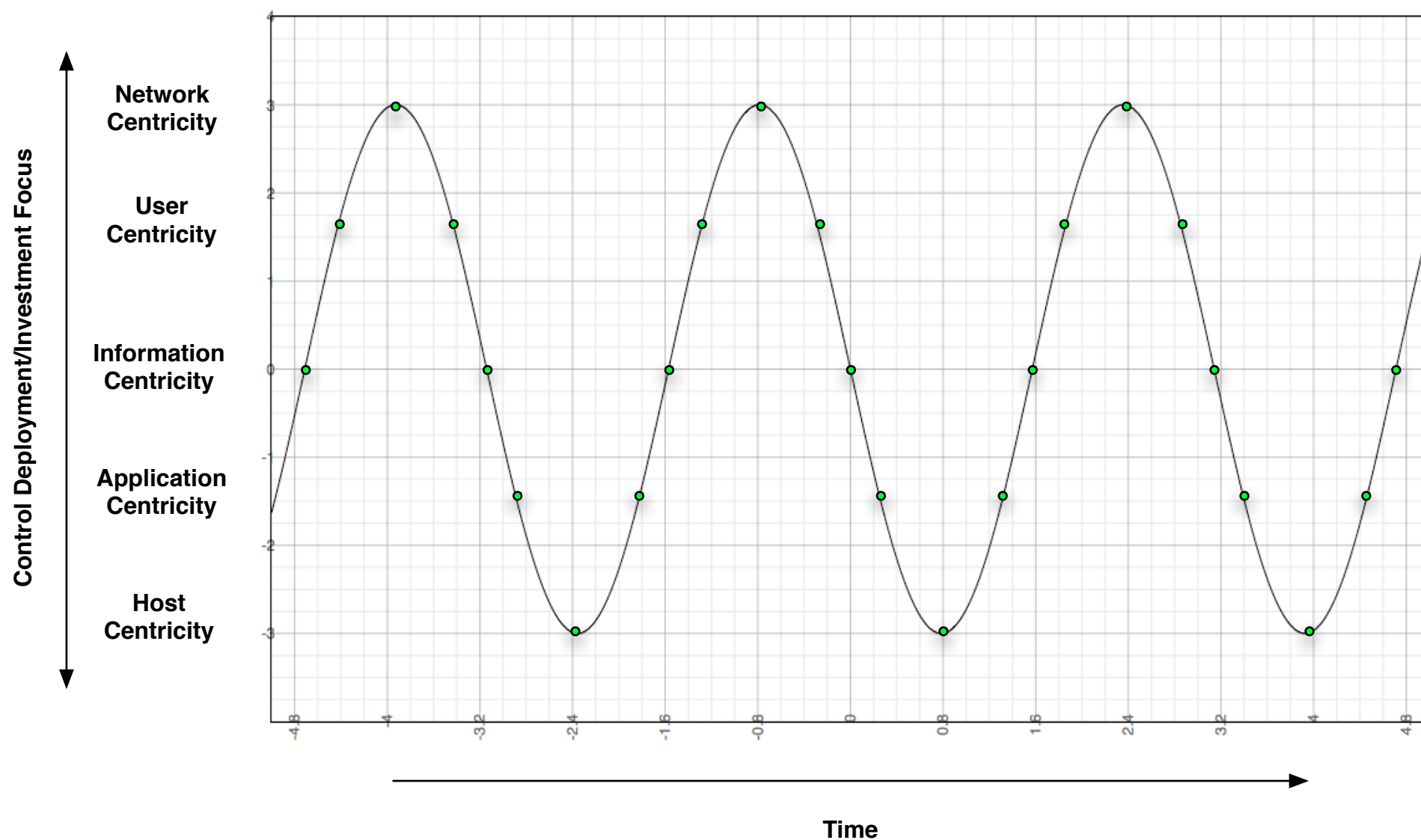
Compute

Data

Bandwidth

# The Hamster Sine Wave of Pain...\*

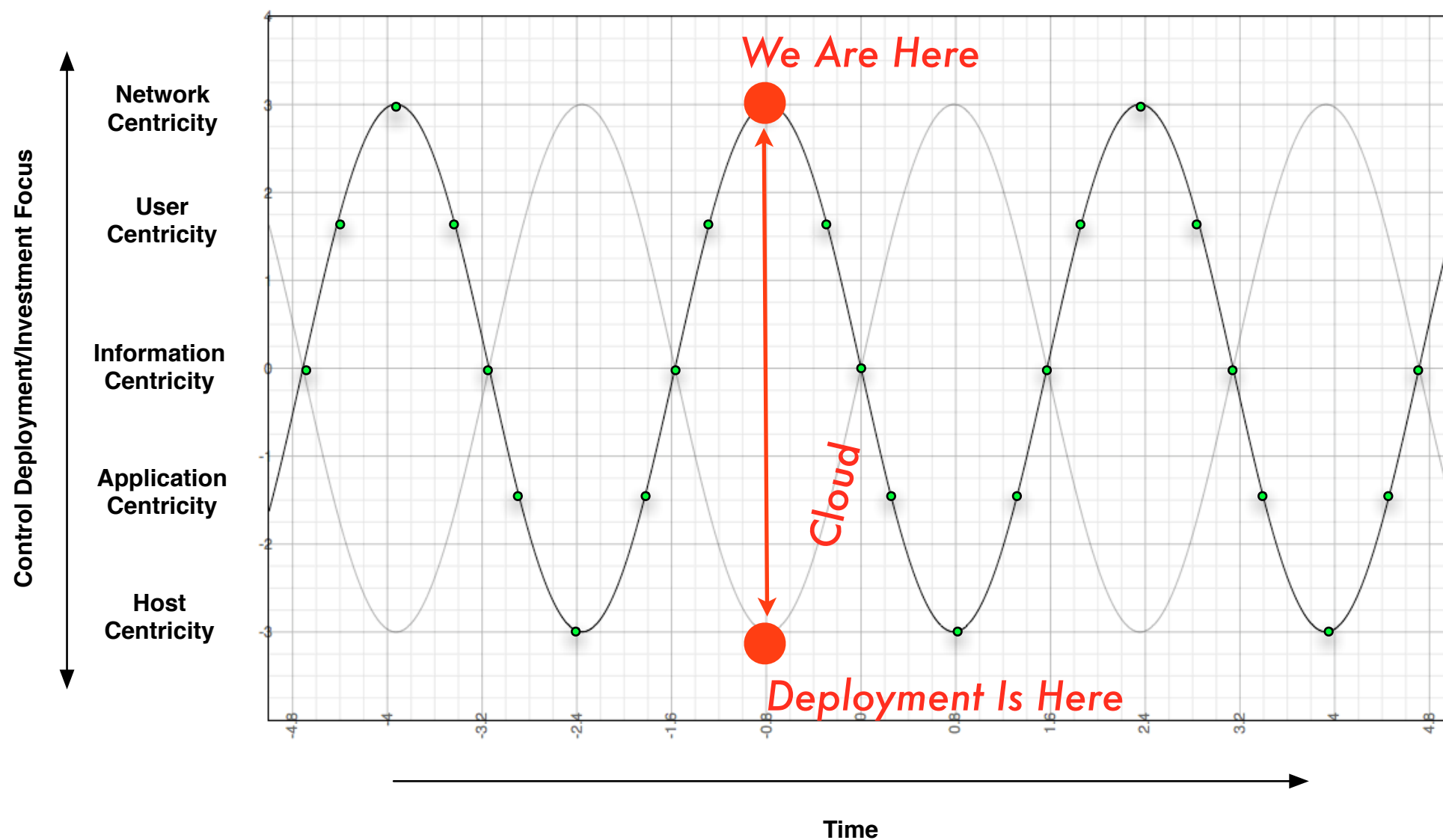
The Security Hamster Sine Wave of Pain



\* With Apologies to Andy Jaquith & His Hamster...

# The Hamster Sine Wave of Pain...\*

The Security Hamster Sine Wave of Pain



\* With Apologies to Andy Jaquith & His Hamster...



## *::Converged Simplicity - Pushing the Envelope*



- As we converge compute, network and storage our speeds and feed issues don't subside, they intensify
- Integrating virtualized security capabilities at network scale becomes even more challenging: 10GbE/40GbE/100GbE... virtualized DC's are pushing to terabit fabrics
- As we'll see, this is a squeezing the balloon problem

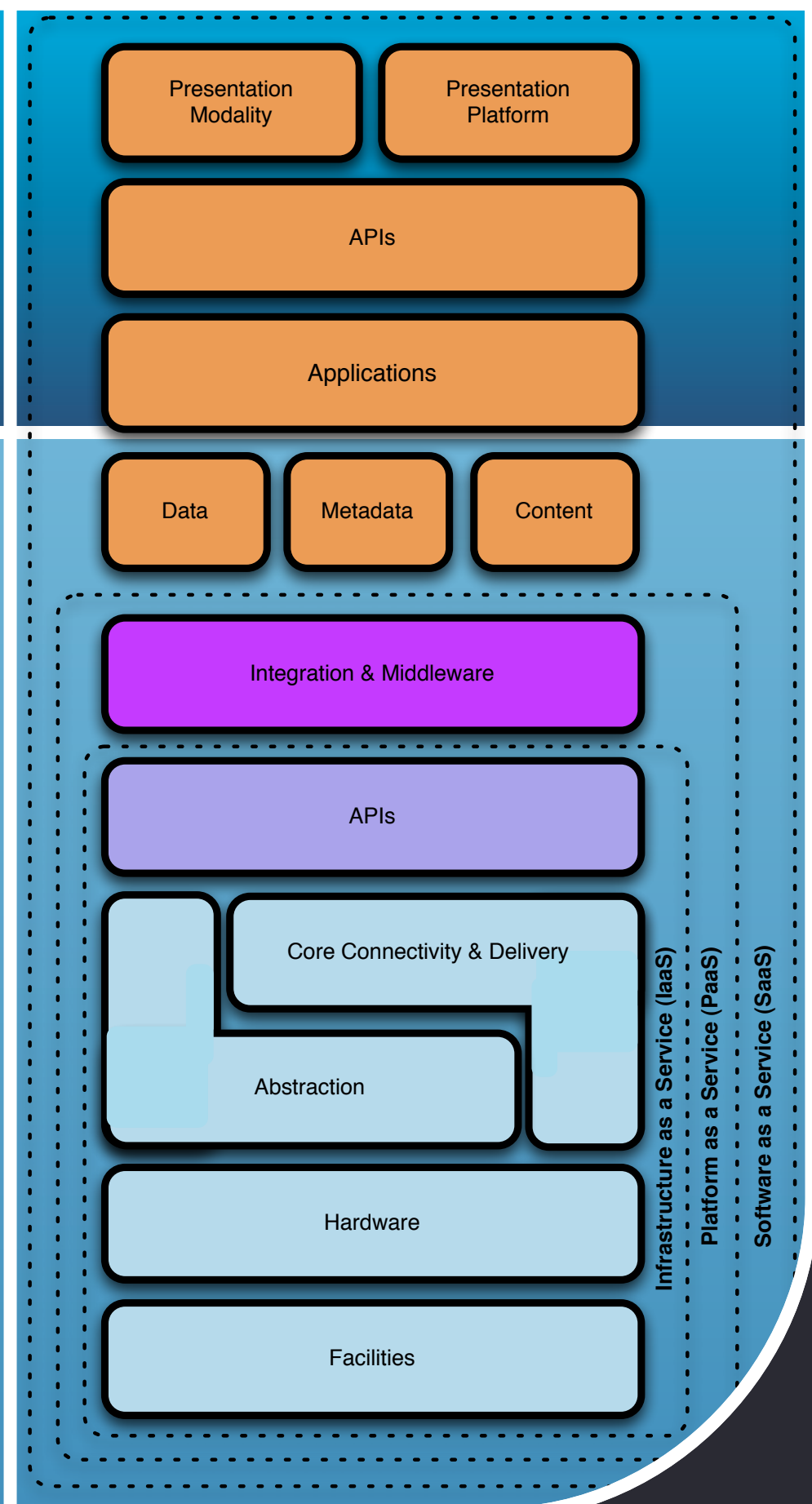


*There Ain't Nuthin' Wrong With The InterTubes!*



# *We Are Product Rich, But Solution Poor*

- What's true with VirtSec is true with Cloud, only more so. Viva Le 4 Horsemen!
- Depending upon the type of Cloud, you may not get feature parity for security.
- Your visibility and ability to deploy or have a compensating control deployed may not be possible or reasonable.
- As it stands now, the abstraction of Infrastructure is really driving the cyclic shift from physical network controls to logical/virtual & back into the host/guest



# *Owning the Cloud*

*Infostructure*

*Metastructure*

*Infrastructure*





# ::Cloudanatomy

*Infostructure*

- **Content & Context -**  
Apps, Data, Metadata, Services

*Metastructure*

- **Glue & Guts -**  
IPAM, IAM, BGP, DNS, SSL, PKI

*Infrastructure*

- **Sprockets & Moving Parts -**  
Compute, Network, Storage

## *Cloud Happiness :: Warm & Fuzzies*

The Cloud can provide the following security benefits:

- *Centralized Data (sort of...)*
- *Segmented data/applications*
- *Better Logging/Accountability*
- *Standardized images for asset deployment*
- *Better Resilience to attack & streamlined incident response*
- *More streamlined Audit and Compliance*
- *Better visibility to process*
- *Faster deployment of applications, services, etc.*



# *::Familiar Security Challenges*

- *Availability & SLA's*
- *Confidentiality & Privacy*
- *Visibility & Manageability*
- *Portability & Interoperability*
- *Reliability & Resiliency*
- *Vendor Lock-in*
- *eDiscovery & Forensics*
- *Information Lifecycle*
- *Change Control*
- *Compliance*



## *::and What's Old is New(s) Again*

- Access Control
- Data Leakage
- Authentication
- Encryption
- Denial Of Service/DDoS
- Key Management
- Vulnerability Management
- Application Security
- Database Security
- Storage Security
- SDLC
- Protocol Security
- Identity Management
- Risk Management

# ::Information Intercourse?

Infostructure

Metastructure

Infrastructure



- Clouds on Clouds on Clouds...
- Amorphous perimeters and the migration to multi-tenancy
- Socialist security & co-mingled data in multi-tenant elastic environments
- Really crusty protocols and even more stale approaches to integration
- Security becomes a question of SCALE...

*Unstacking Turtles...*



# ::Caveats

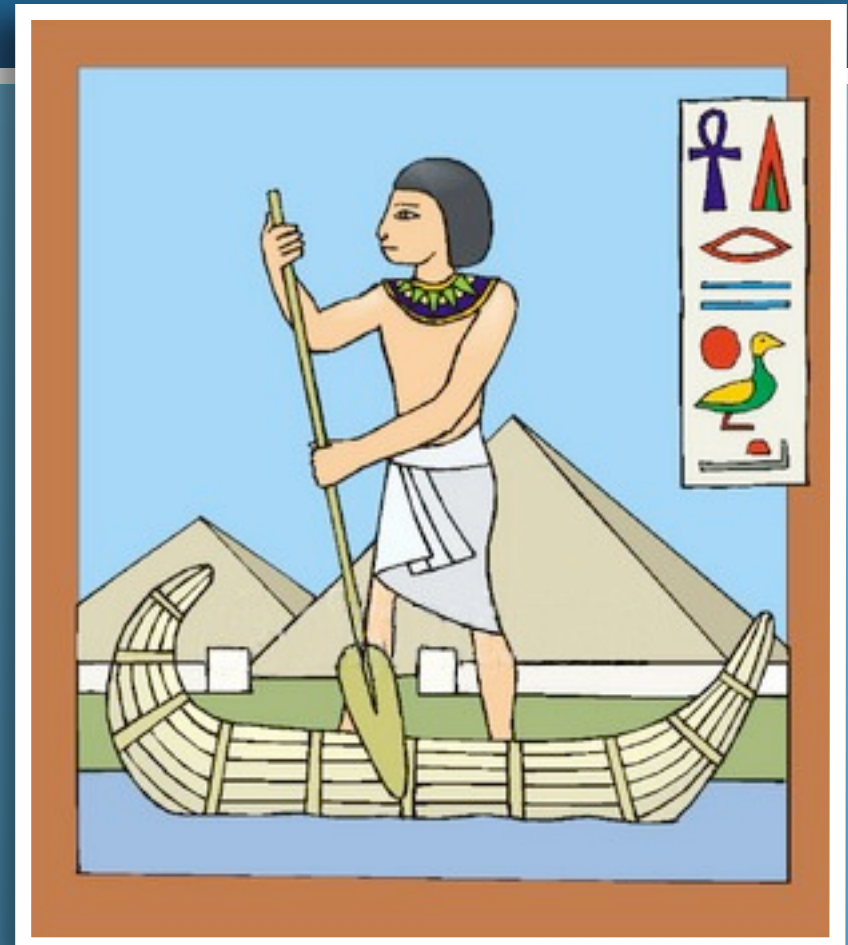
- The following is constructed to make you think
- We're going to discuss a lot of interesting things
- Some are academic, some are practical
- Some things are specific to cloud, others not
- The names have not been changed to protect anyone, nor so they seek to impugn anyone
- Think about the big picture, not the little illustrations





# An Example Is In Order...

- Imagine a fictional Public IaaS Cloud Provider...
- Let's call them "*Da Nile Web Services\**"
- Virtualization, multi-tenancy & Isolation based on a VMM: Elastic Compute, Network & Storage Services...
- Let's take a journey & imagine how what we're going to discuss might affect this fictional provider of service



\*It ain't just a river in Egypt (or South America...)



Infrastructure

# Physical FAIL

- 365 Main - Cascading Power Distribution/Generation Failures
- Rackspace - Truck drives into transformer. Things go boom.
- CI Hosts - Robbery. Four Times
- Core IP Networks - FBI Seizure

*\*HT to Jesse Robbins: Failure Happens, CloudCamp Interop*



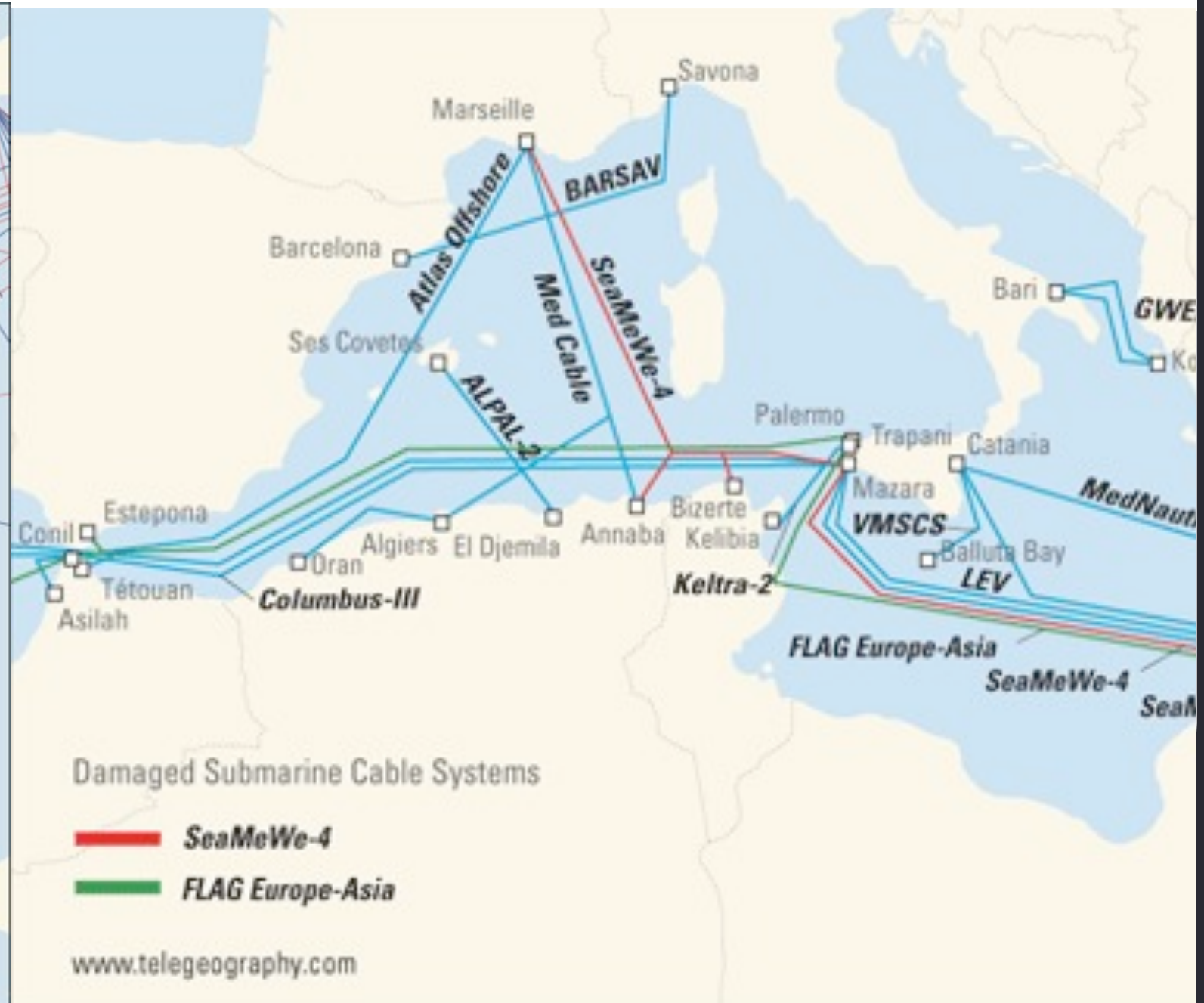
## Infrastructure

*Doh!*

- As large Cloud providers consolidate to mega datacenters, bandwidth, peering & transit traffic patterns will shift based on the physical location
- Mobility of NextGen Infrastructure & virtualization/Cloud tech. will exacerbate this
- Shared infrastructure increases the failure impact radius



# Infrastructure :: Shared Wavelengths



Infrastructure

:: *Shared Wavelengths*



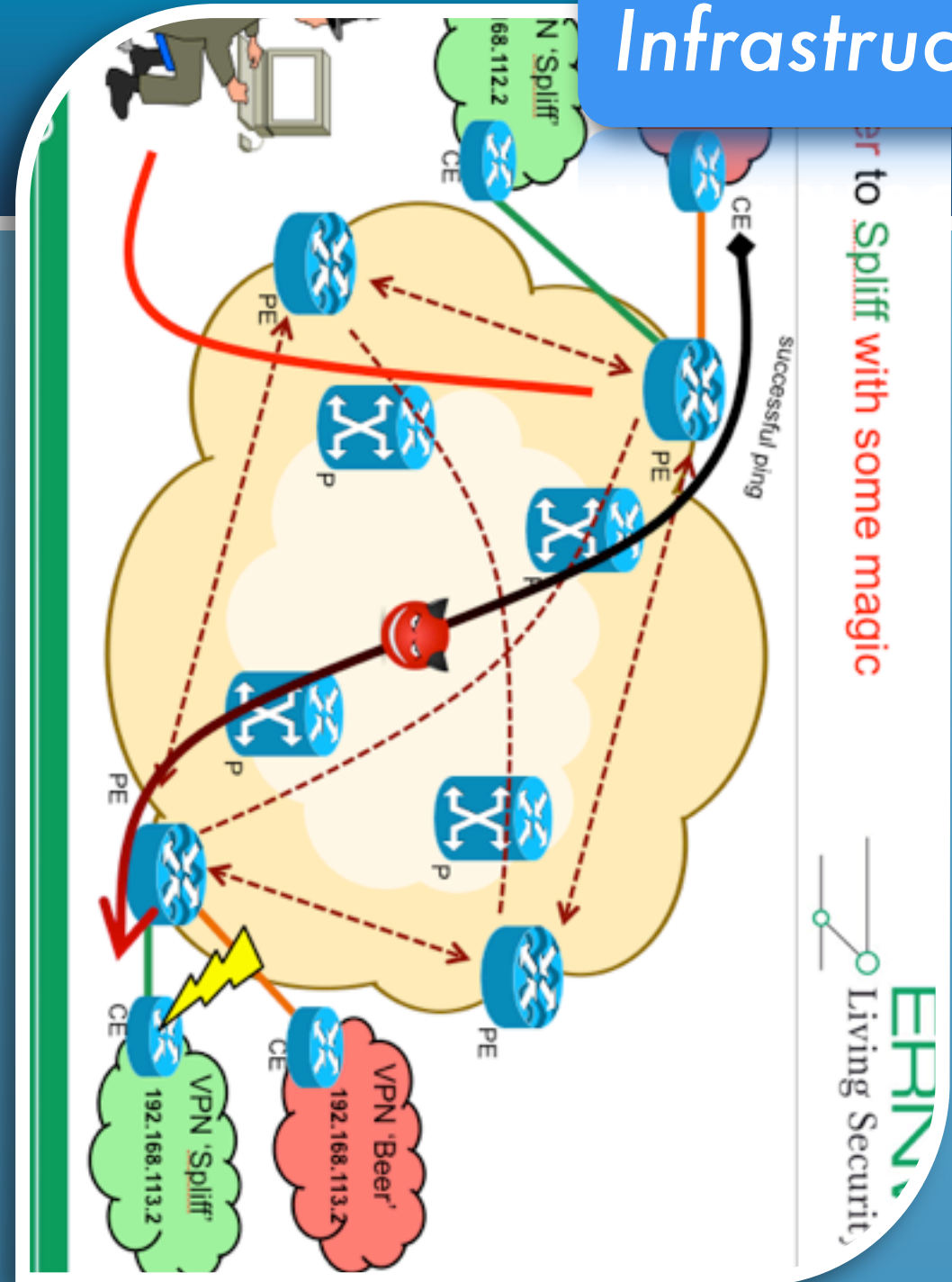
The beauty of Cloud is that with  
infinite scale comes infinite FAIL!



# :: Bit Buckets, Carrier Ethernet, MPLS and L2/3 VPNs

- Core Infrastructure Exploits
- ERNW's Carrier Ethernet & MPLS subversion (Owning Carrier Networks)
- Carriers & the NSA's "free email/voice archiving"
- Big, Flat L2 networks bring Old Skool I337 back. Remember Yersinia?

## Infrastructure







## Infrastructure

*:: CPU/Chipset &  
VMM Compromise*

Some examples of Joanna Rutkowska & ITL's work on CPU/Chipset and Virtualization subversion:

- Xen VMM Dom0 Escalation
- Xen VM escapes
- Bluepillling Xen w/nested virtualization
- Bypassing Intel's TXT
- SMM attacks
- BIOS rootkits

Infrastructure

:: VMM Monoculture



# Infrastructure :: Shared VM/VA/AMIs

Home > Resources > AWS Management Console BETA > Amazon EC2

Welcome, Christofer Hoff | Settings | Sign Out

Amazon EC2 Amazon Elastic MapReduce Amazon CloudFront

### Navigation

Region: US-East

- > EC2 Dashboard
- INSTANCES
  - > Instances
- IMAGES
  - > AMIs
  - > Bundle Tasks
- ELASTIC BLOCK STORE
  - > Volumes
  - > Snapshots
- NETWORKING & SECURITY
  - > Elastic IPs
  - > Security Groups
  - > Key Pairs

### Amazon Machine Images

Launch Register New AMI De-register Permissions

Viewing: All Images All Platforms 1 to 50 of 3277 AMIs

	AMI ID	Manifest	Visibility	Platform
<input type="checkbox"/>	ami-6c55b205	ec2-paid-ibm-images/lotus-web-content-management-standard-edition-€	Public	Other Linux
<input type="checkbox"/>	ami-6f55b206	ec2-paid-ibm-images/websphere-portal-and-lotus-web-content-managen	Public	Other Linux
<input type="checkbox"/>	ami-a21affcb	ec2-public-images/fedora-core-6-x86_64-base-v1.06.manifest.xml	Public	Fedora
<input type="checkbox"/>	ami-a21cfccb	ec2-paid-ibm-images/db2-workgroup-9.7-64-bit.manifest.xml	Public	Other Linux
<input type="checkbox"/>	ami-ac1cfcc5	ec2-paid-ibm-images/db2-express-9.7-32-bit.manifest.xml	Public	Other Linux
<input type="checkbox"/>	ami-b454b3dd	ec2-paid-ibm-images/websphere-smash-32-bit.manifest.xml	Public	Other Linux
<input type="checkbox"/>	ami-bd9d78d4	ec2-public-images/demo-paid-AMI.manifest.xml	Public	Other Linux
<input type="checkbox"/>	ami-c64daaaf	ec2-public-windows-images/SqlSvrStd2003r2-x86_64-Win-v1.06.manife	Public	Windows
<input type="checkbox"/>	ami-c74daaae	ec2-public-windows-images/SqlSvrStd2003r2-x86_64-WinAuth-v1.06.m	Public	Windows
<input type="checkbox"/>	ami-d1ca2db8	aws-toolkit-for-eclipse-amis-us/haproxy-v1.0.2.manifest.xml	Public	Other Linux
<input type="checkbox"/>	ami-d84daab1	ec2-public-windows-images/SqlSvrExp2003r2-x86_64-Win-v1.06.manif	Public	Windows
<input type="checkbox"/>	ami-d94daab0	ec2-public-windows-images/SqlSvrExp2003r2-x86_64-WinAuth-v1.06.m	Public	Windows
<input checked="" type="checkbox"/>	ami-da4daab3	ec2-public-windows-images/SqlSvrExp2003r2-i386-Win-v1.06.manifest.	Public	Windows

#### 1 Amazon Machine Image selected

AMI ID:	ami-da4daab3	Product Code:	-	Kernel ID:	-
Owner:	amazon	Architecture:	i386	Ramdisk ID:	-
Visibility:	Public	Image Type:	machine	Platform:	Windows
State:	available				
Manifest:	ec2-public-windows-images/SqlSvrExp2003r2-i386-Win-v1.06.manifest.xml				

Infrastructure

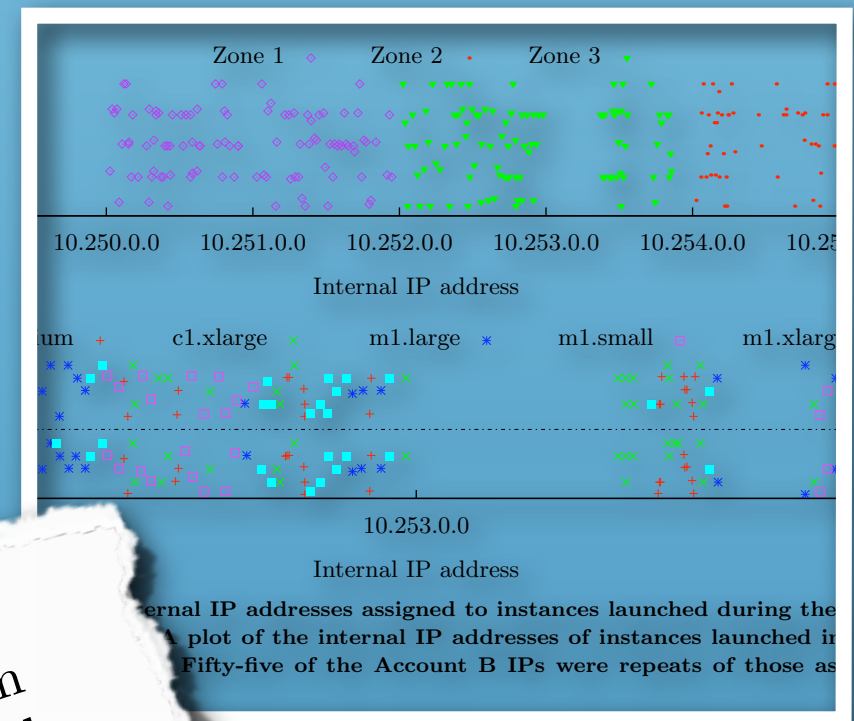
:: Shared VM/VA/AMIs





# Infrastructure :: Mapping Cloud Infrastructure

- Cloud Cartography\* - Mapping Cloud Infrastructure & Brute Forcing Co-Resident EC2 AMIs w/ Side-Channel Attacks



## 9. CONCLUSIONS

In this paper, we argue that fundamental risks arise from sharing physical infrastructure between mutually distrustful users, even when their actions are isolated through machine virtualization as within a third-party cloud compute service.

\* Ristenpart, Tromer, Shacham, Savage

## Infrastructure



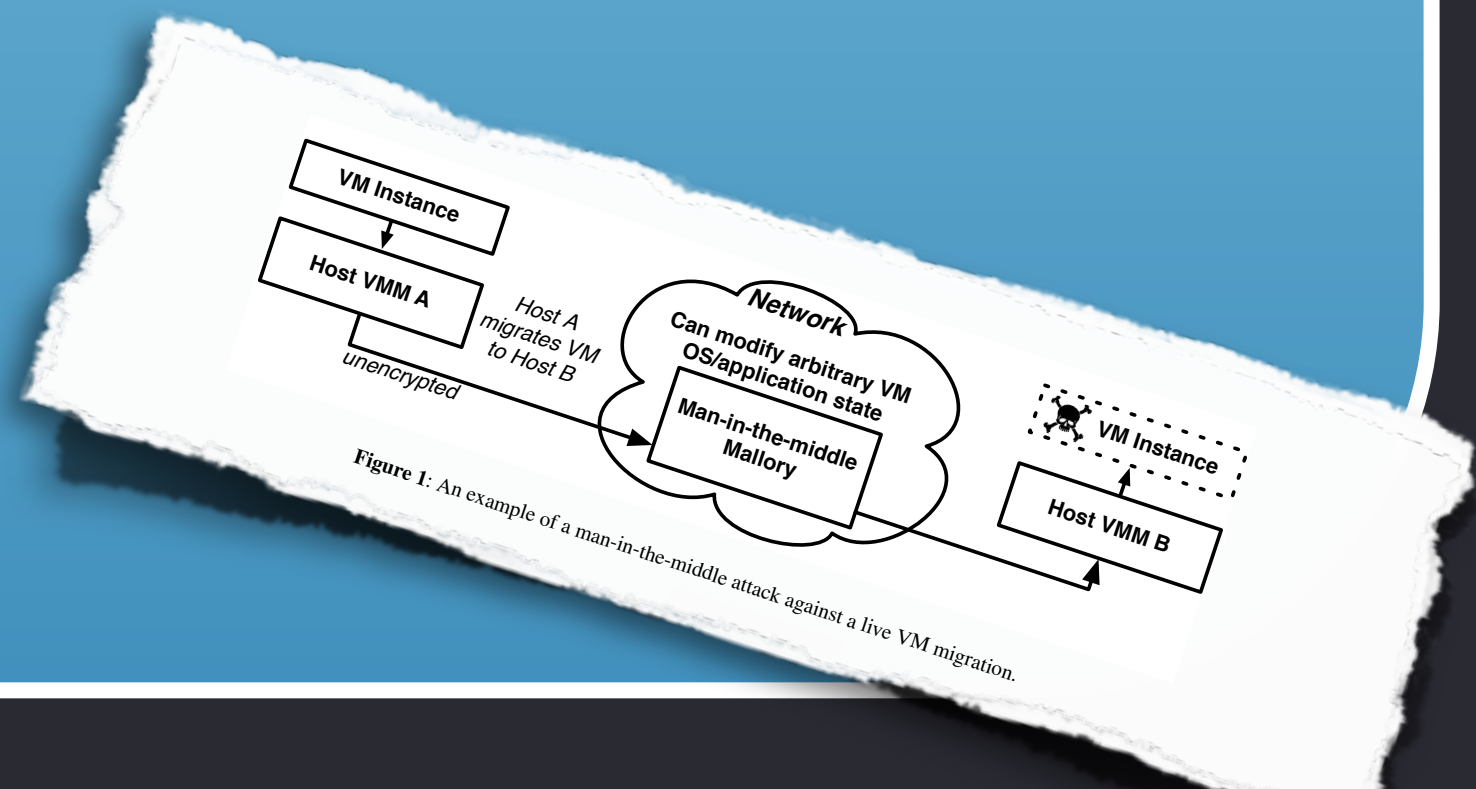
## :: Mapping Cloud & The German Tank Problem

- During World War II, German Panther tanks production was accurately estimated by Allied intelligence using statistical methods.
- Guy Rosen's concept of using AWS EC2 Resource IDs to externally count # of resources provisioned during a specific timeframe

\*<http://www.jackofallclouds.com/2009/09/anatomy-of-an-amazon-ec2-resource-id/>

## Infrastructure :: *vMotion Poison Potion*

- John Oberheide's\* vMotion subversion (with extensions re: long distance VMotion over said Carrier Ethernet/MPLS)

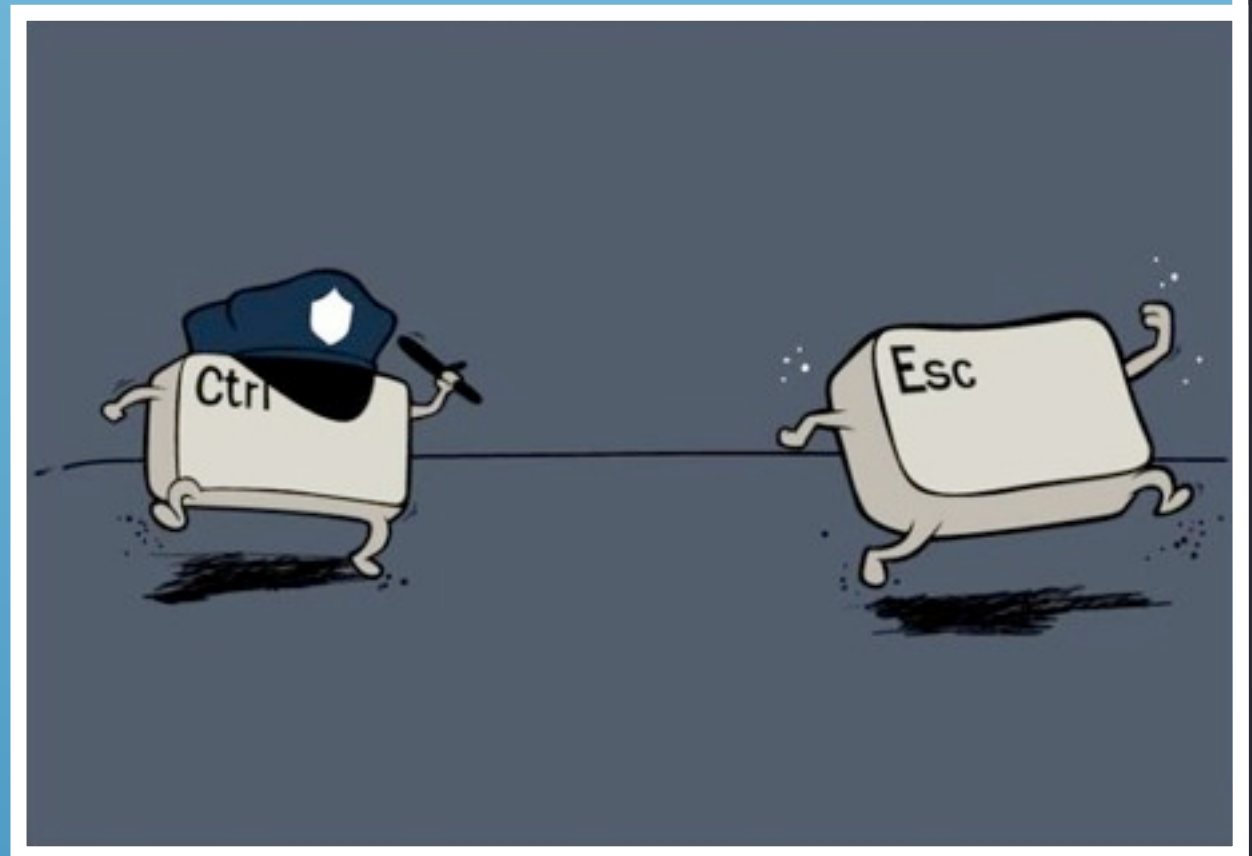


\* Oberheide, Cooke, Jahanian



## Infrastructure :: *Cloudburst VM Escapes*

- Cloudburst VM Escapes\* - Abusing emulated device drivers to provide host to guest escape in virtualized environments





# Metastructure :: BGP, DNS & SSL



## The Flaw at the Heart of the Internet

By Dan Kaminsky

Dan Kaminsky is a security researcher at the University of California, Berkeley. He is the author of the book "The Flaw at the Heart of the Internet" and the creator of the "Flaw at the Heart of the Internet" project. He is also a member of the Open Security Foundation and the Open Source Security Foundation.



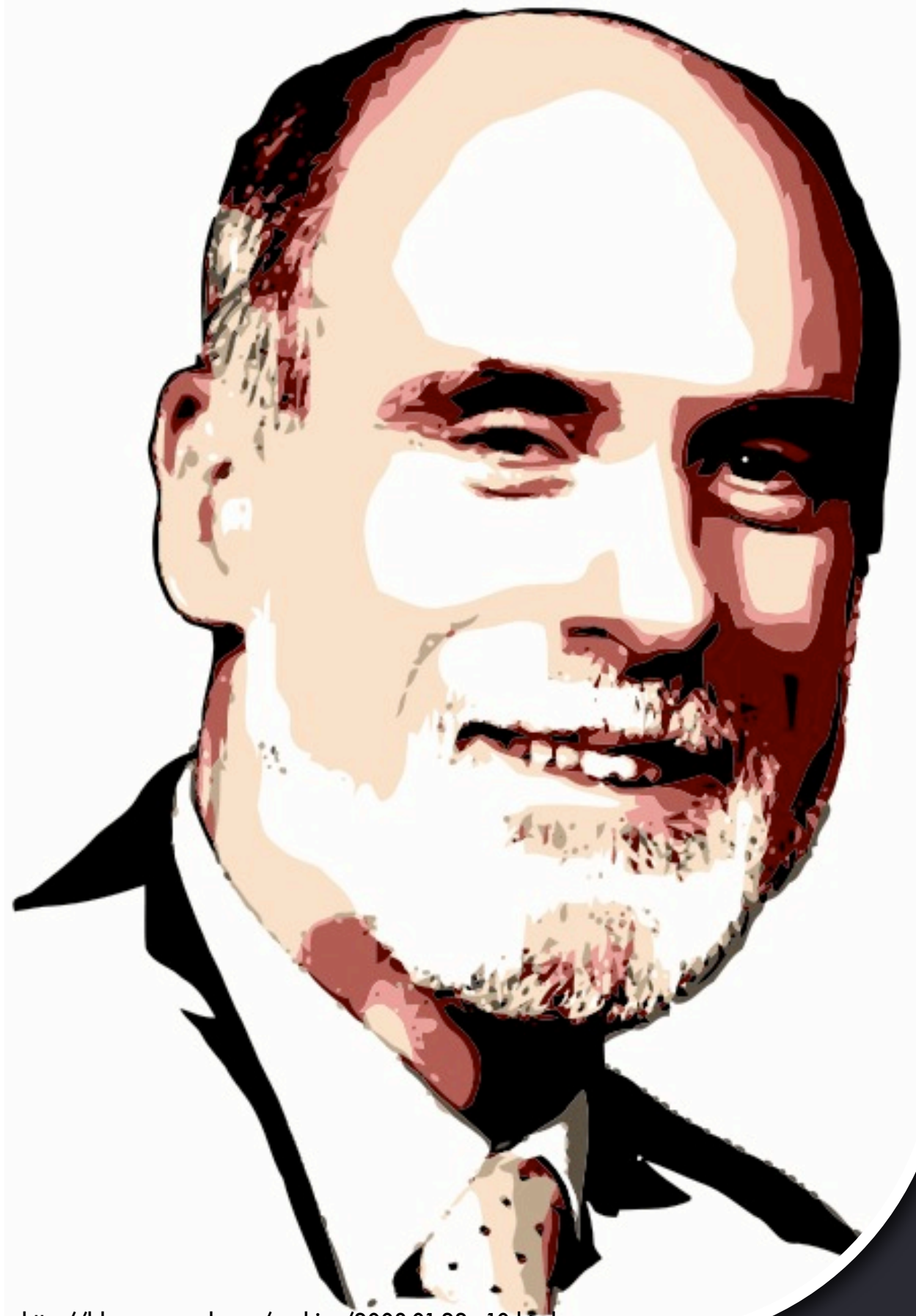
- Kaminsky's DNS attacks
- ERNW's | Kapela & Pilosov's BGP attacks, YouTube (Prefix Hijacking, MITM)
- Moxie Marlinspike's SSL/TLS - Chained Certs, Null Certificate Prefix Bug, MITM, General Browser sux0r
- Sotirov et. al. Rogue CA & MD5 (...and so on, and so on...)

## Metastructure

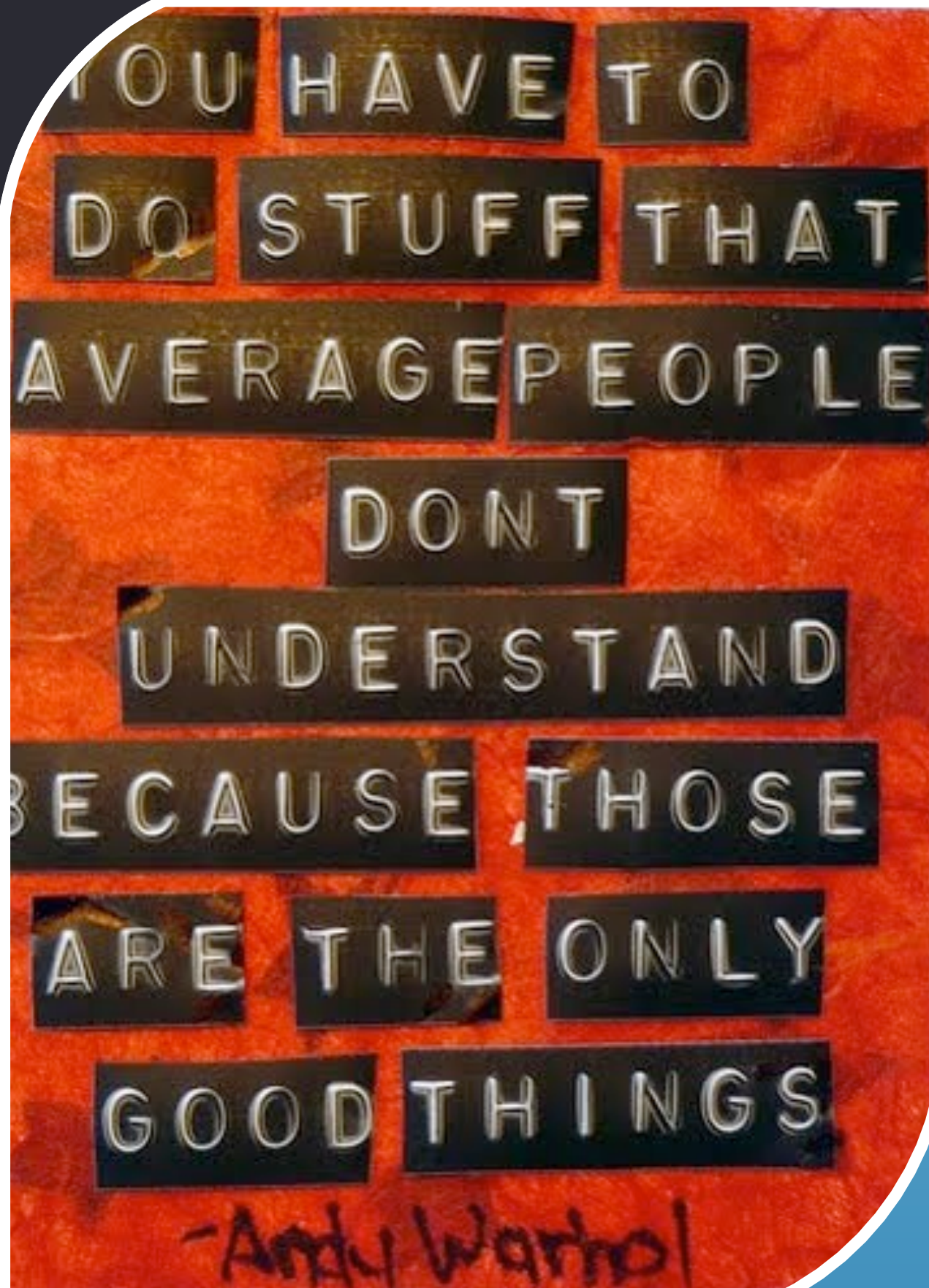
### Uncle Vint Sez...

// Each cloud is a system unto itself. There is **no way to express the idea of exchanging information between distinct computing clouds** because there is no way to express the idea of "another cloud." ...there is **no way to express how that protection is provided and how information about it should be propagated to another cloud** when the data is transferred.

//







## Metastructure

::APIs, Interfaces & "Simplicity"

- There are literally dozens of competing cloud interface and API specifications & standards
- If complexity is the enemy of security, what is abstracted simplicity?

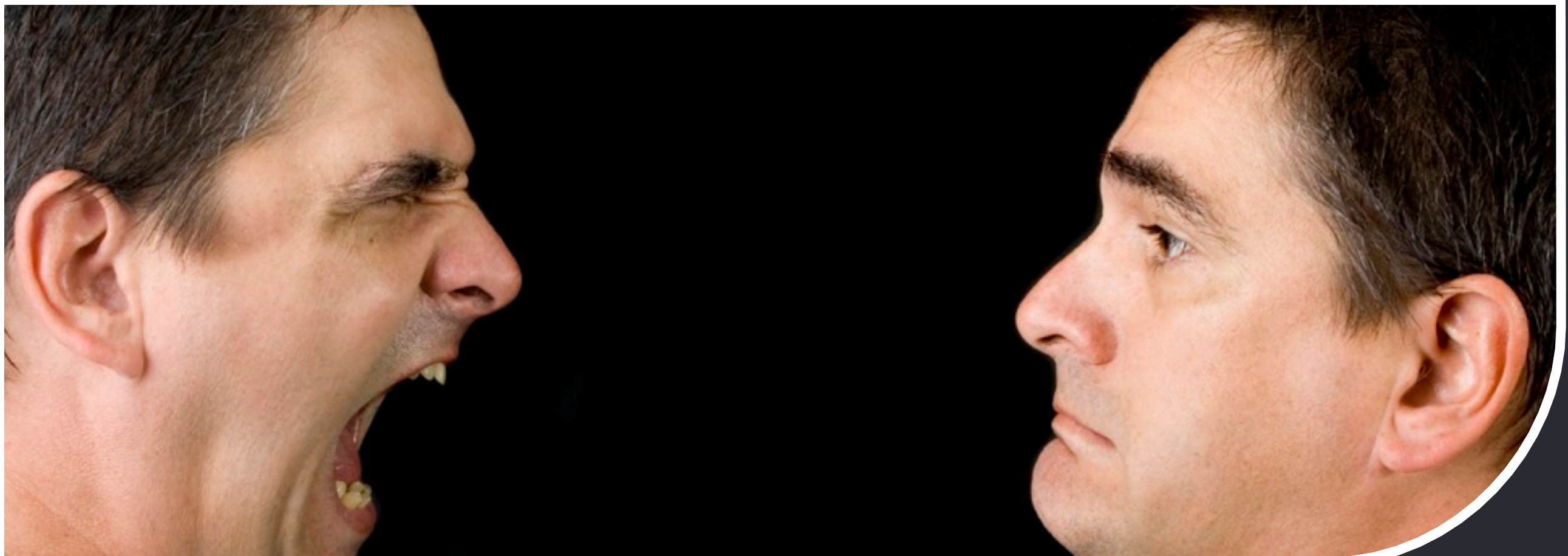


Metastructure

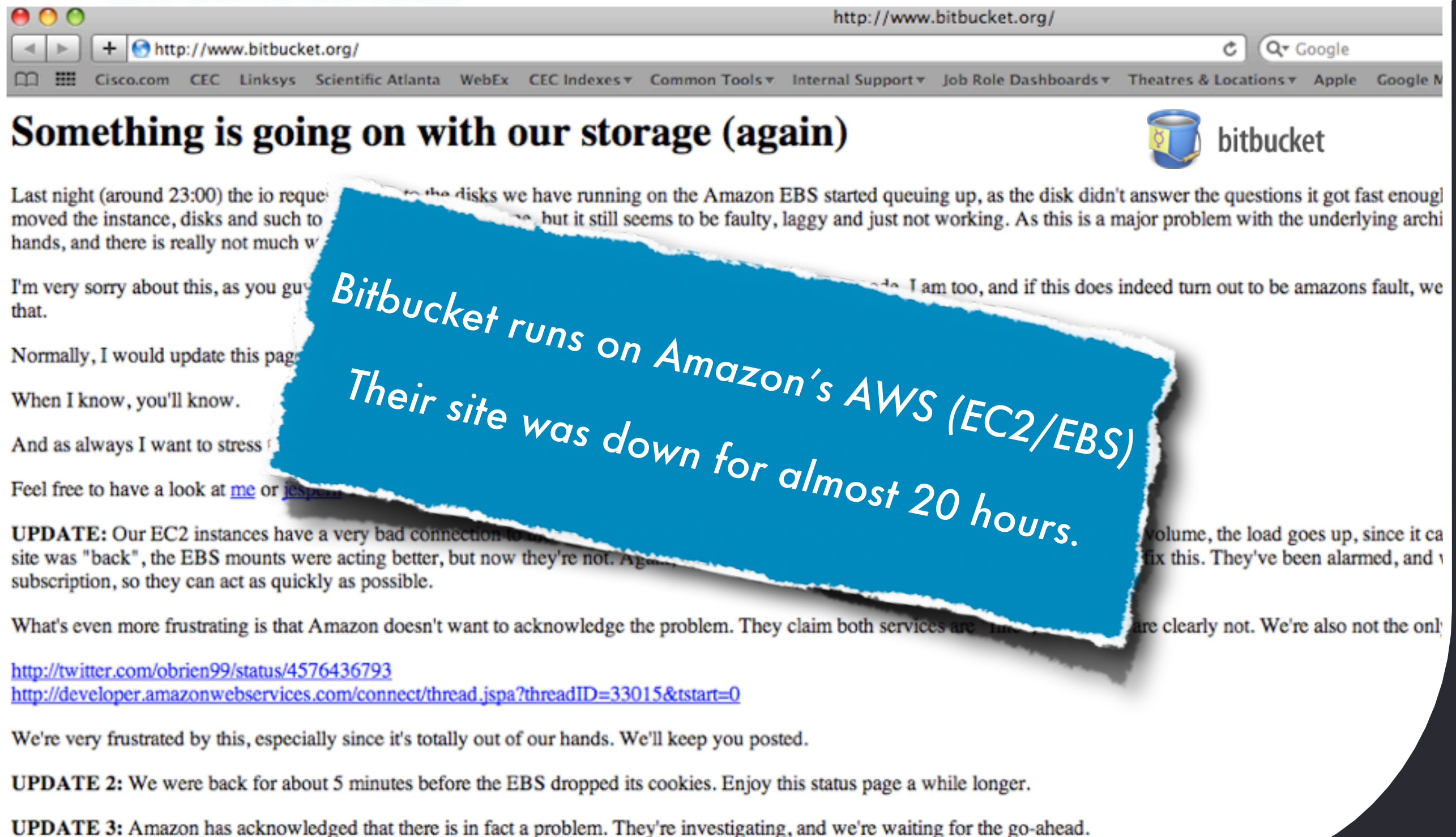
*Stuck In the Middle*

Infostructure

- Developers want to point-click-deploy to Cloud from an IDE
- To them, Cloud is a platform with API's & Interfaces, not infrastructure
- Metastructure *\*should\** be transparent, but isn't
- Infrastructure breaks infostructure, metastructure breaks infrastructure
- Rock, paper, scissors







The screenshot shows a web browser window with the address bar at <http://www.bitbucket.org/>. The page title is "Something is going on with our storage (again)". The Bitbucket logo is in the top right. The main text describes a storage issue on Amazon EBS. A large blue overlay with white text reads: "Bitbucket runs on Amazon's AWS (EC2/EBS) Their site was down for almost 20 hours." Below the overlay, the text continues with an update and links to a Twitter status and an Amazon Web Services thread.

**Something is going on with our storage (again)**

Last night (around 23:00) the io requests to the disks we have running on the Amazon EBS started queuing up, as the disk didn't answer the questions it got fast enough. We moved the instance, disks and such to new ones, but it still seems to be faulty, laggy and just not working. As this is a major problem with the underlying architecture, we're not sure how long it will take to fix this. I am too, and if this does indeed turn out to be Amazon's fault, we're sorry about this, as you guys know. I'm very sorry about this, as you guys know that.

Normally, I would update this page when I know, you'll know.

And as always I want to stress that we're not the only ones who are affected. If you're using Bitbucket, you're affected. Feel free to have a look at [me](#) or [jesper](#).

**UPDATE:** Our EC2 instances have a very bad connection to the EBS. When the site was "back", the EBS mounts were acting better, but now they're not. Again, we're not the only ones who are affected. If you're using Bitbucket, you're affected. We're not the only ones who are affected. If you're using Bitbucket, you're affected. We're not the only ones who are affected. If you're using Bitbucket, you're affected.

What's even more frustrating is that Amazon doesn't want to acknowledge the problem. They claim both services are fine, but they're clearly not. We're also not the only ones who are affected. If you're using Bitbucket, you're affected. We're not the only ones who are affected. If you're using Bitbucket, you're affected.

<http://twitter.com/obrien99/status/4576436793>  
<http://developer.amazonwebservices.com/connect/thread.jspa?threadID=33015&tstart=0>

We're very frustrated by this, especially since it's totally out of our hands. We'll keep you posted.

**UPDATE 2:** We were back for about 5 minutes before the EBS dropped its cookies. Enjoy this status page a while longer.

**UPDATE 3:** Amazon has acknowledged that there is in fact a problem. They're investigating, and we're waiting for the go-ahead.

## Infostructure

# :: Who Owns Cloud Failure?

From this point on, we were treated like they owed us money, which is quite the difference from basically being called a liar earlier on.

Closing in (15 hours after reporting it)

OK, so we are finally getting somewhere. We all agreed that there was a serious problem between our EC2 instances and our EBS. This is around the time I was asked me to try and put the application back online.

I kindly asked the manager to look into it. He said he was on it.

We were attacked. Bigtime. We had a massive flood of UDP packets coming in to our IP, basically eating away all bandwidth to the box. This explains why we couldn't read with any sort of acceptable speed from our EBS, as that is done over the network. So, basically a massive-scale DDOS. That's nice.

This is 16-17 hours after we reported the problem, which frankly, is a bit disheartening. Why did it take so long to discover? Oh well.

Amazon... and everything went back to normal. We surveyed... after deciding that everything was holding up fine, we were in the morning.)



http://blog.bitbucket.org/2009/10/04/

Cisco.com CEC Linksys Scientific Atlanta

From this point on, we were treated like they basically being called a liar earlier on.

Closing in (15 hours after reporting it)

OK, so we are finally getting somewhere. W problem between our EC2 instances and our asked me to try and put the application back

I kindly asked the manager I had on the pho He said he wasn't really sure, and that he w engineers.

I dial in, and they start explaining what the

Now, I have been specifically advised not to our customers to explain what went wrong. were looking pretty bad due to this. I've already page, as well as on IRC, but let me re-iterate

We were attacked. Bigtime. We had a mas basically eating away all bandwidth to the b acceptable speed from our EBS, as that is DDOS. That's nice.

This is 16-17 hours after we reported the p take so long to discover? Oh well.

Amazon blocked the UDP traffic a couple o We surveyed the services for a while longer fine, we went to bed (it was 4am in the mor

"If you single-source your infrastructure provider, one day you're going to get your butt handed to you on a platter. The appearance of 'infinite scale' does not mean you'll automagically realize 'infinite resilience or availability'"

- Me

YouTube Yahoo! News (459) 1P

bitbucket

A hand is shown dropping a coin into a white piggy bank. The piggy bank is sitting on a patch of green grass. The background is a bright blue sky with some white clouds. The entire scene is framed within a white border with rounded corners.

## Infostructure

:: *Misunderestimation*

- Cloud: WebAppSec v AppSec?
- Information Exfiltration
- CloudFlux & FastFlux  
CloudBots
- DDoS & EDoS - Economic  
Denial of Sustainability





Infostructure

*This Sting(k)s...*

### OWASP Top 10

- Injection Flaws
- Cross Site Scripting
- Malicious File Execution
- Insecure Direct Object Reference
- Cross Site Request Forgery (CSRF)
- Information Leakage & Error Handling
- Broken Authentication & Session Management
- Insecure Cryptographic Storage
- Insecure Communications
- Failure to restrict URL access

Infostructure

# :: Layer 8

- Systemic process changes that affect how users interact with services that can change at a moment's notice
- The 'Oops' factor (esp. in SaaS) is going to be an issue...

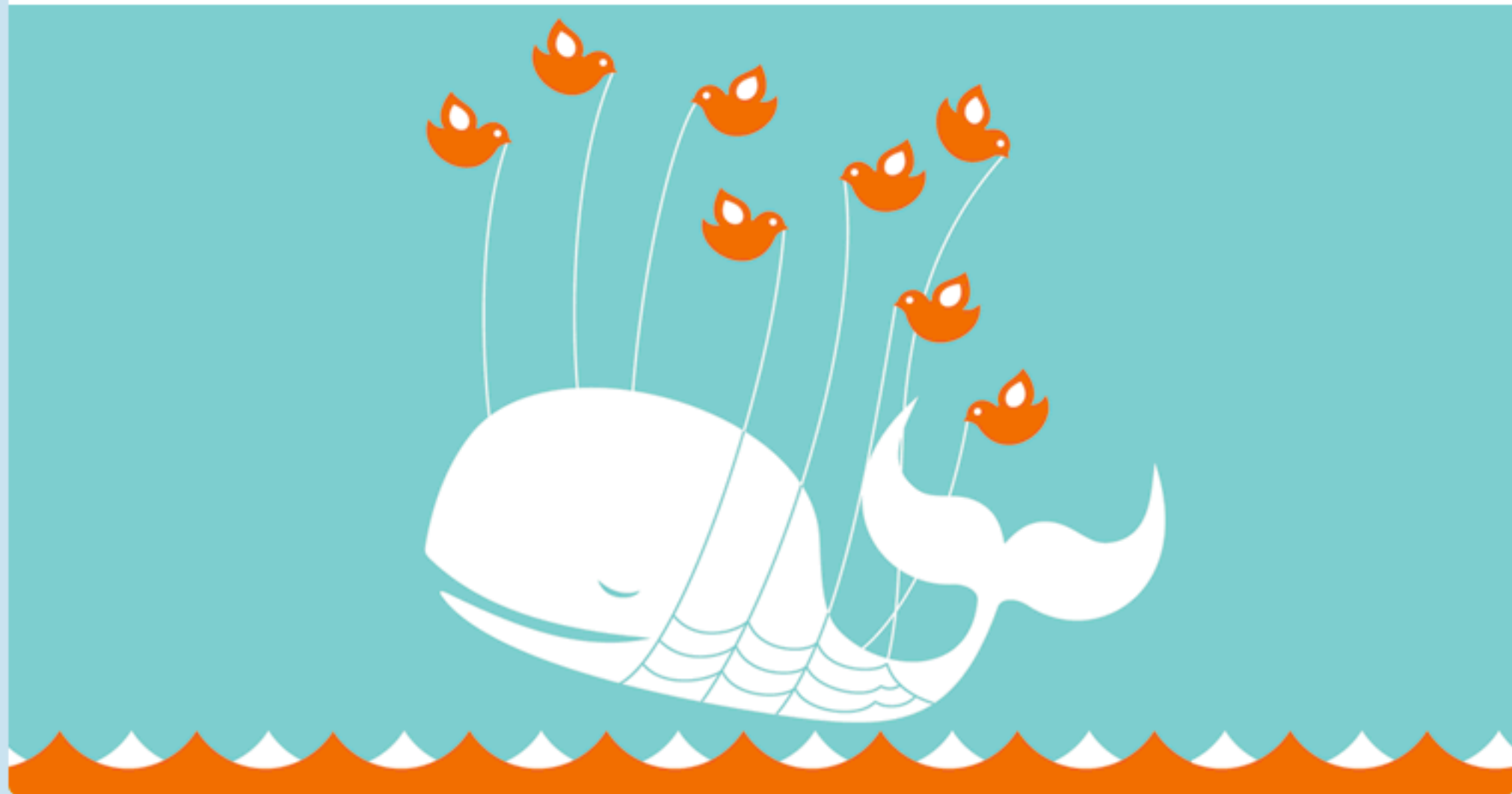


twitter

Home >

## Twitter is over capacity.

Too many tweets! Please wait a moment and try again.



© 2009 Twitter [About Us](#) [Contact](#) [Blog](#) [Status](#) [API](#) [Help](#) [Jobs](#) [TOS](#) [Privacy](#)

46.213

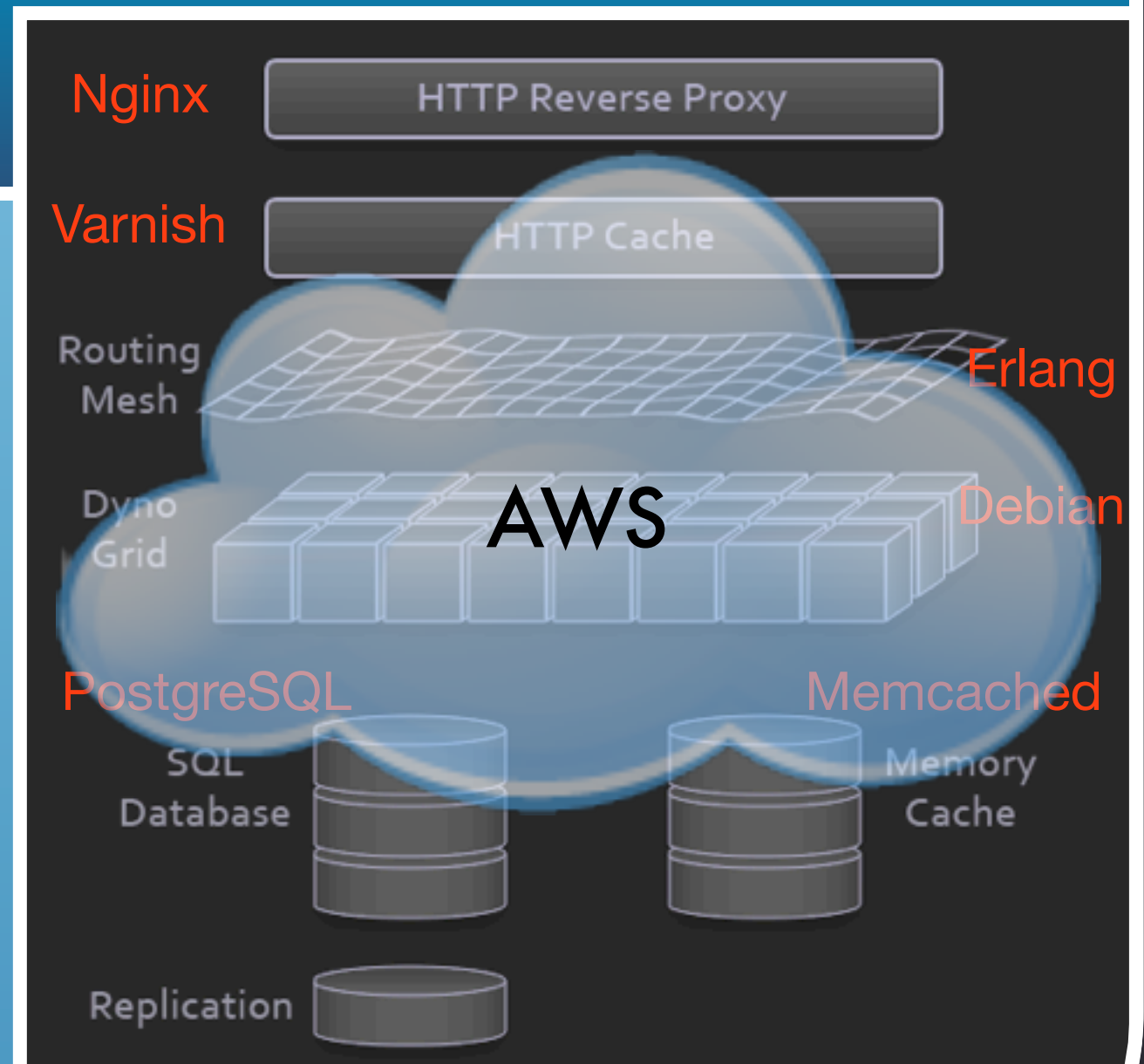
35

arrett Lyon

non-elastic infrastructure that is poorly configured

# Then There's the Other Extreme...

- All this abstraction...
- Sits atop more abstraction...
- In the form of AWS...



Heroku...





Perception IS Reality

*:: Cloud Providers*

*You Can't Have It Both Ways*

**You Can't Claim:**

- Service Superiority & Availability
- Better Security
- Better Performance & Cost

**Back That Up With:**

- 1990's SLA's
- Outages & Breaches
- Lack Of Support

**And Then Say:**

- IT Goes Down, So We Can Too
- Your Expectations are Too High
- We're Still Better...

*I've Only Got  
a few Minutes...*

So I didn't even get to mention:

- PKI
- Storage Security
- IAM
- Encryption
- SOA/WS-\*
- Interoperability

...and the hits keep coming...



# *It Ain't About Being New...*

- People are so wrapped up in new flashy 'sploits
- This is about being pragmatic and fixing the stuff that's fundamentally broken & has been for some time
- Where's the threat modeling, risk assessment and management?



# :: Cloudification Redux

## Infostructure

Application/WebApp Insecurity, SQL Injection, Information Exfiltration

## Metastructure

BGP, SSL & DNS Hijacking

## Infrastructure

MPLS, Routing & Switching, Chipset & Virtualization Compromise

In Cloud, MUCH of this is out of your control...



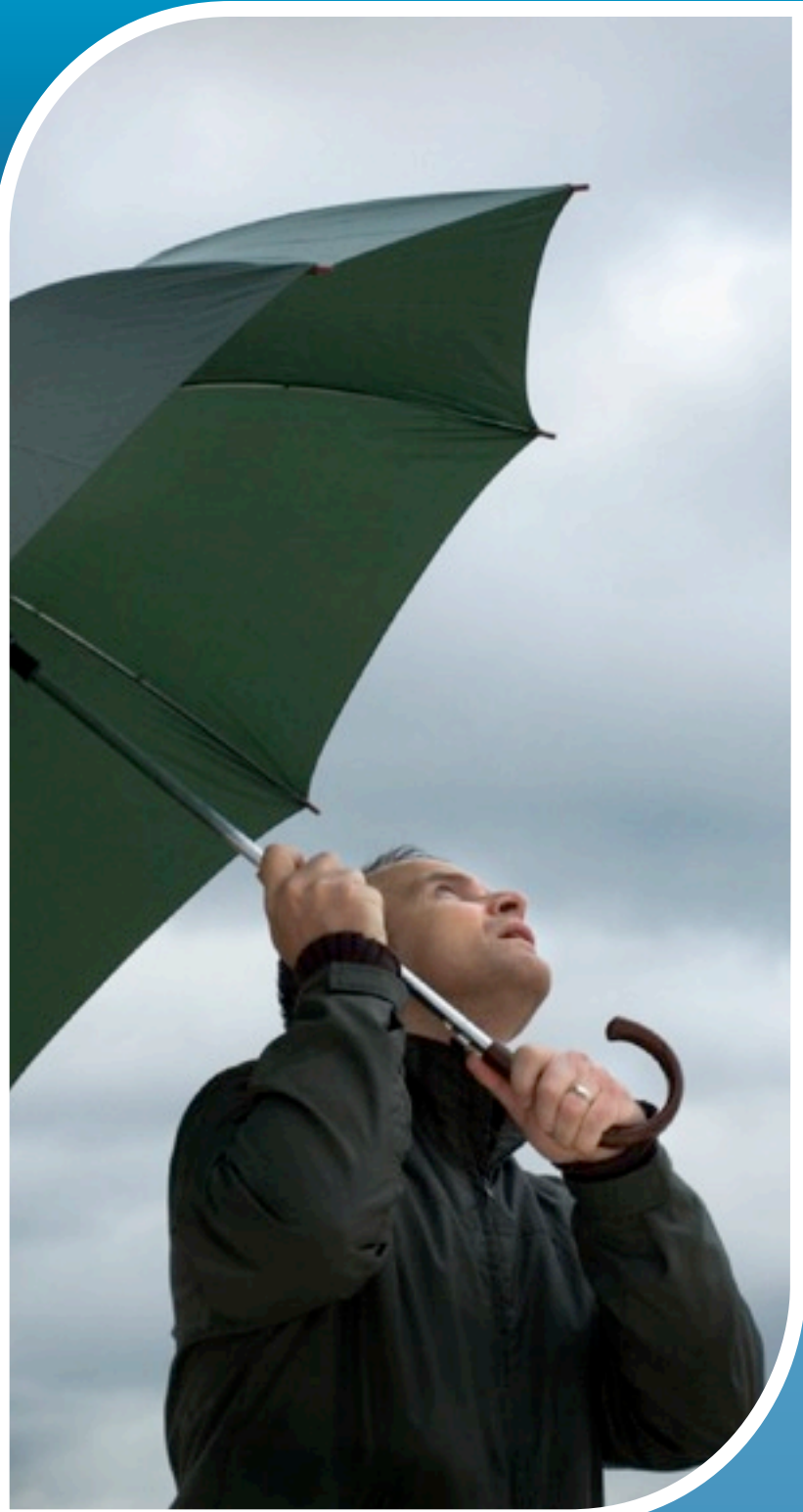


**SECURITY**  
YOU'RE DOING IT WRONG

## *Wrapping Up...*

- Attacks on and using large-scale Public Cloud providers are coming & Cloud services are already being used for \$evil
- Hybrid security solutions (and more of them) are needed
- Service Transparency, Assurance & Auditability is key (A6 API)
- Providers have the chance to make security better. Be transparent.

# *New Solutions To Old Problems*



The Realities of Today's CloudSec Solutions Landscape:

- Whatever the provider exposes in the SaaS/PaaS/IaaS Stack
- Virtualization-Assist API's (If Virtualized)
- Virtual Security Appliances (VM-based)
- Software in the Guest (If Virtualized)
- Integrating Appliances & Unified Computing Platforms (Network-based solutions)
- Leveraging Trusted Computing Elements

# *::What Are We Doing About It?*

- Emerging **Infrastructure**
- Converged Compute, Network & Storage solutions emerging
- Virtualization Platforms evolving
- IP NGN's deploying
- Crippling **Metastructure**
- Struggling with **Infostructure**





# *::What Are We Doing About It?*

- Emerging Infrastructure
- Crippling **Metastructure**
  - DNSSec
  - BGP Extensions
  - IPv6
  - LISP, HIP, etc...
  - Open API's & Interfaces
- Struggling with Infostructure





# ::What Are We Doing About It?

- Emerging Infrastructure
- Crippling Metastructure
- Struggling with Infostructure
  - We still have buffer overflows
  - The Browser Battle is lost
  - Applying L1-6 "solutions" to Layer 7 & 8 "problems"
  - Totally disconnected from Metastructure & Infrastructure



*::Cloud...*

We made the  
mess, now it's  
time we started  
thinking about  
how to clean it  
up...



# More Resources...

## **Cloud Computing**

<http://groups.google.com/group/cloud-computing>

## **Cloud Computing Interoperability Forum**

<http://groups.google.com/group/cloudforum>

## **Cloud Storage**

<http://groups.google.com/group/cloudstorage>

**Attend a local**  **CloudCamp**

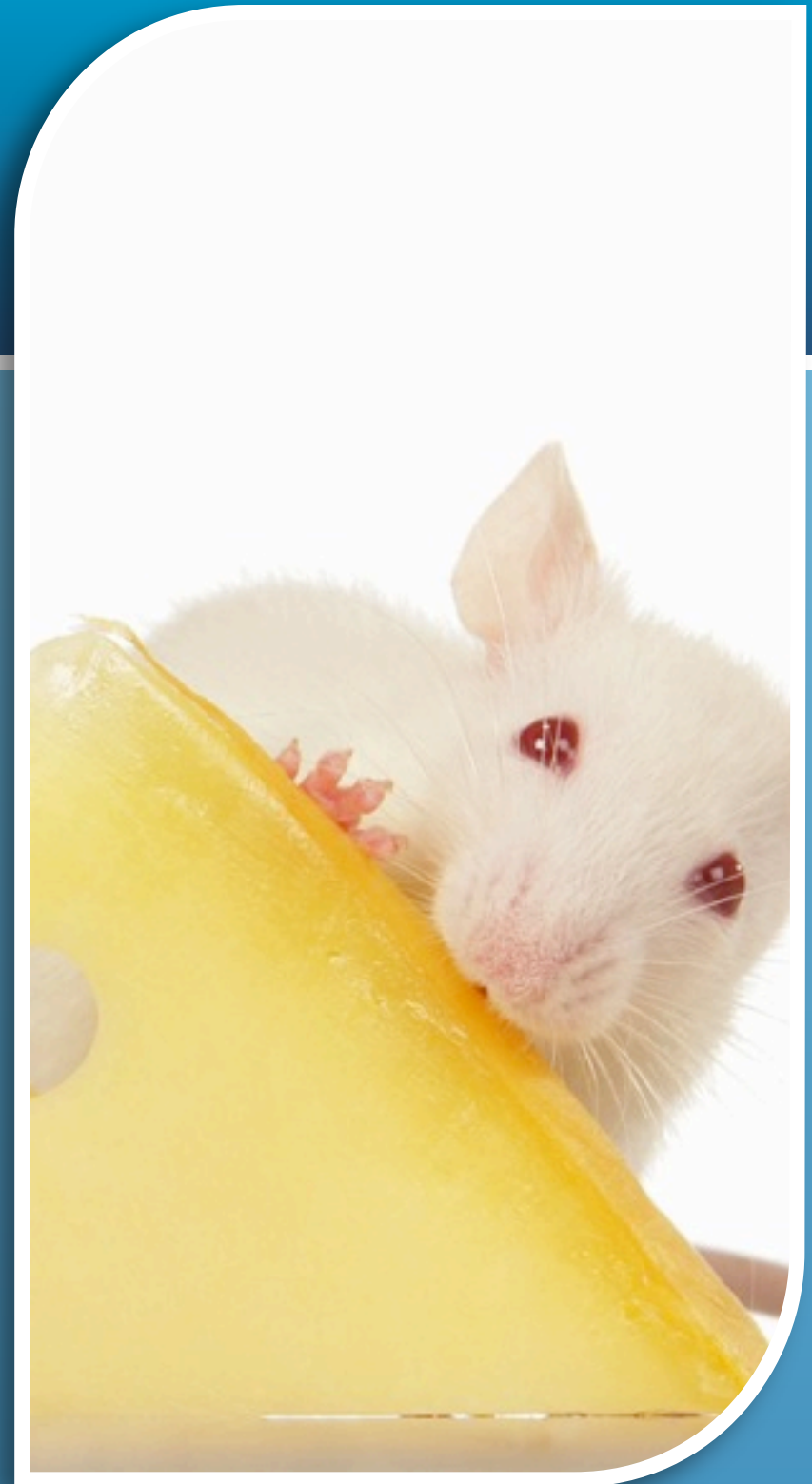
**Read Craig Balding's Blog** <http://www.cloudsecurity.org>

**Read My Blog:** <http://www.rationalsurvivability.com>



# Someone Moved My Cybercheese...

- People who would not ordinarily think about security are doing so
- While we're scrambling to adapt, we're turning over rocks and shining lights in dark crevices
- Sure, Bad Things™ will happen
- But, Really Smart People™ are engaging in meaningful dialog & starting to work on solutions
- You'll find that much of what you have works...perhaps just differently; setting expectations is critical





IF It All Comes Down To Trust...



What are we going to differently about who  
we trust, how and why?

*Thanks*

**HACKERS FOR CHARITY.ORG**

Name: Christofer HOFF

Twitter: @Beaker

Email: [choff@packetfilter.com](mailto:choff@packetfilter.com)

-or-

[hoffc@cisco.com](mailto:hoffc@cisco.com) [work]

Blog:

[www.rationalsurvivability.com](http://www.rationalsurvivability.com)

Phone: +1.978.631.0302

