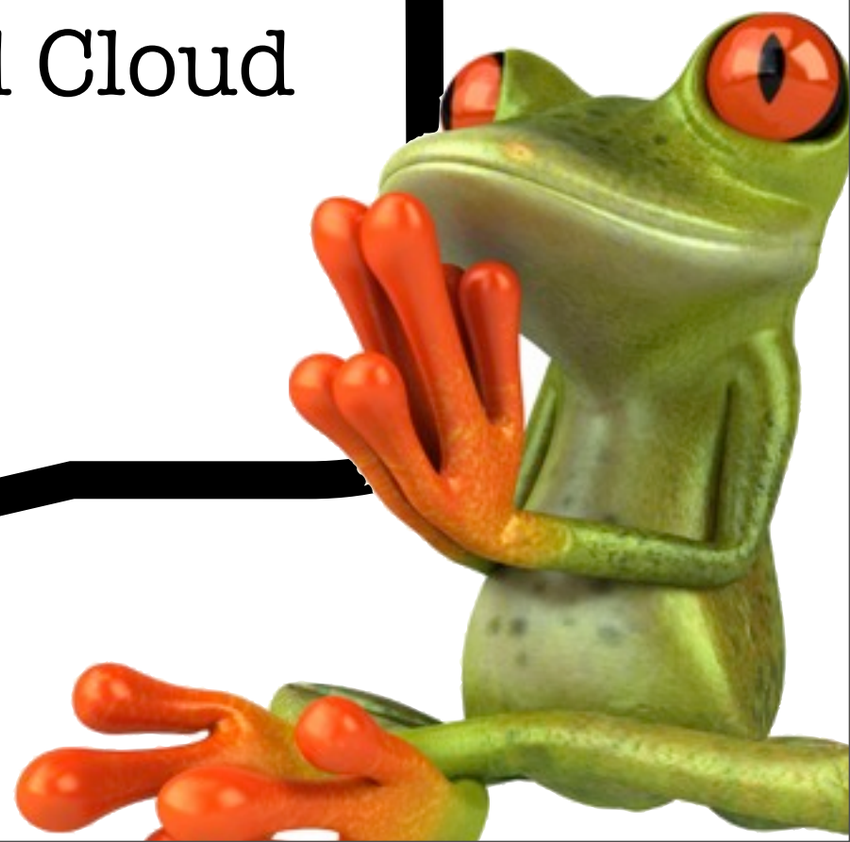
The Frogs Who Desired a King

A Virtualization & Cloud Computing Security Fable

Set To Interpretive Dance

What We'll Discuss

- Æsop's: The Frogs Who Desired a King
- Defining "The Cloud"
- The Fable of Virtualization and Cloud Computing Security
- Deal With It



Æsop's Frogs

Hoff | The Frogs Who Desired a King | 2009

Kermit and Krew...

Deity With a Sense Of Humor

Frogs On a Log

The Bossy Bird

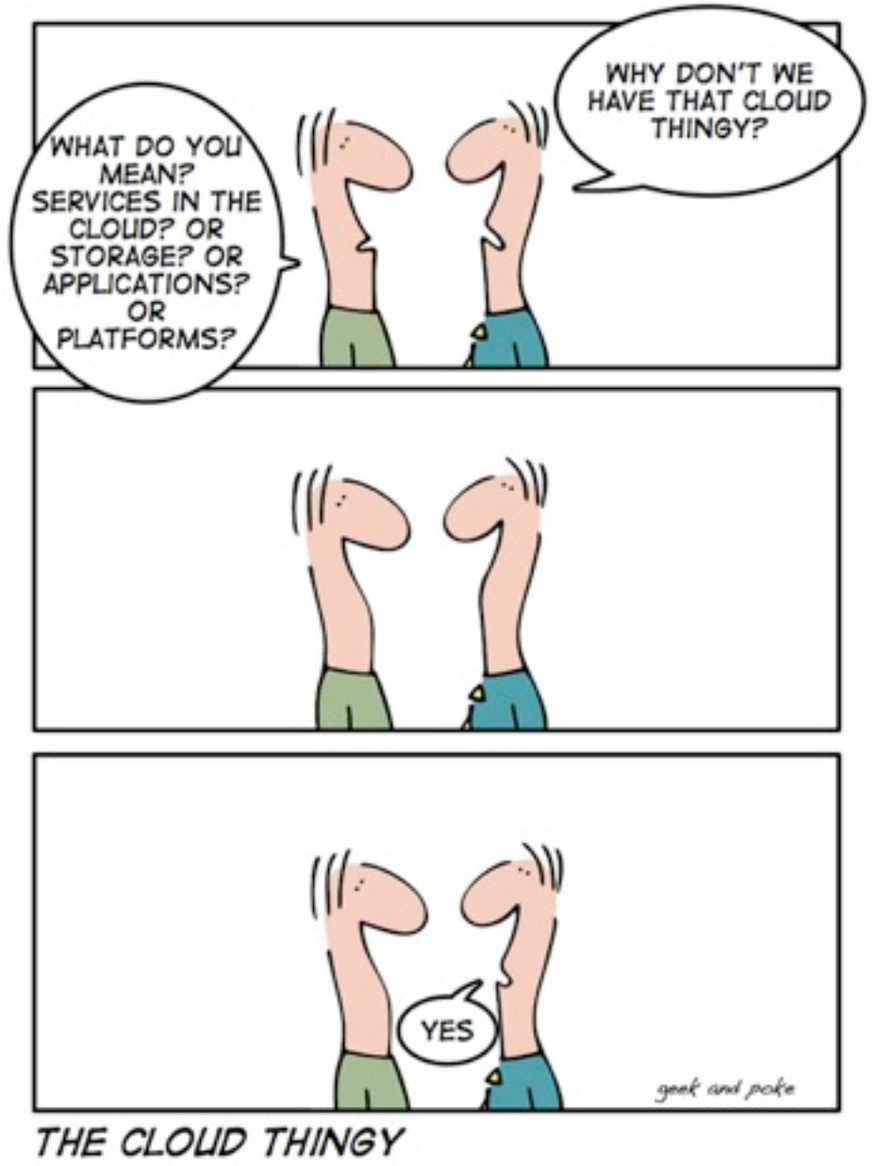
Buffet In the Bayou

The Point

"King stork was welcome to
replace a log,

They tittered at the thrill,
then hushed, agog."*

*Thom Gunn "The Court Revolt"


WHAT DO YOU MEAN? SERVICES IN THE CLOUD? OR STORAGE? OR APPLICATIONS? OR PLATFORMS?
WHY DON'T WE HAVE THAT CLOUD THINGY?
YES
geek and poke
THE CLOUD THINGY

The Cloud

What the !@#$% IS Cloud Computing?

Cloud :: The Obligatory Definition

IT resources and services that are abstracted from the underlying infrastructure and provided "on-demand" and "at scale" in a multi-tenant environment

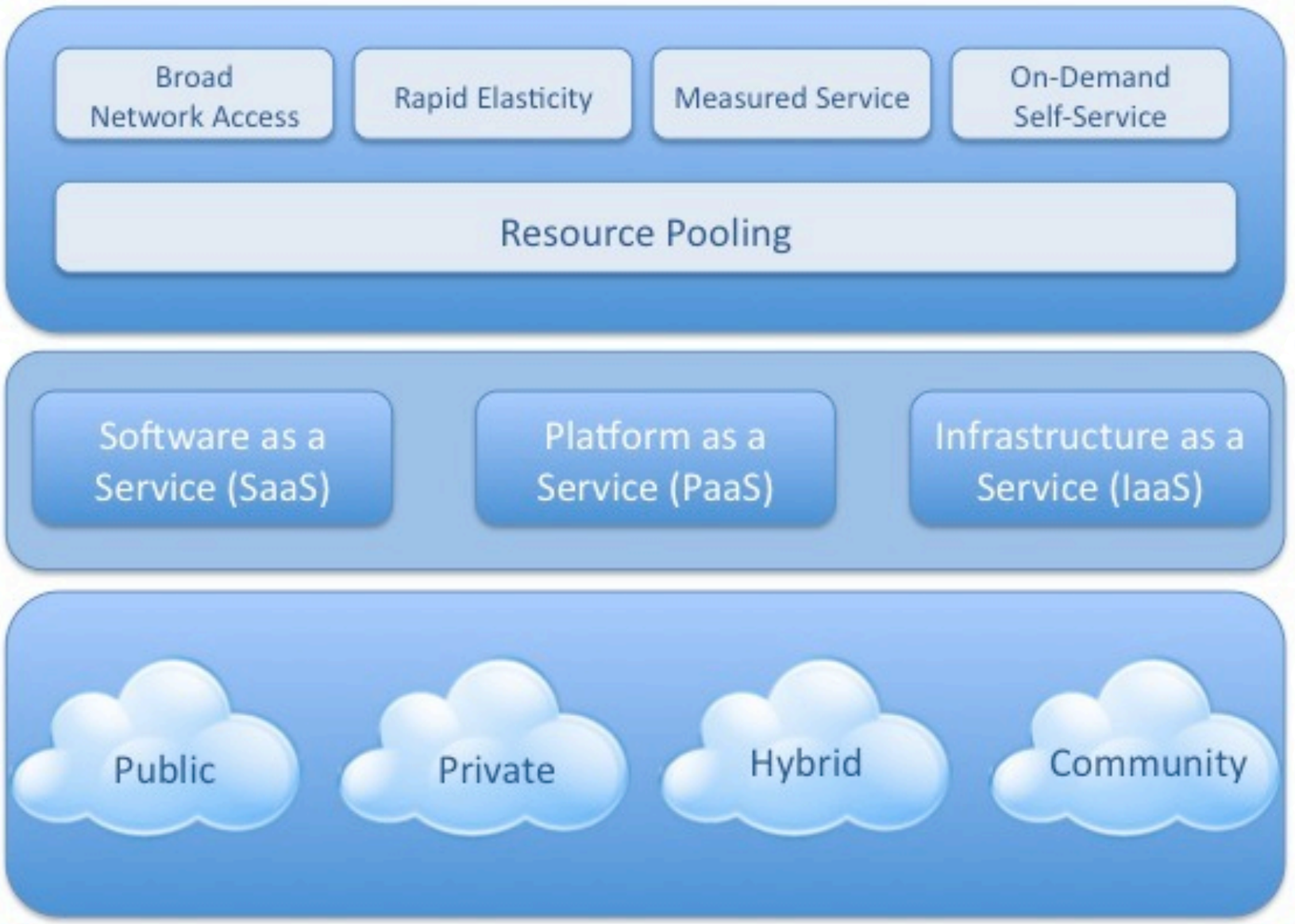
CloudWow! You'll Say "HOW?" Every Time...

Cutting Through the Fluff: Key Ingredients In Cloud Definition

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

Play NISTy For Me...

Visual Model Of NIST Working Definition Of Cloud Computing
http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html



Sir James (Urquhart) Has It Right...

"Cloud Is An Operations Model, Not A Technology"

Some Things Are Cloud Candidates...

Cloud Ready?

- When the processes, applications and data are largely independent
- When the points of integration are well defined
- When a lower level of security will work just fine
- When the core internal enterprise architecture is healthy
- When the Web is the desired platform
- When cost is an issue
- When the applications are new

*Used with permission from David Linthicum

...Others Not So Much

Not so Cloud Ready?

- When the processes, applications and data are largely coupled
- When the points of integration are not well defined
- When a high level of security is required
- When the core internal enterprise architecture needs work
- When the application requires a native interface
- When cost is not an issue
- When the applications are legacy

*Used with permission from David Linthicum

Cutting Through the Fluff: The SPI Cloud Model

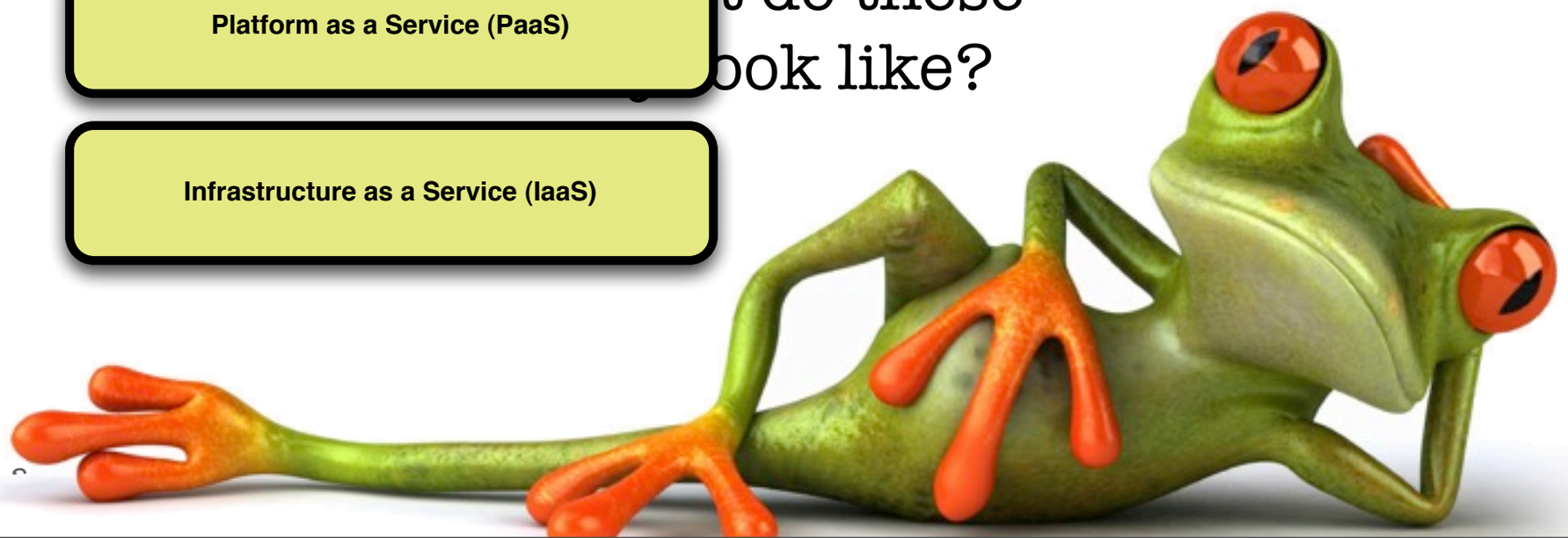
- Three archetypal models that people talk about about when they say “Cloud:”

Software as a Service (SaaS)

Platform as a Service (PaaS)

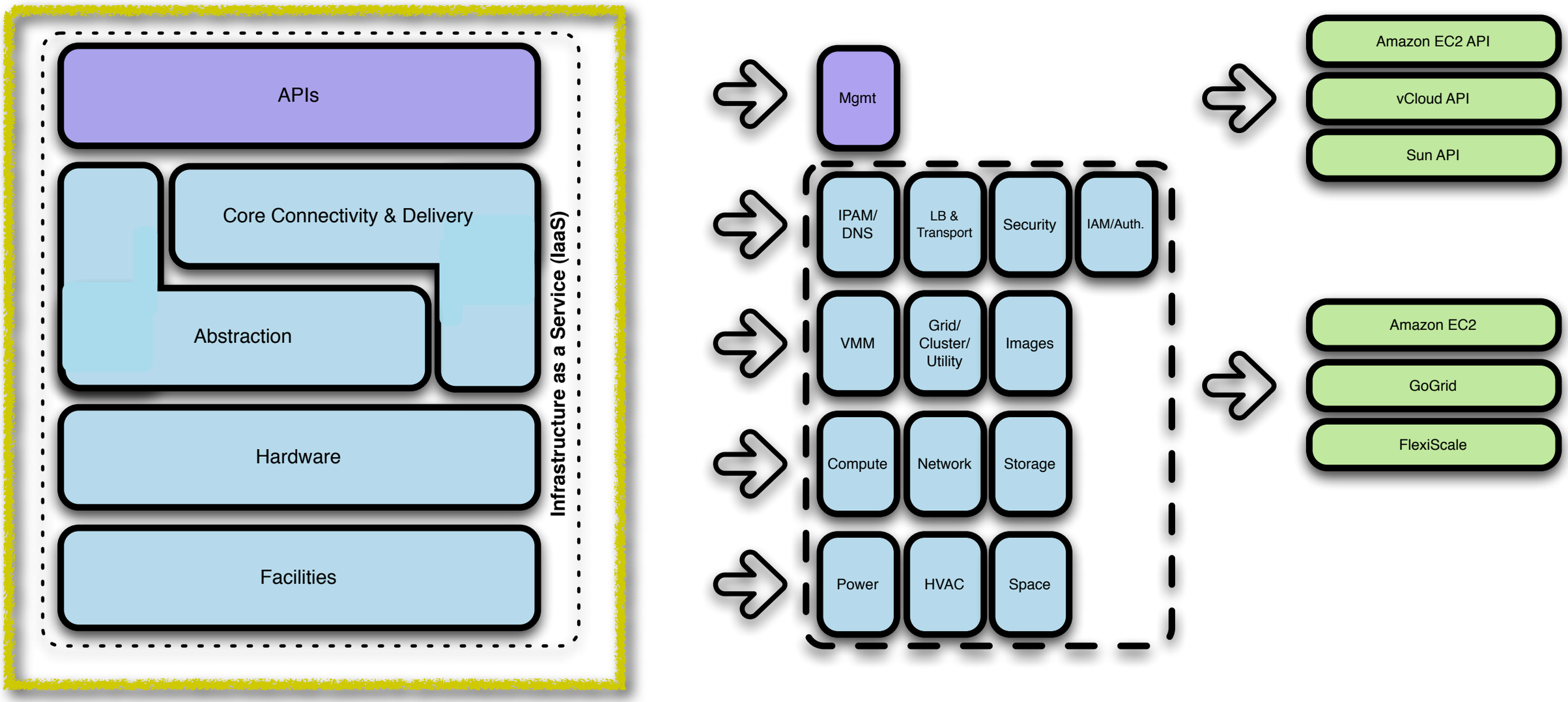
Infrastructure as a Service (IaaS)

t do these
ook like?

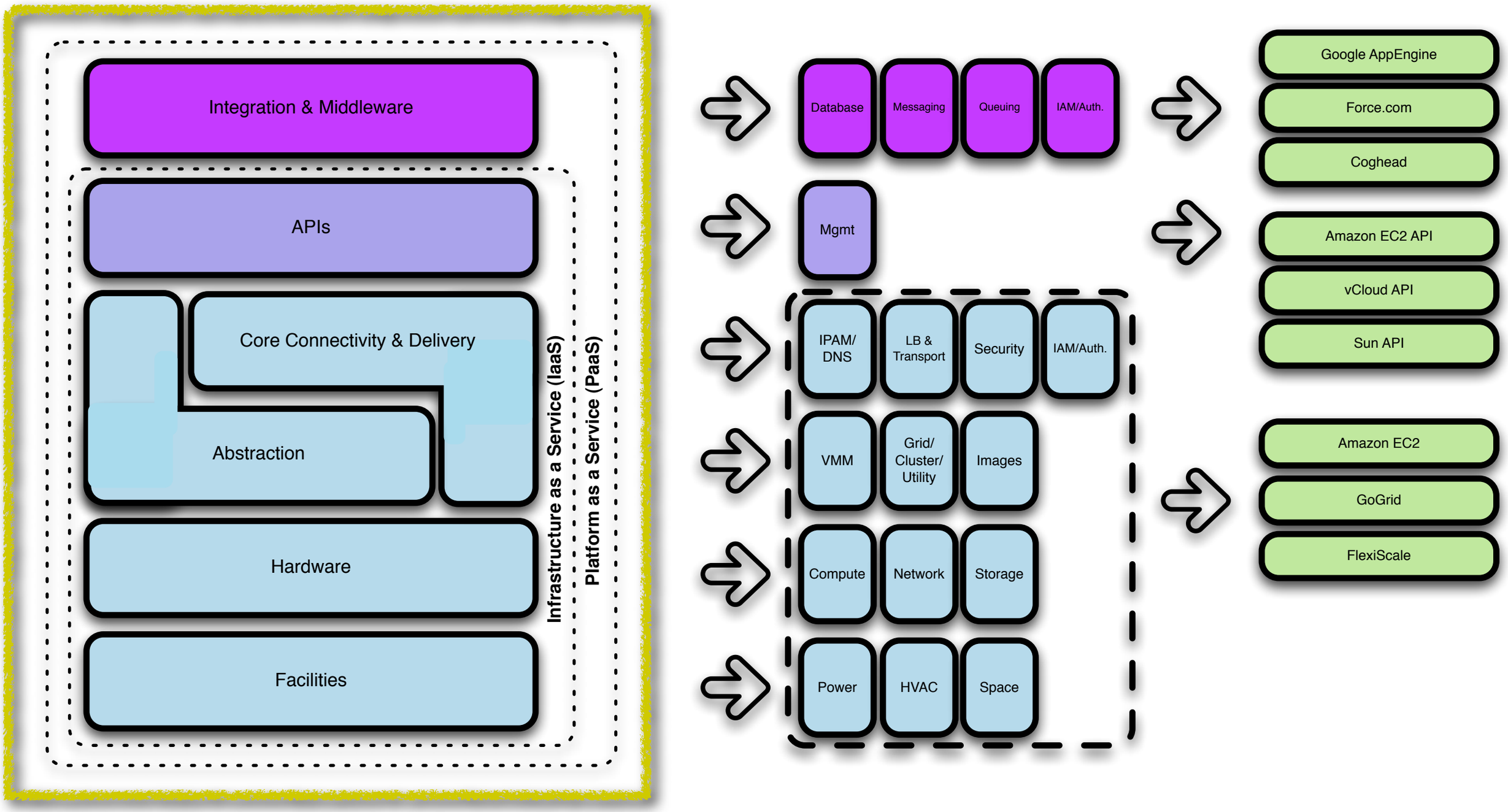


The Seven Layer Dip Answer...

Cloud Model :: Infrastructure as a Service (IaaS)

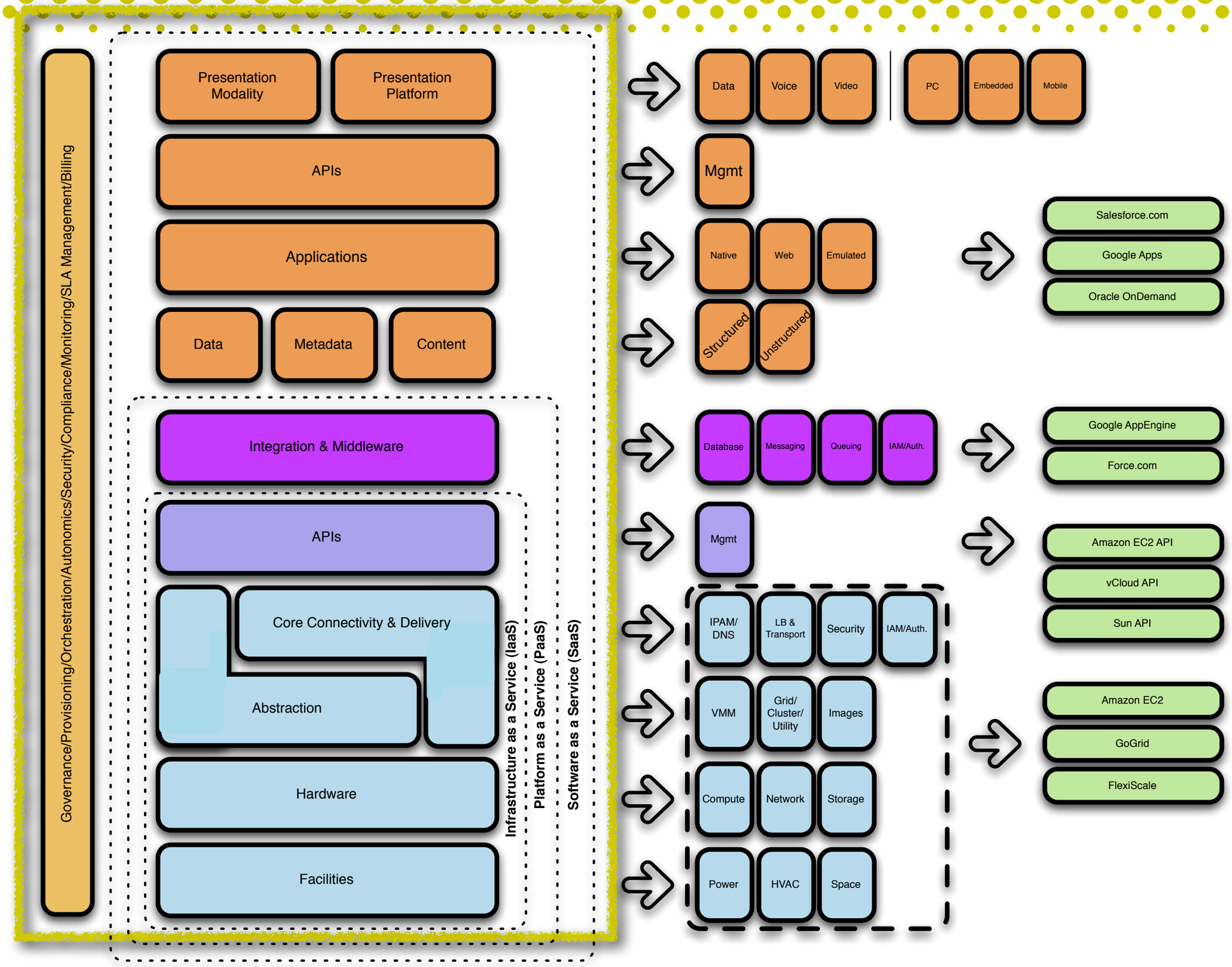


Cloud Model :: Platform as a Service (PaaS)



Hoff | The Frogs Who Desired a King | 2009

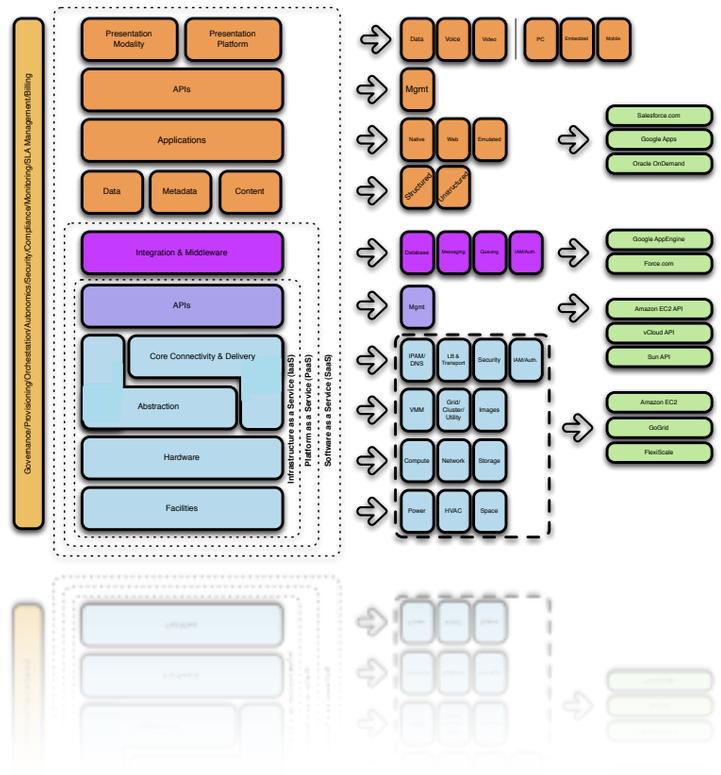
Cloud Model :: Software as a Service (SaaS)



Lots Of *aaSes...Variations On a Theme

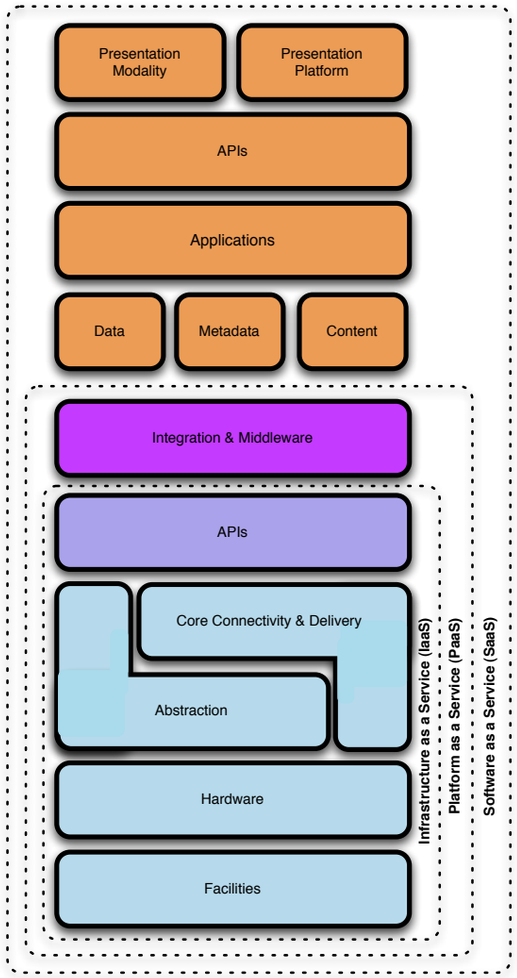
Packaging these up in combination yields lots of *aaS(es):

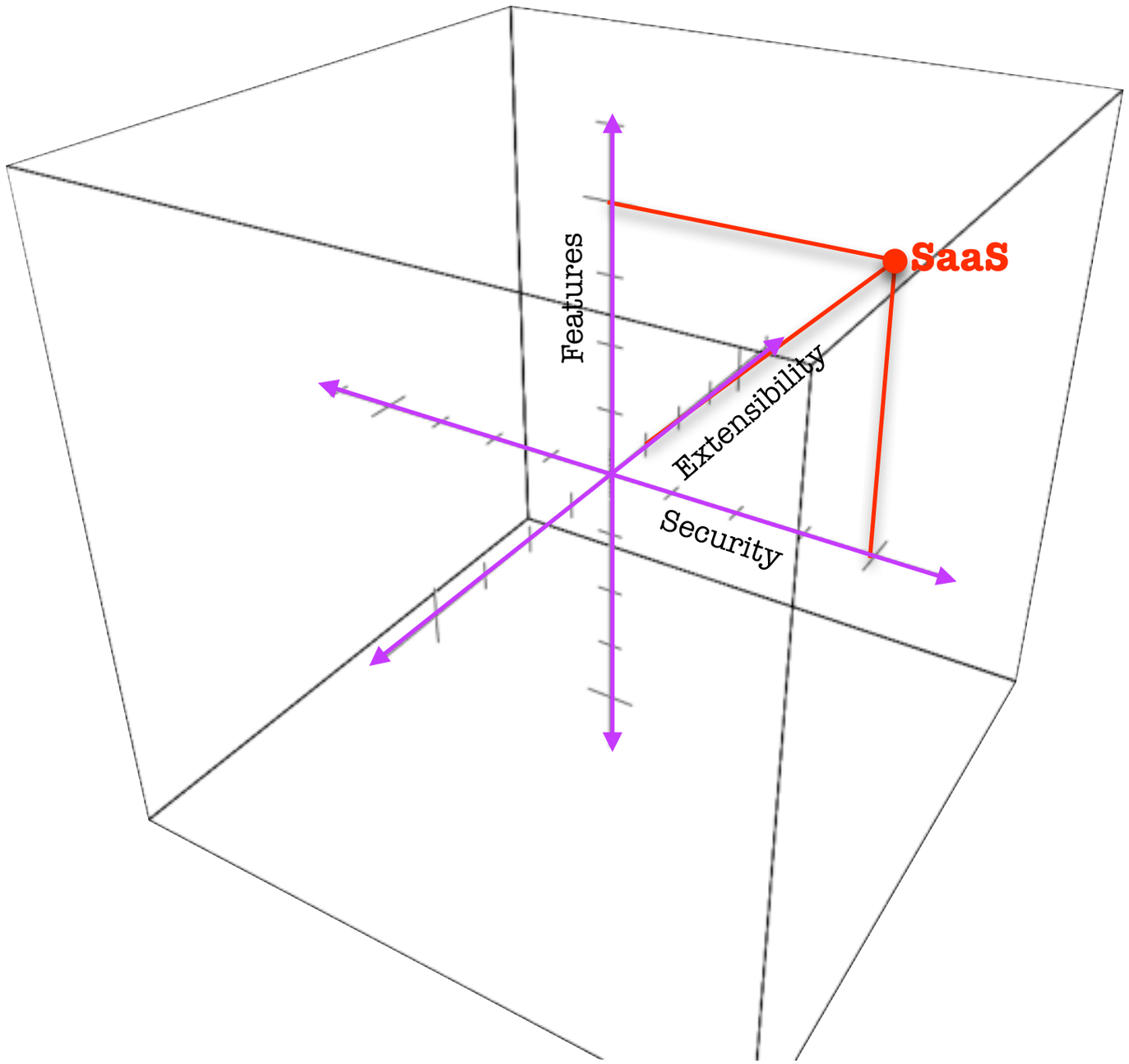
- Storage as a Service
- Database as a Service
- Information as a Service
- Process as a Service
- Integration as a Service
- Security as a Service
- Management as a Service
- Testing as a Service...



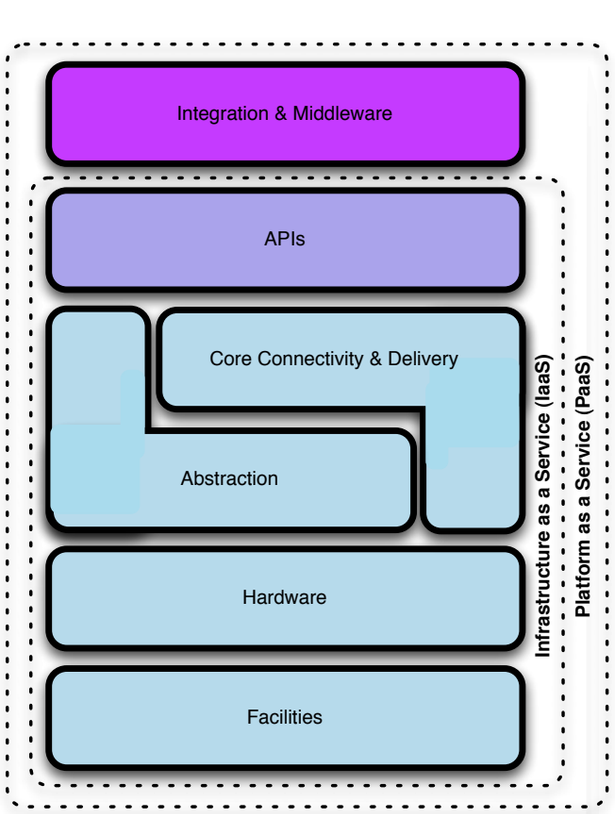
*David Linthicum: Defining the Cloud Computing Framework http://cloudcomputing.sys-con.com/node/811519

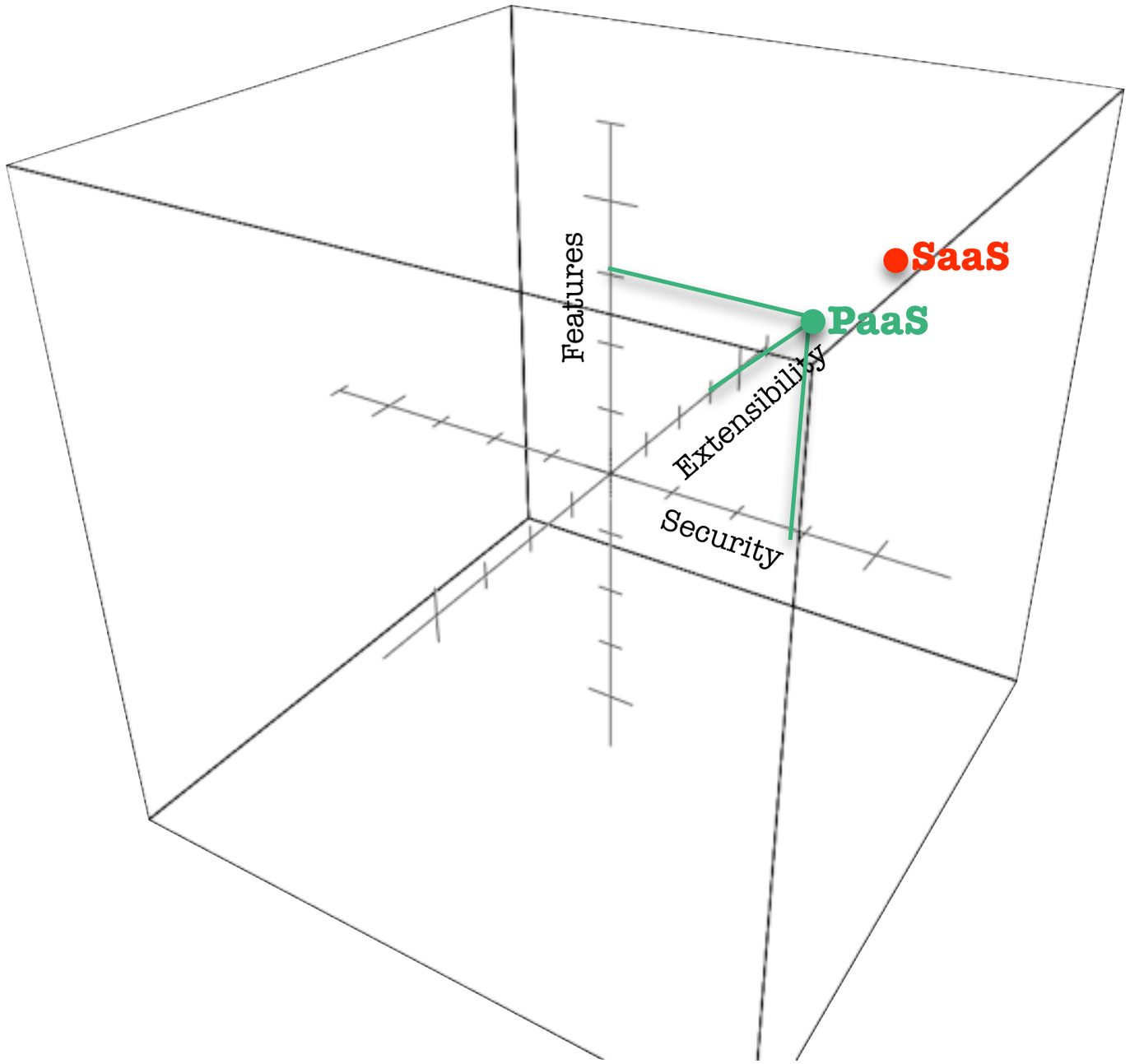
The Many Dimensions Of Cloud



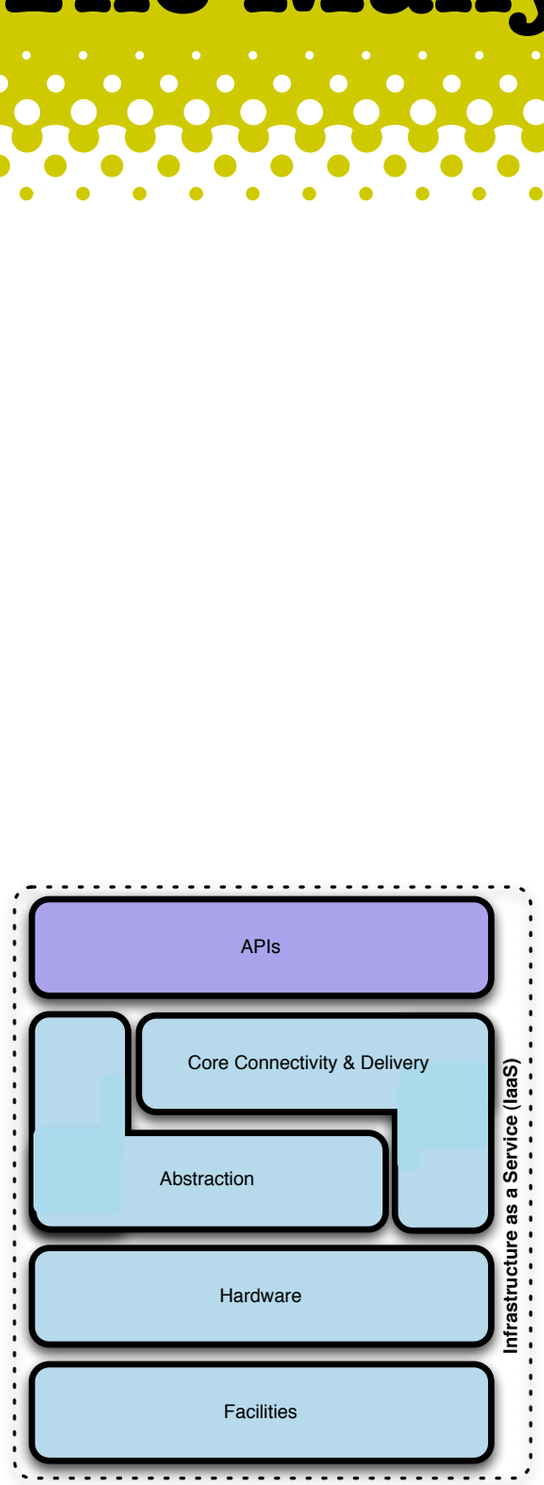


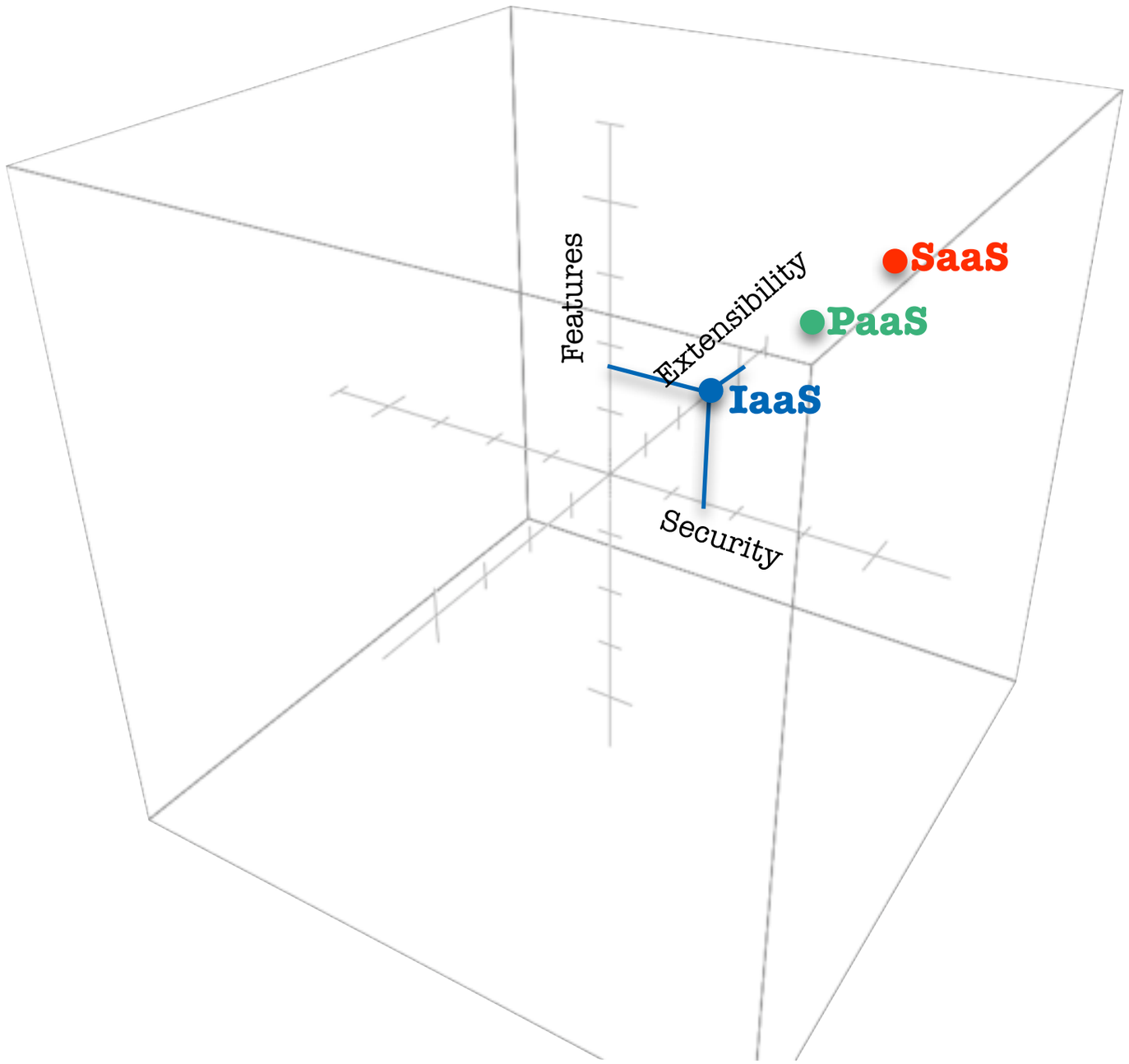
The Many Dimensions Of Cloud





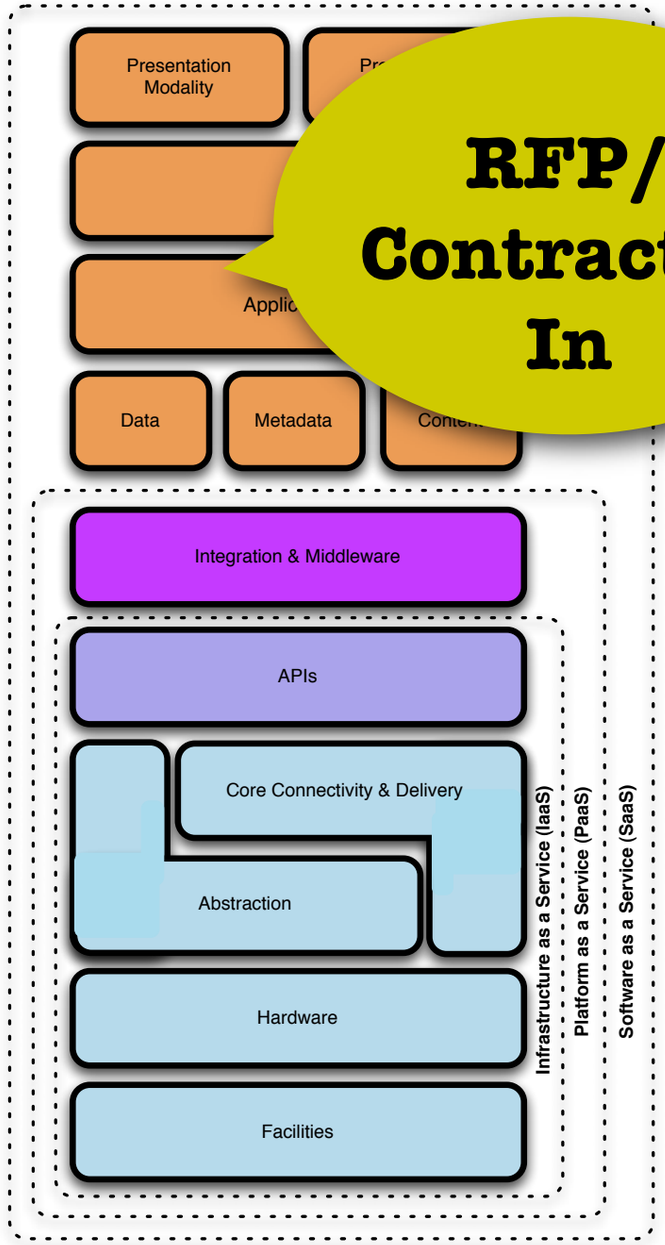
The Many Dimensions Of Cloud





What This Means To Security

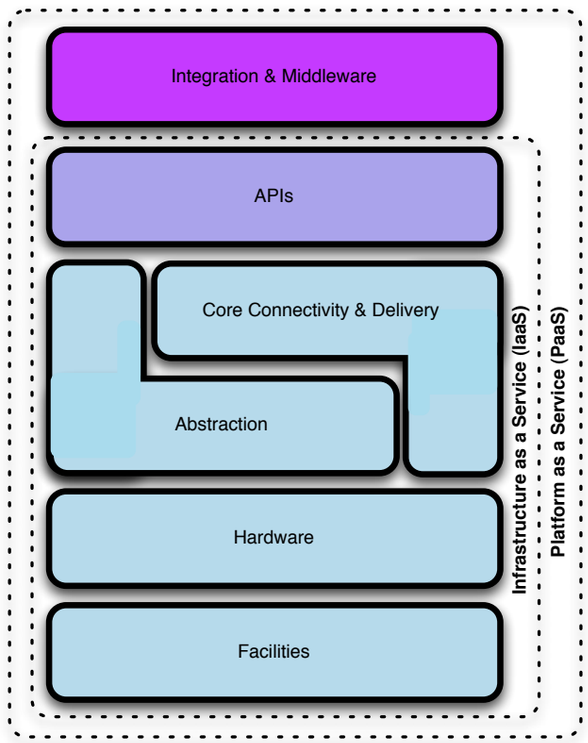
Salesforce - SaaS



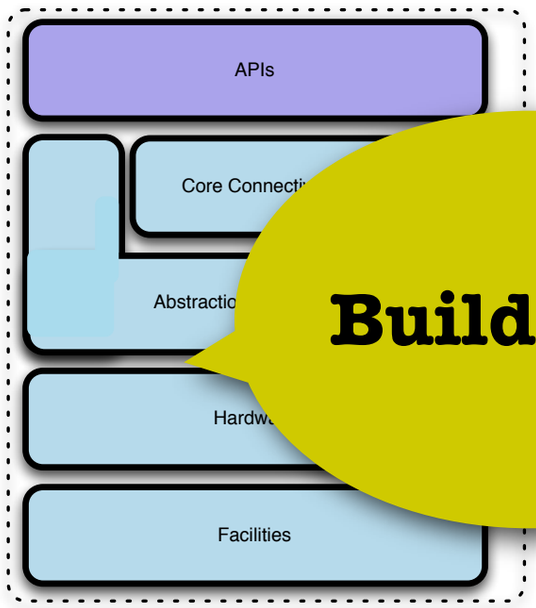
RFP/ Contract It In

The lower down the stack the Cloud provider stops, the more security **ou** are tactically responsible for plementing & managing yourself.

Google AppEngine - PaaS



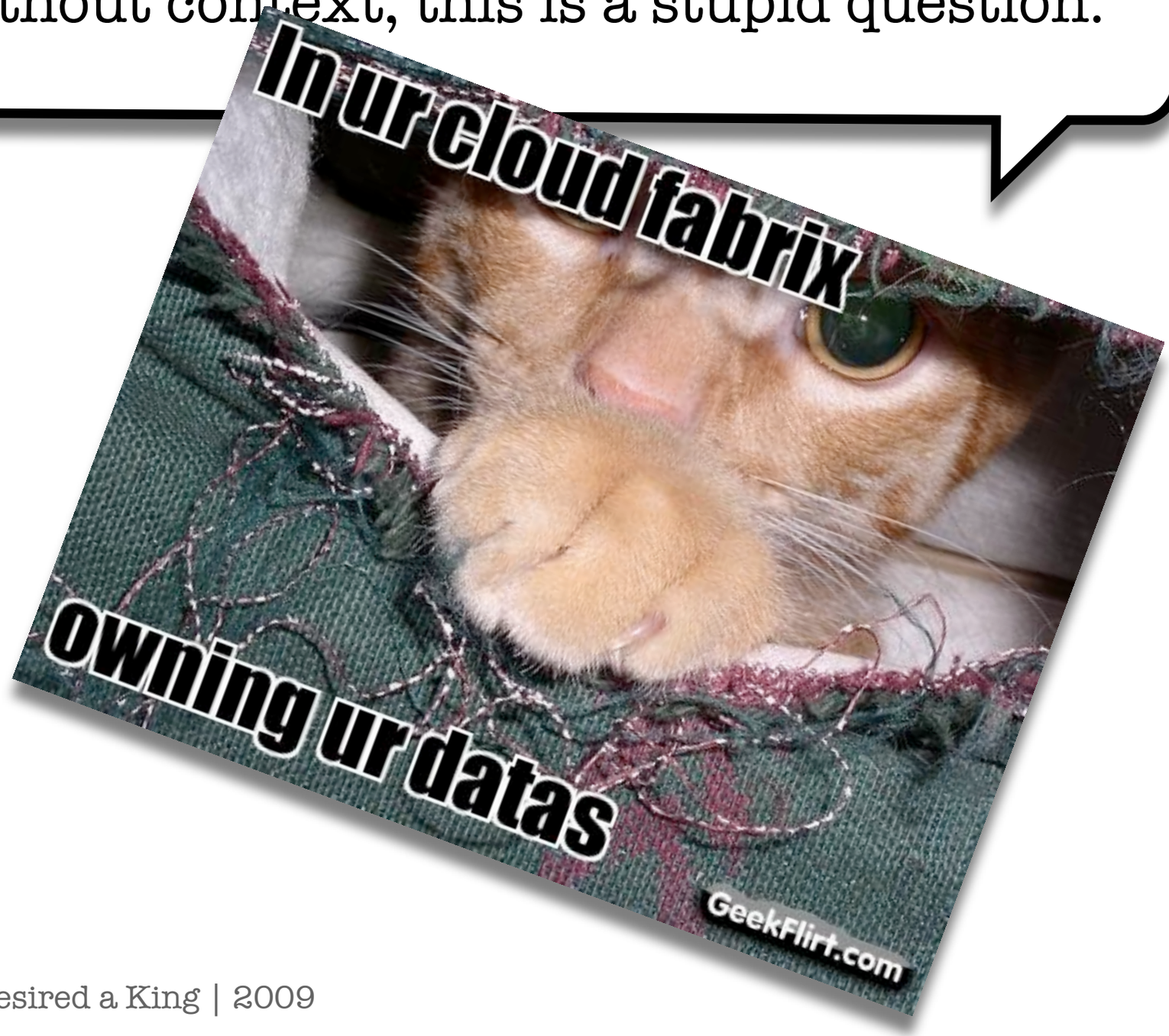
Amazon EC2 - IaaS



Build It In

Cloud: More or Less Secure?

Without context, this is a stupid question.



Reduction Of Risk? Really?

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

Be wary of how much of this song you sing (or hear being sung) given what we just discussed.

So How's That Different Than Outsourced Services Today?

The differences really come down to four things:

- The types of applications / data being "outsourced"
- Where your assets are
- Who manages them & how
- How controls are integrated

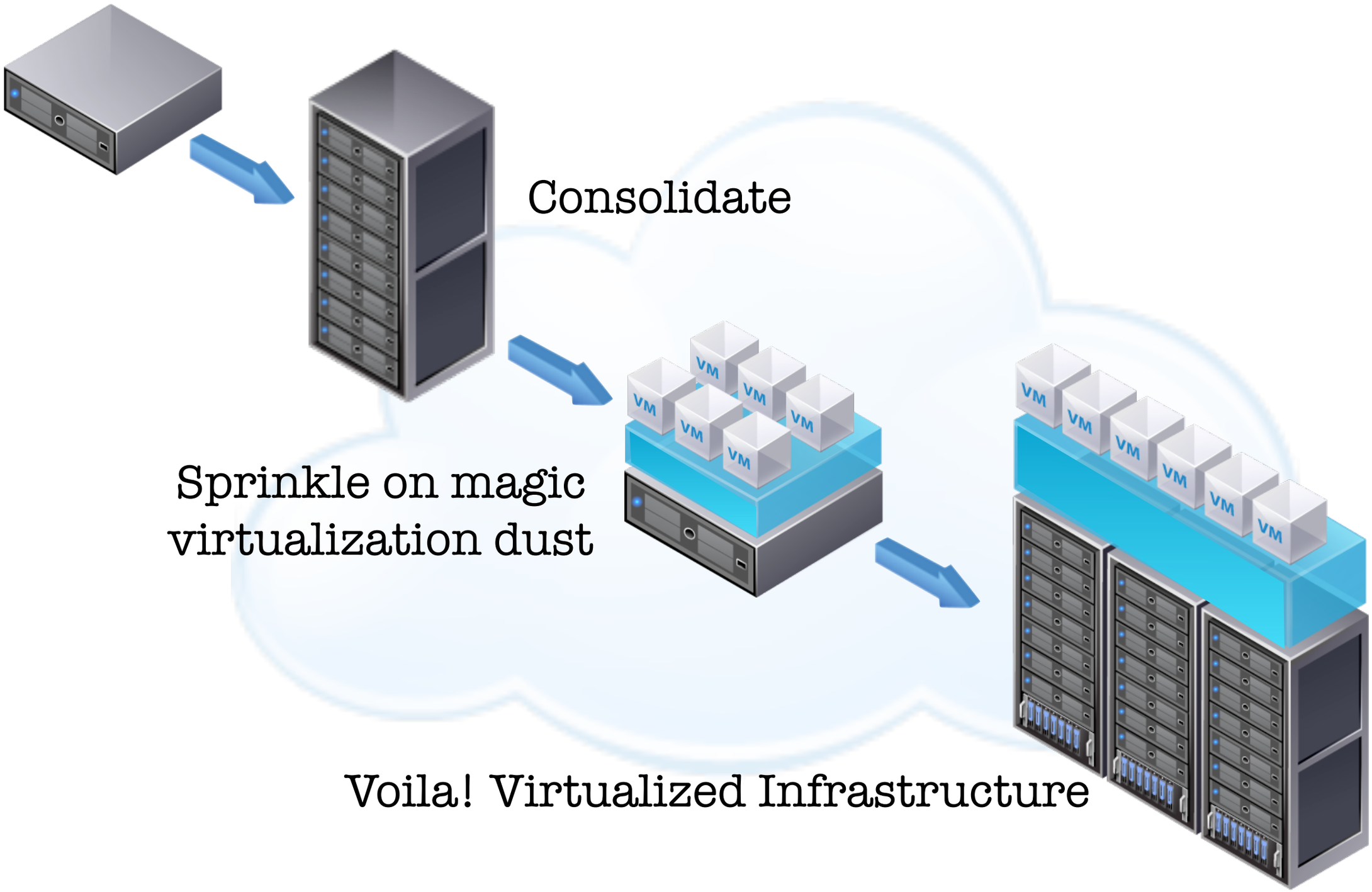
...Peeling Back the Covers

The things that go bump in the night:

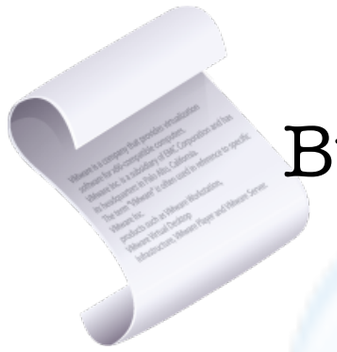
- Single Tenancy / Multi-tenancy
- Isolated Data / Co-mingled Data
- Dedicated Security / Socialist Security
- On-premise / Off-premise

A Typical Large Enterprise's Forward-Looking Journey to the Cloud

Phase One: Virtualize



Phase Two: Automate & Optimize



Business Process & Rules via the governance layer

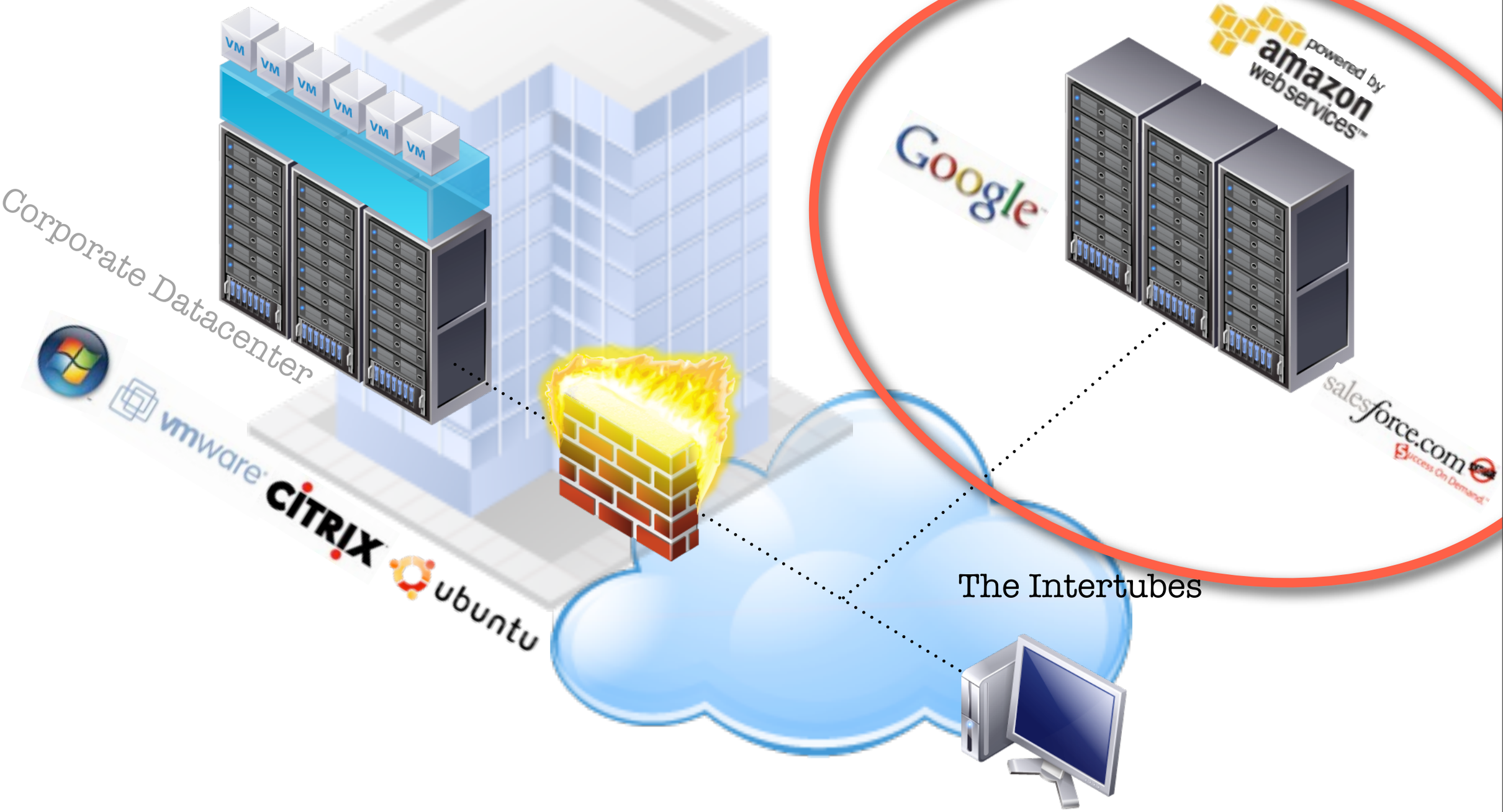
Feeds into and out of the autonomics layer:

Yielding an adaptive pool of resources, applications and services abstracted from the infrastructure that delivers it.

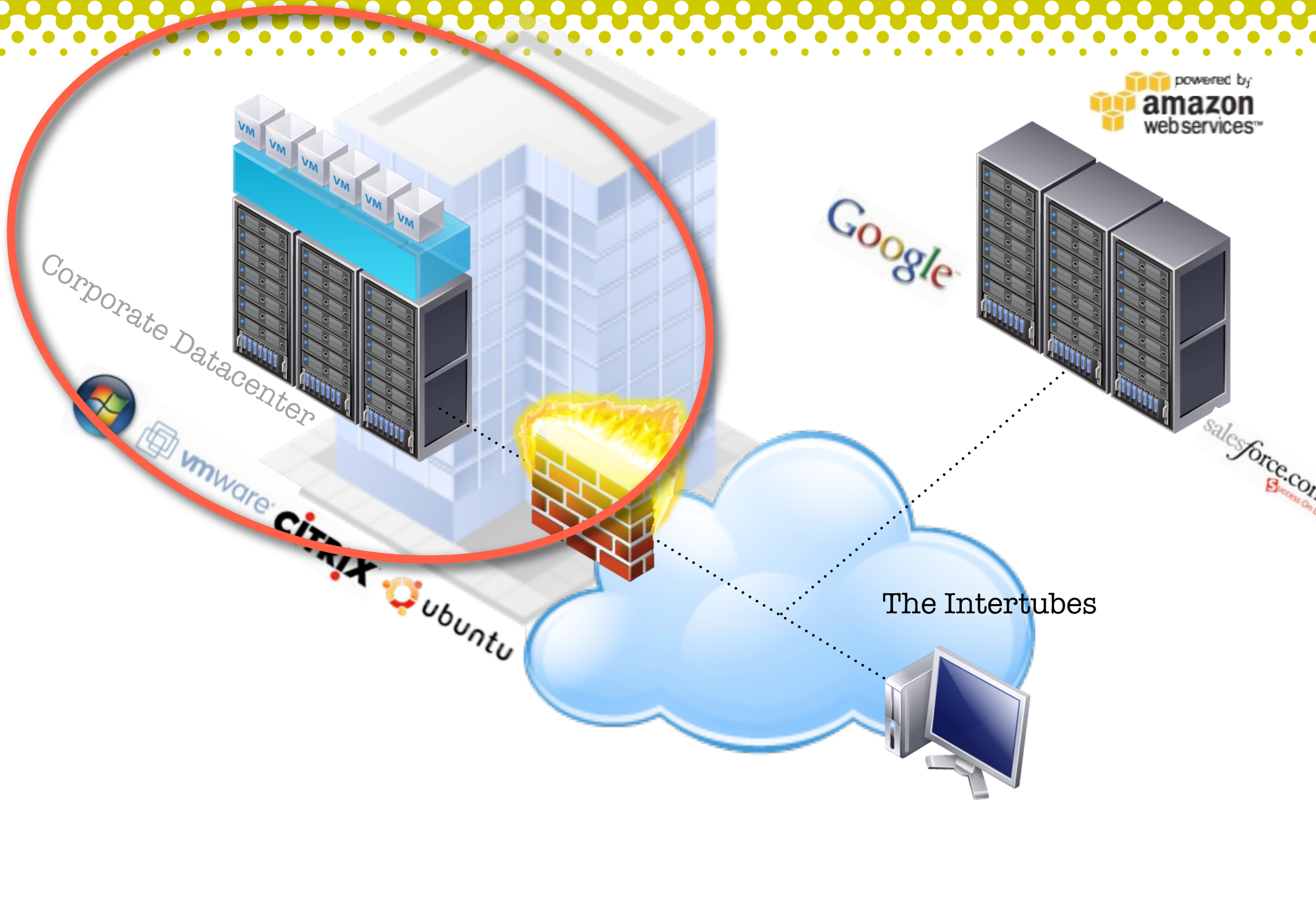
Phase Three: Externalize & Re-Perimeterize

Perspective: Public vs. Private Clouds

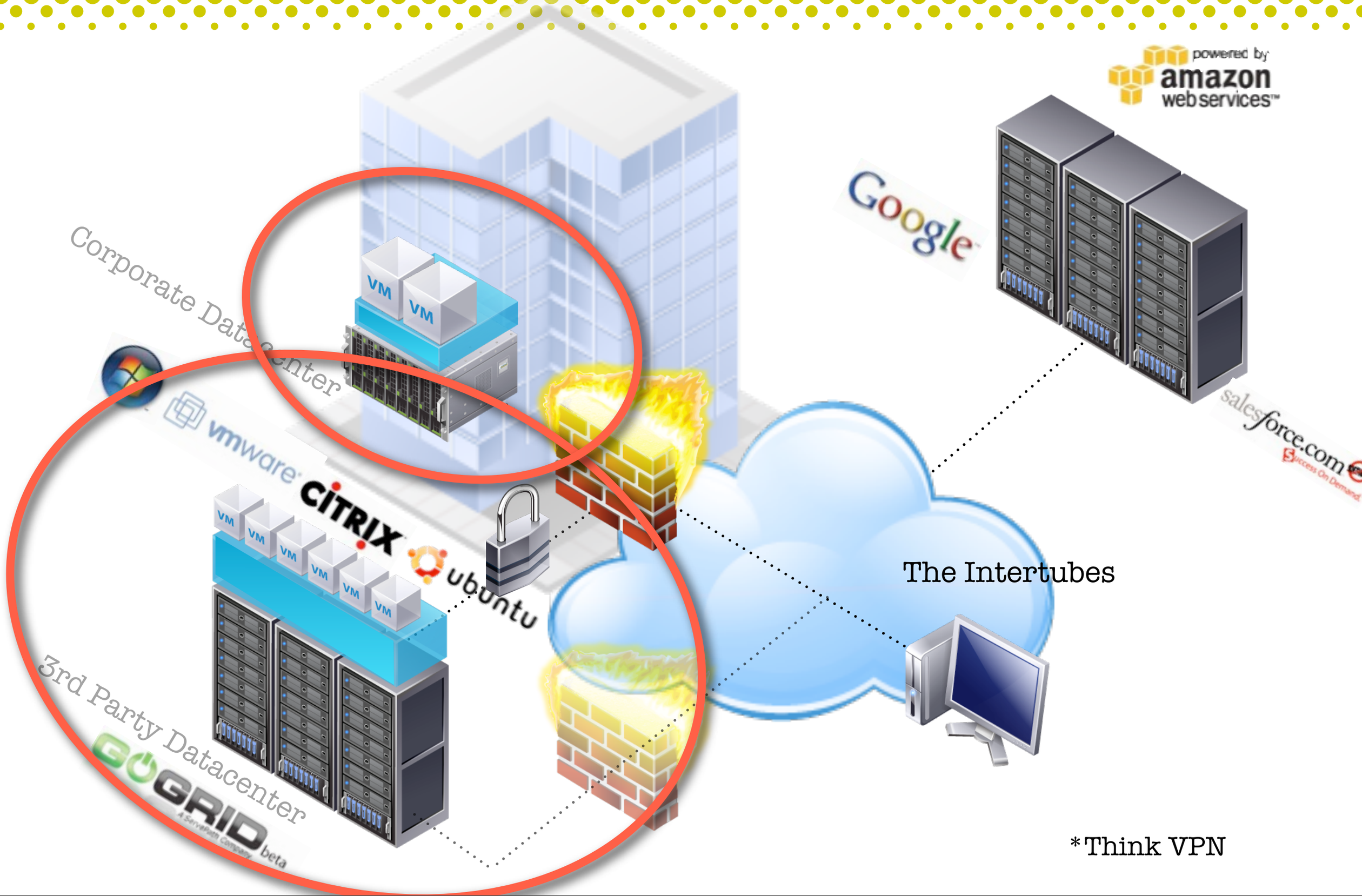
The Public Cloud :: External via the Internet



THEIR Private Cloud :: Amazon-ize Your Intranet

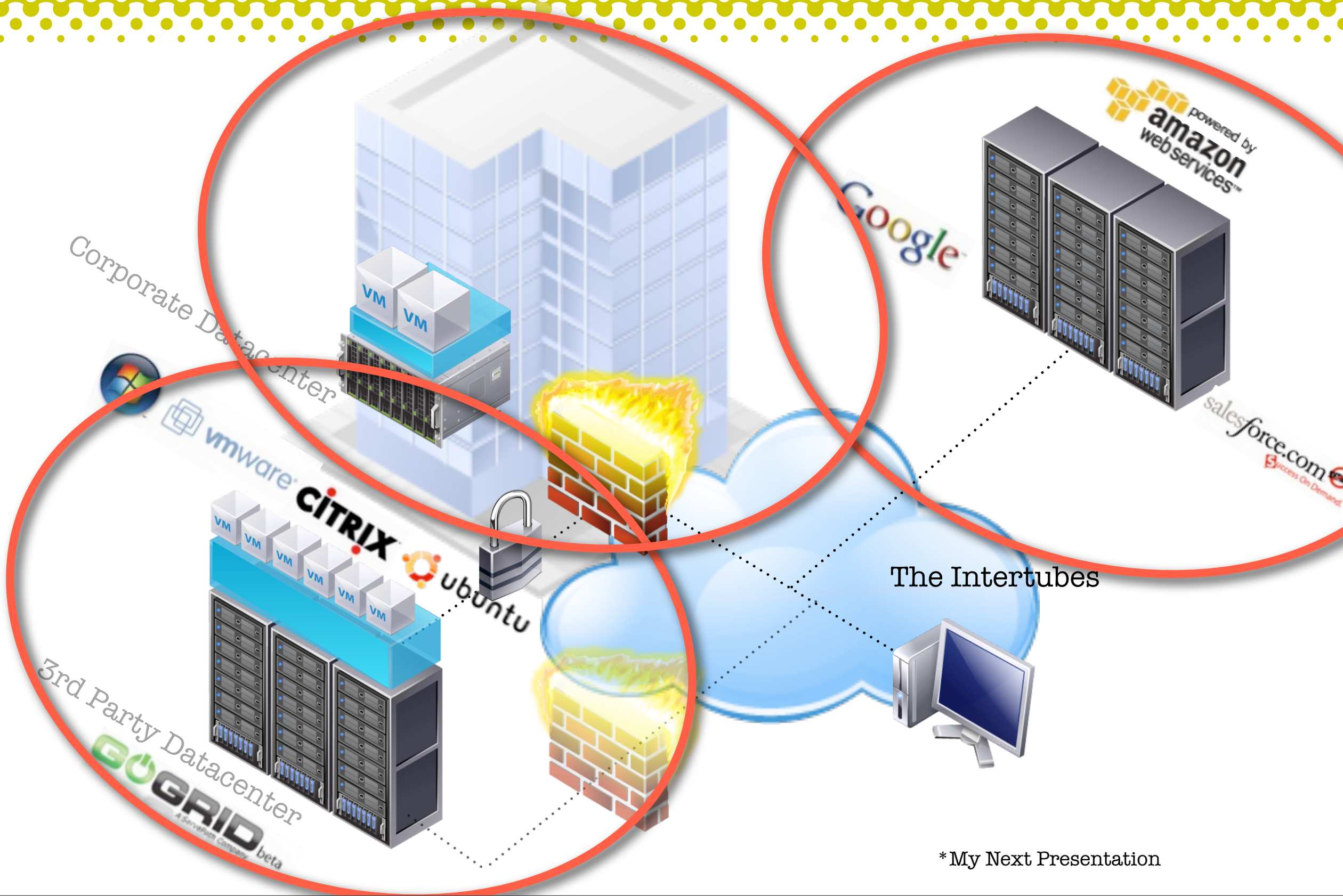


My Private Cloud :: Internal via the Intranet *



*Think VPN

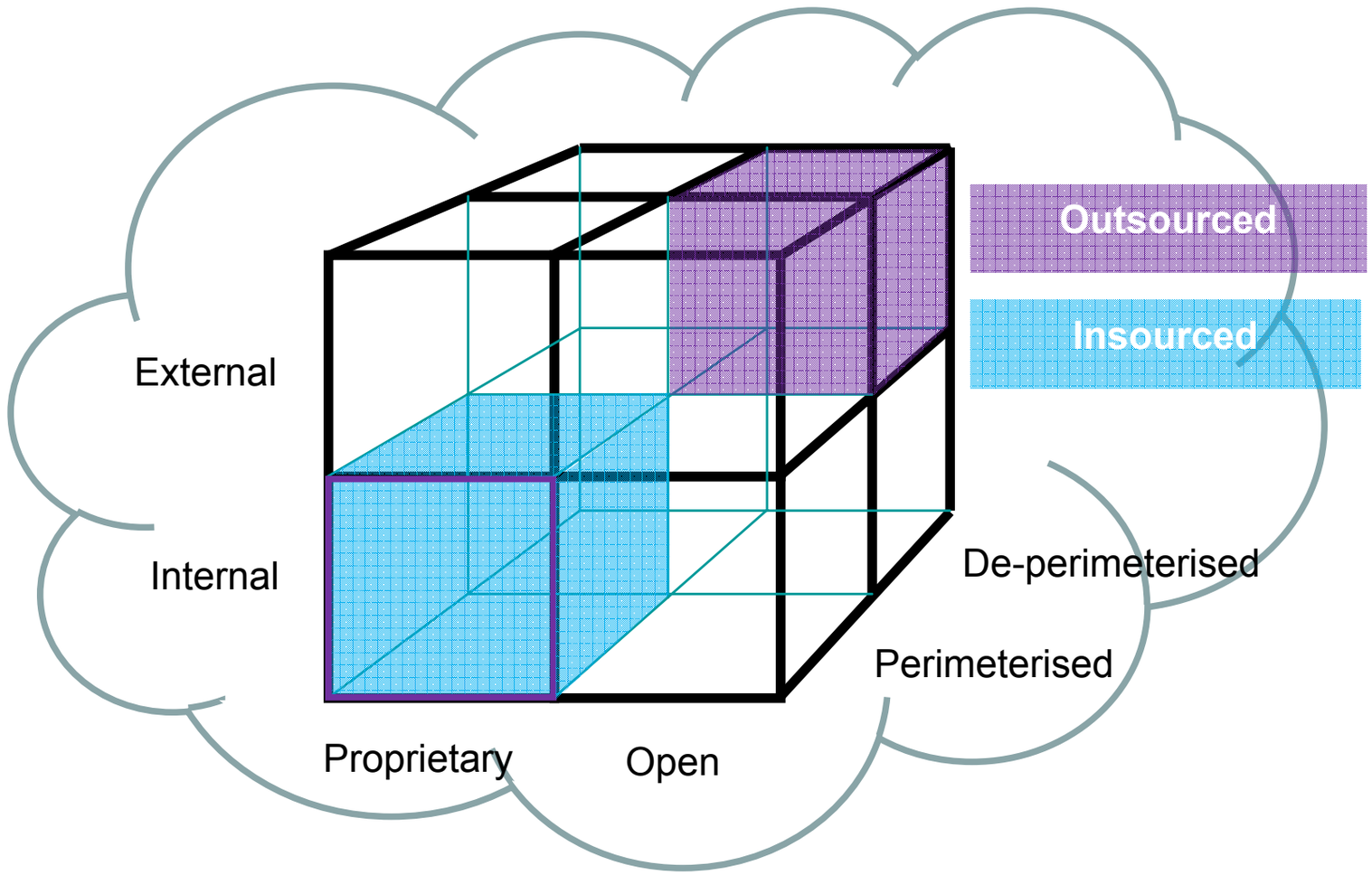
The Hybrid Model :: Cloudifornication *



*My Next Presentation

The Jericho Forum's Cloud Cube Model

Ⓥ Rubik's Rubric: A Great Way To Visualize Cloud Options...



The Cloud Cube Model

Hoff's Two Dimensional Version

ⓥ Defining Cloud Implementations:

	Managed By[1]	Infrastructure Owned By[2]	Infrastructure Located[3]	Accessible and Consumed By[4]
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Private	Organization / Third Party Provider	Organization / Third Party Provider	On-Premise / Off-Premise	Trusted
Hybrid	Both Organization & Third Party Provider	Both Organization & Third Party Provider	Both On-Premise & Off-Premise	Trusted & Untrusted

[1] *Management includes: operations, security, compliance, etc…*
[2] *Infrastructure implies physical infrastructure such as facilities, compute, network & storage equipment*
[3] *Infrastructure Location is both physical and relative to an Organization's management umbrella and speaks to ownership versus control*
[4] *Trusted consumers of service are those who are considered part of an organization's legal/contractual/ policy umbrella including employees, contractors, & business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.*

Laying Out the Timeline...

Phase 1

Stand-Alone Data Centers

Phase 2

Private Cloud

Virtual Private Cloud

Public Cloud

Phase 3

Private Cloud

Hybrid Cloud

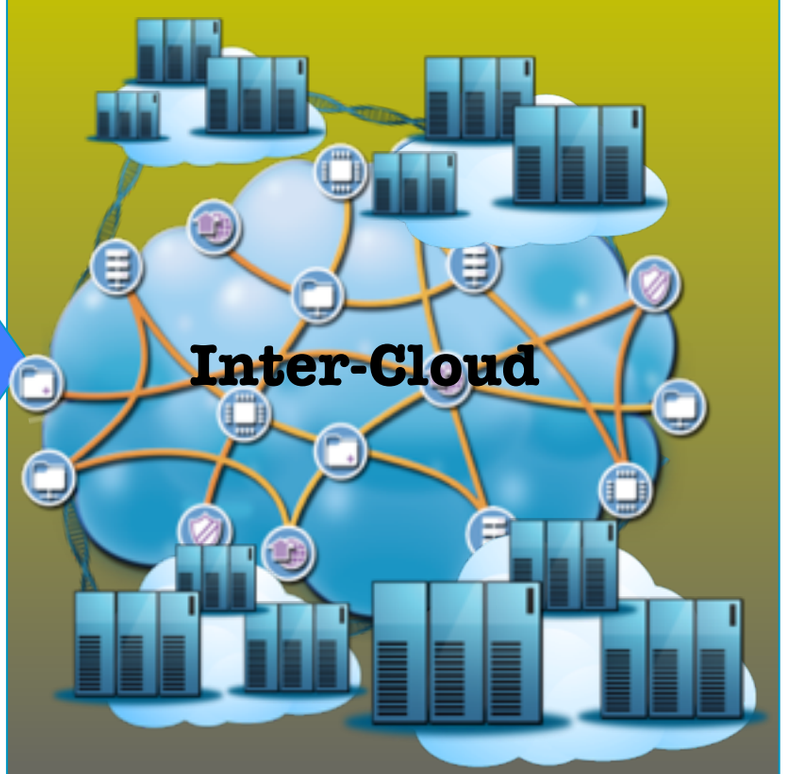
Public Cloud

Phase 4

Open Cloud

Private Cloud

Private Cloud



Inter-Cloud

Public Cloud #1

Public Cloud #2

PRESENT

~2015-2017

Federation / Workload Portability / Interoperability

...and Here We Go

YouTube
Broadcast Yourself ™

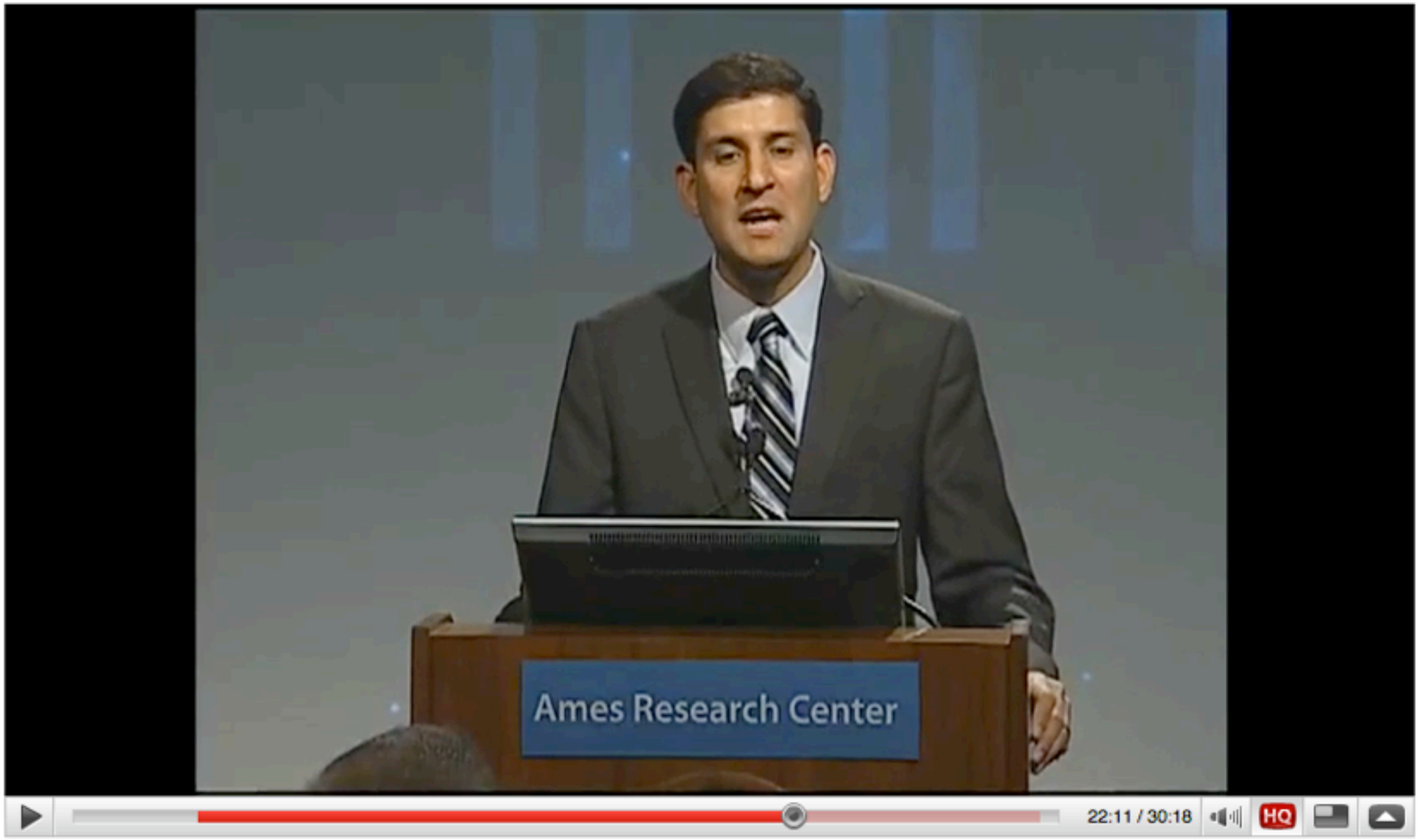
Search

ChristoferHoff ▾ Sign Out

Home Videos Channels Shows

Subscriptions History Upload

Administration Cloud Computing Announcement

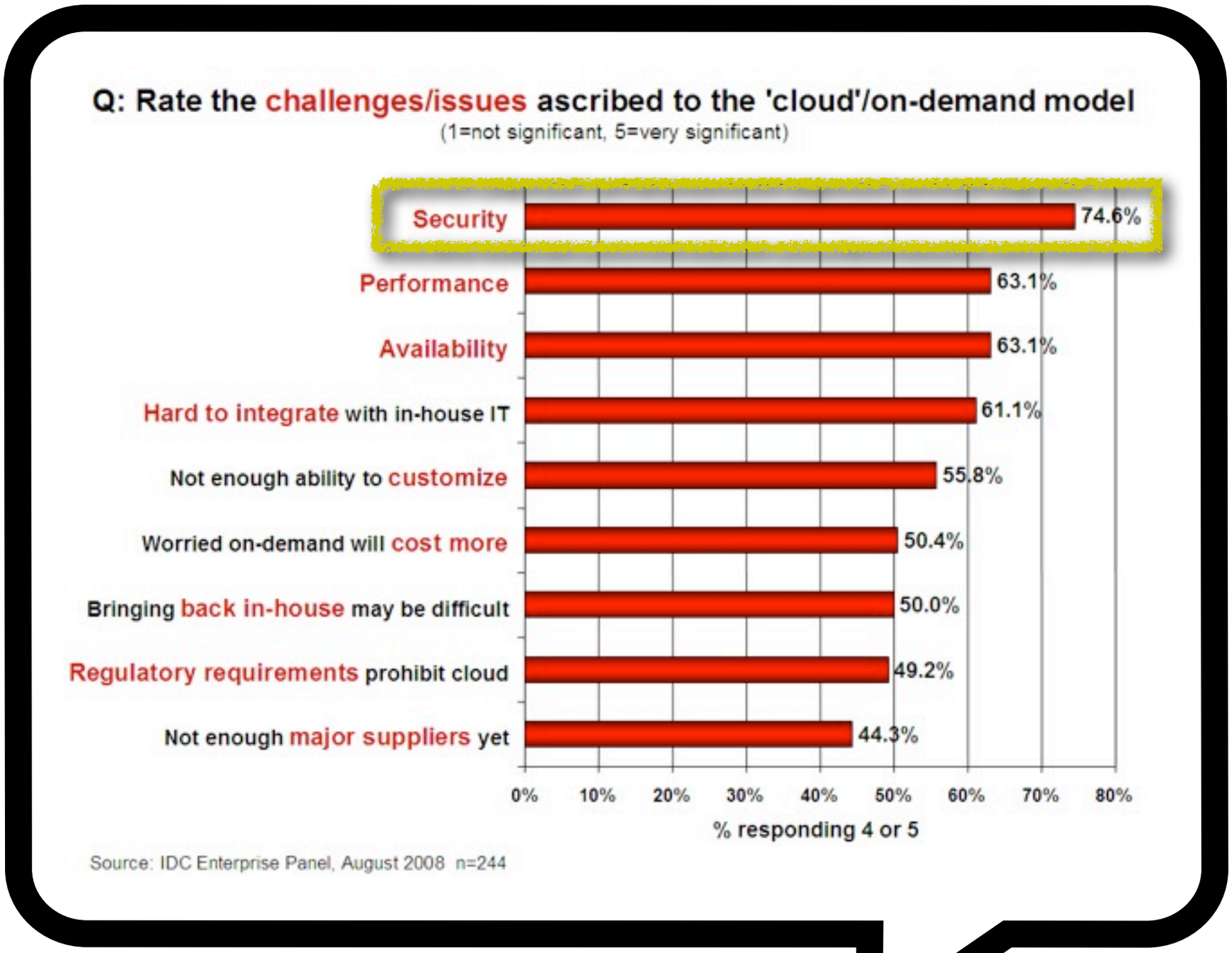


The Fable of VirtSec & CloudSec

Don’t Worry!


NETWORKWORLD
News | Blogs & Columns | Subscriptions | Videos | Events | More
Security | LANs & WANs | VoIP | Infrastructure Mgmt | Wireless | Software | Data Center | SMB | Careers
Cloud Computing | Desktop | Green IT | NAS | SAN | Server | Storage Management | Virtualization | Whitepapers | Webcasts
Cloud security fears are overblown, some say
Share/Email
Buzz up!
2 Comments
Print
Toolshed - IT A&A
It may sound like heresy to say it, but it's possible to worry a little too much about security in cloud computing environments, speakers at IDC's Cloud Computing Forum said on Wednesday.
Security is the No. 1 concern cited by IT managers when they think about cloud deployments, followed by performance, availability, and the ability to integrate cloud services with in-house IT, according to IDC's research.
Keeping data secure is critical, of course, but companies need to be realistic about the level of security they achieve inside their own business, and how that might compare to a cloud provider such as Amazon Web Services or Salesforce.com, speakers here said.
Developers and Identity Services : Tackling Identity Data with Identity Hub: Download now
"I think a lot of security objections to the cloud are emotional in nature, it's reflexive," said Joseph Tobolski, director for cloud computing at Accenture. "Some people create a list of requirements for security in the cloud that they don't even have for their own data center."
Keep
on
Most Rea
Bathrooms
Vivek Kundr
Prototype w
Speedy Saf
Microsoft W

Oh, Wait, Worry...



So We're Supposed To Do Nothing?

"...the answer to most problems was: Don't do anything. Always King Log, never King Stork ——'Live and let live.'"

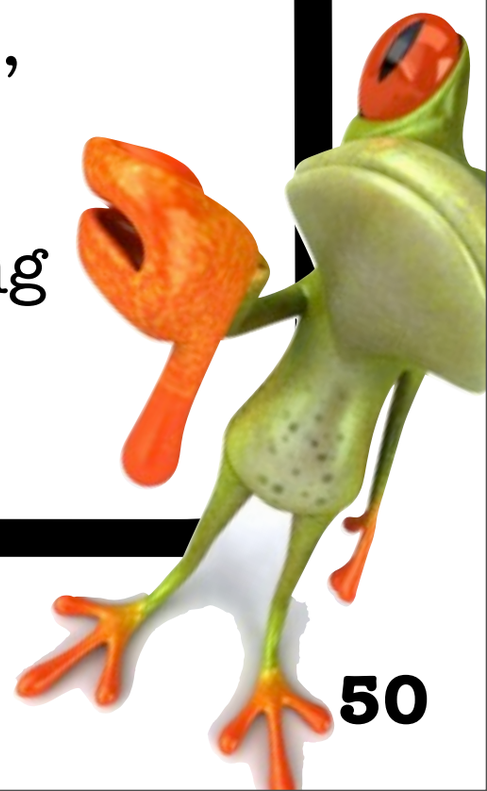
Robert Heinlein, Glory Road

No, But a Little Perspective...

- We've rushed to embrace virtualization without solving many of its attendant security, privacy and management challenges in environments over which we have direct control of our information and infrastructure
- We've brushed past real time infrastructure (RTI) which brings discipline and the technology needed for robust automation, autonomics, orchestration, provisioning , re-purposing and governance
- Now we're hustling to push to "The Cloud," introducing new operational and business models, stretching technology and with a complete lack of standards?

Oh, C'Mon...

What Could Possibly Go Wrong?

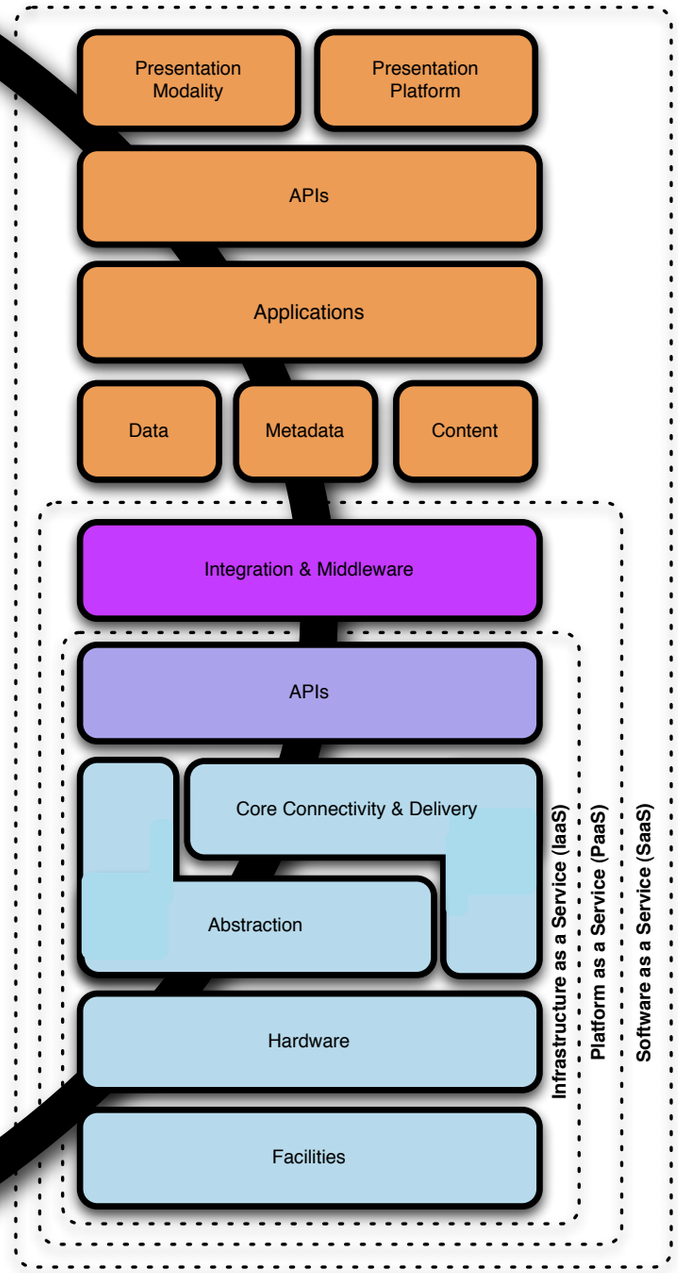


Cloudifornication & Simplexity?

- “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
- It’s a ‘squeezing the balloon problem’
- The cyclical and very dynamic punctuated equilibrium of computing isn’t meshing well with static security

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



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

Achtung! Divergent Models

Mainframes

Das Cloud

Web2.0

Client/Server

Web1.0

Display

Compute

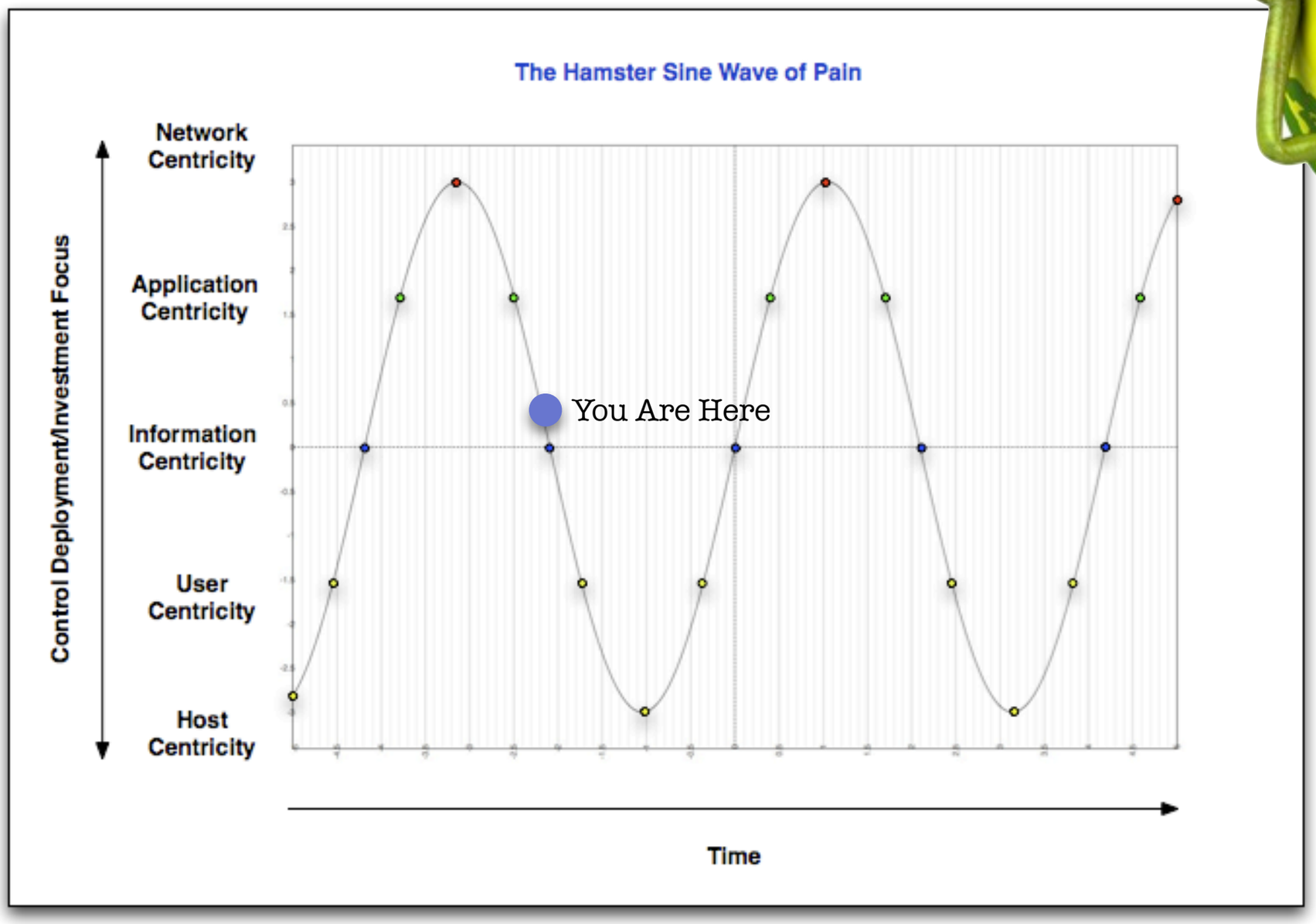
Data

Bandwidth

	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

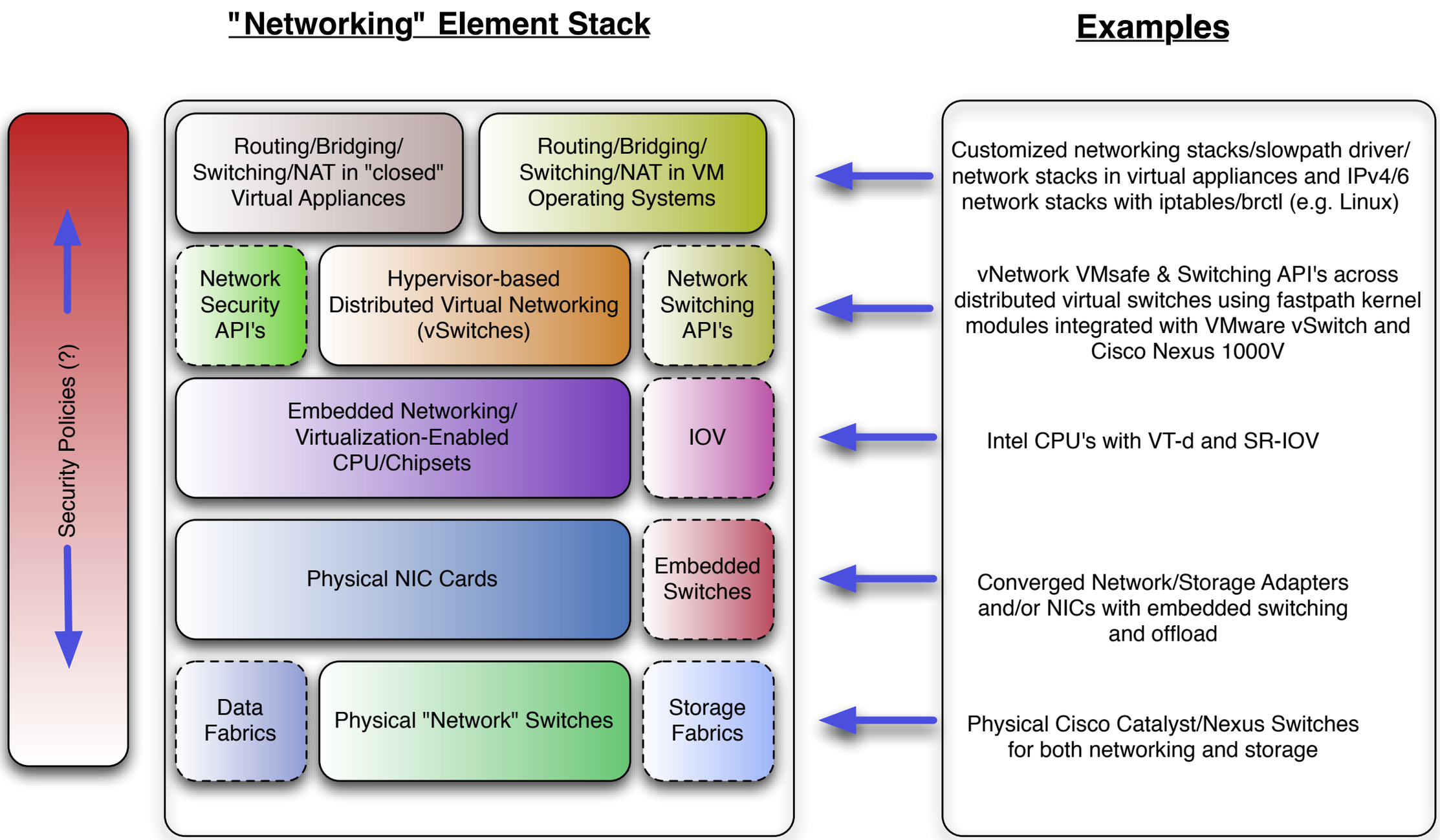
* Credit: Gunnar Peterson

The Hamster Sine Wave of Pain... *



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

Convergence Is Simplexity



That Was Just Networking...

Let's not forget
how converged
fabrics &
I/O Virtualization
Affects Compute
& Storage...

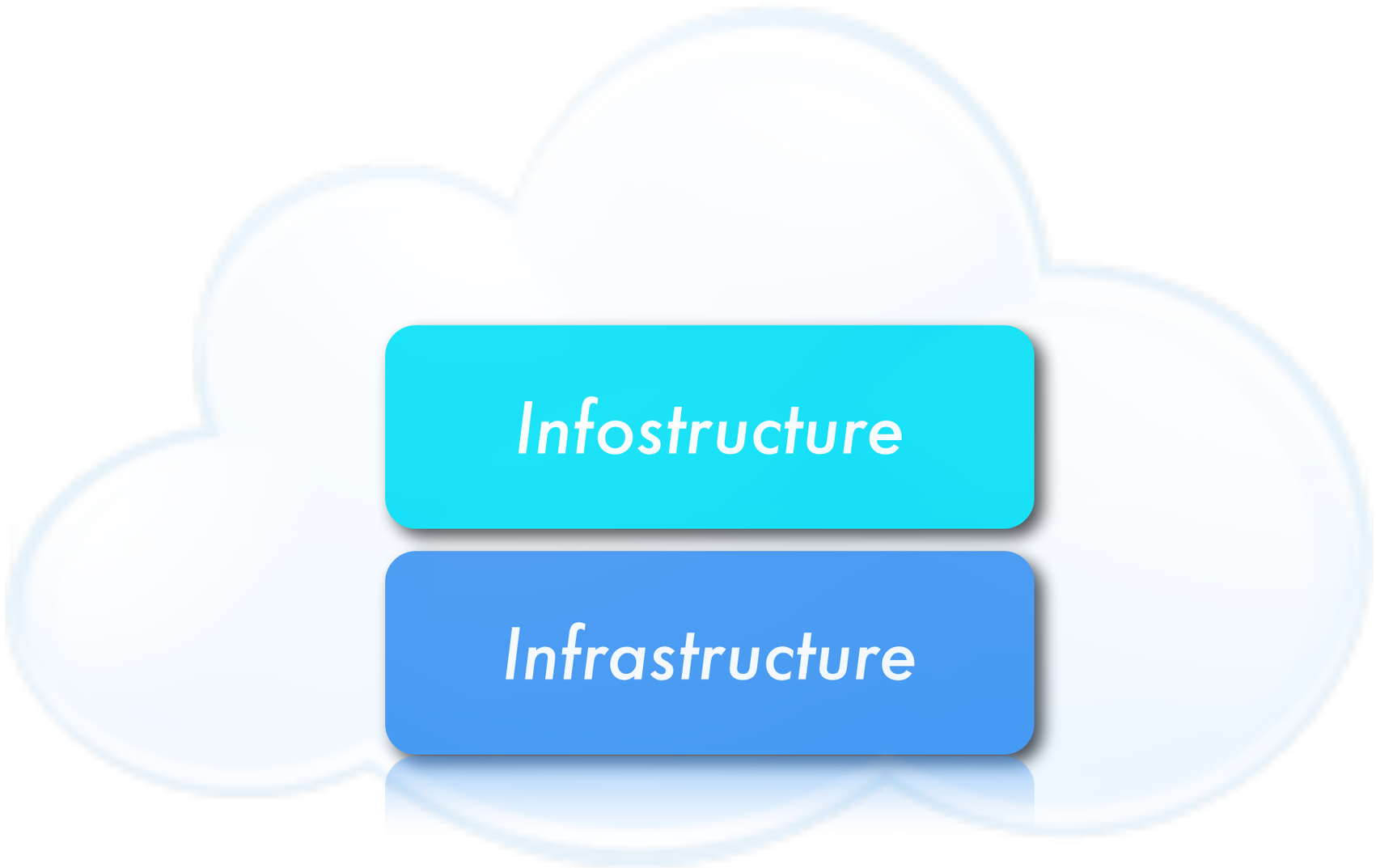
But Just To Spice Things Up...
Bingo-ism With Some Threats Old & New

Hoff | The Frogs Who Desired a King | 2009

There Ain't Nuthin' Wrong With The InterTubes!

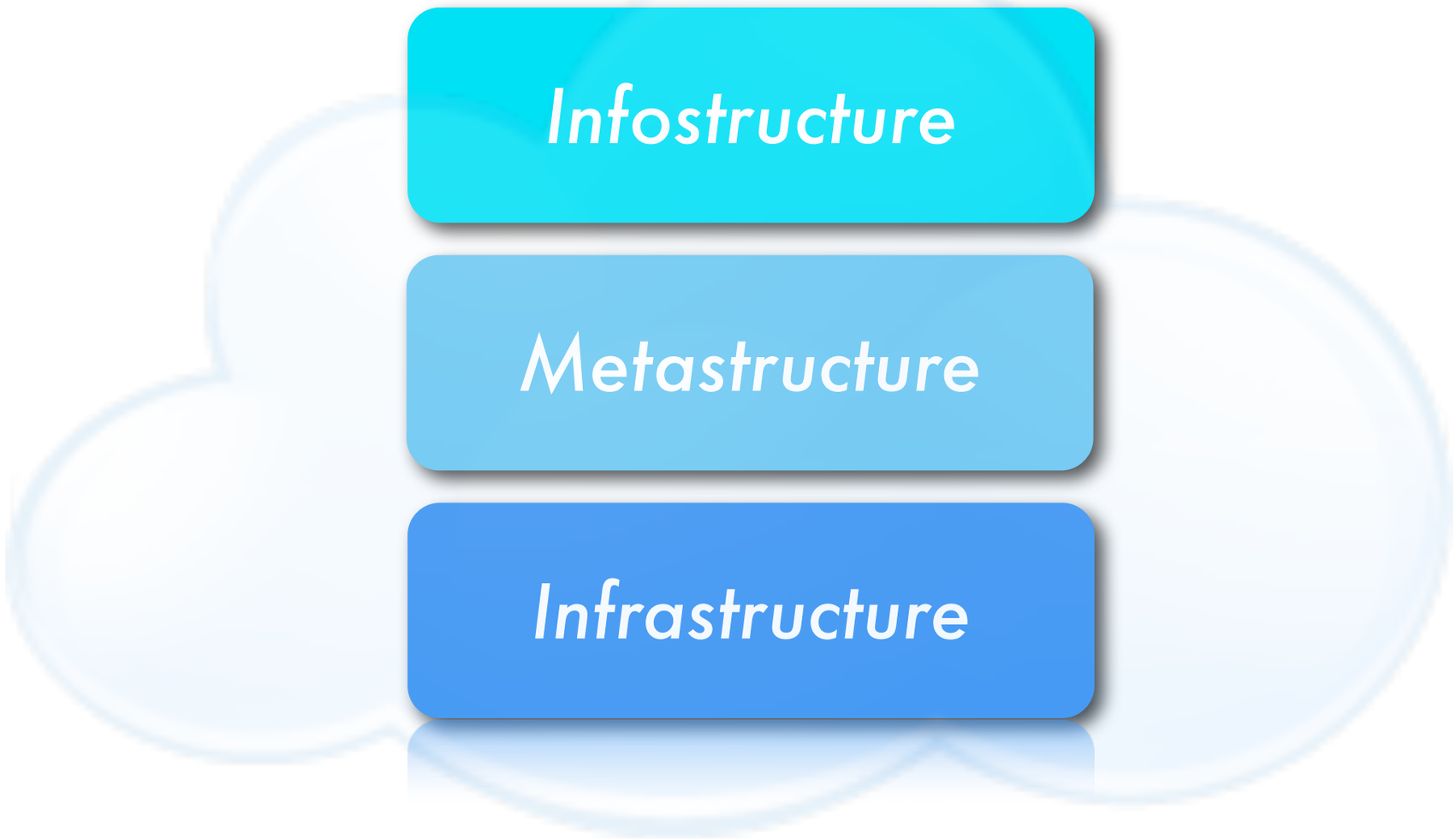
Hoff | The Frogs Who Desired a King | 2009

Cloudanatomy : Meet the Triplets



Hoff | The Frogs Who Desired a King | 2009

Cloudanatomy : Meet the Triplets



Hoff | The Frogs Who Desired a King | 2009

Cloudanatomy : Meet the Triplets

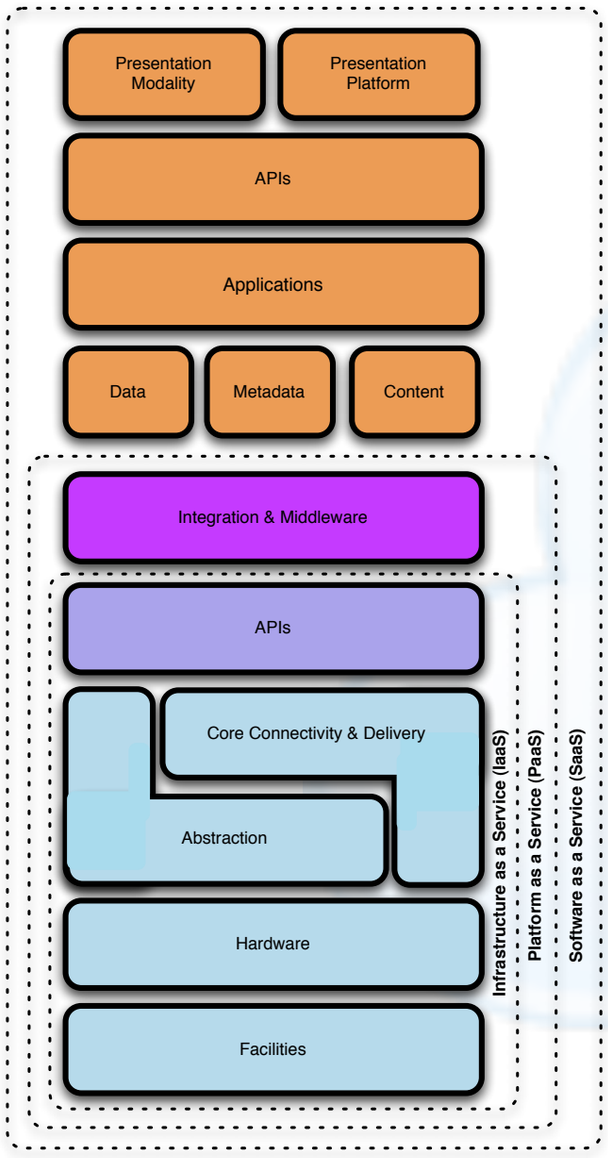
Infostructure

Metastructure

Infrastructure

- **Content & Context** - Applications, Data/Metadata, Services
- **Glue & Guts** - IPAM, IAM, SSL, BGP, DNS, etc.
- **Sprockets & Moving Parts** - Compute, Network, Storage

Cloudanatomy : Meet the Triplets



Infostructure

- **Content & Context** -
  Applications, Data/Metadata, Service

Metastructure

- **Glue & Guts** -
  IPAM, IAM, SSL, BGP, DNS, etc.

Infrastructure

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

Hoff | The Frogs Who Desired a King | 2009

These Sound Familiar...

Infostructure

- Application/WebApp Insecurity, SQL Injection

Metastructure

- BGP, SSL & DNS Hijacking

Infrastructure

- Chipset & Virtualization Compromise

...And So Do These

Let's Highlight just a few ...

- (t)rust
- Availability
- Confidentiality & Privacy
- Visibility & Manageability
- Portability & Interoperability
- Reliability & Resiliency
- Audit
- Compliance

...and What's Old Is New(s) Again

One Cloud Forward, Two Steps Backward

- Access Control
- Application Security
- Data Leakage
- Database Security
- Authentication
- Storage Security
- Encryption
- SDLC
- Denial Of Service
- Protocol Security by Politeness (BGP/DNS/SSL)
- Key Management
- Identity Management
- Vulnerability Management

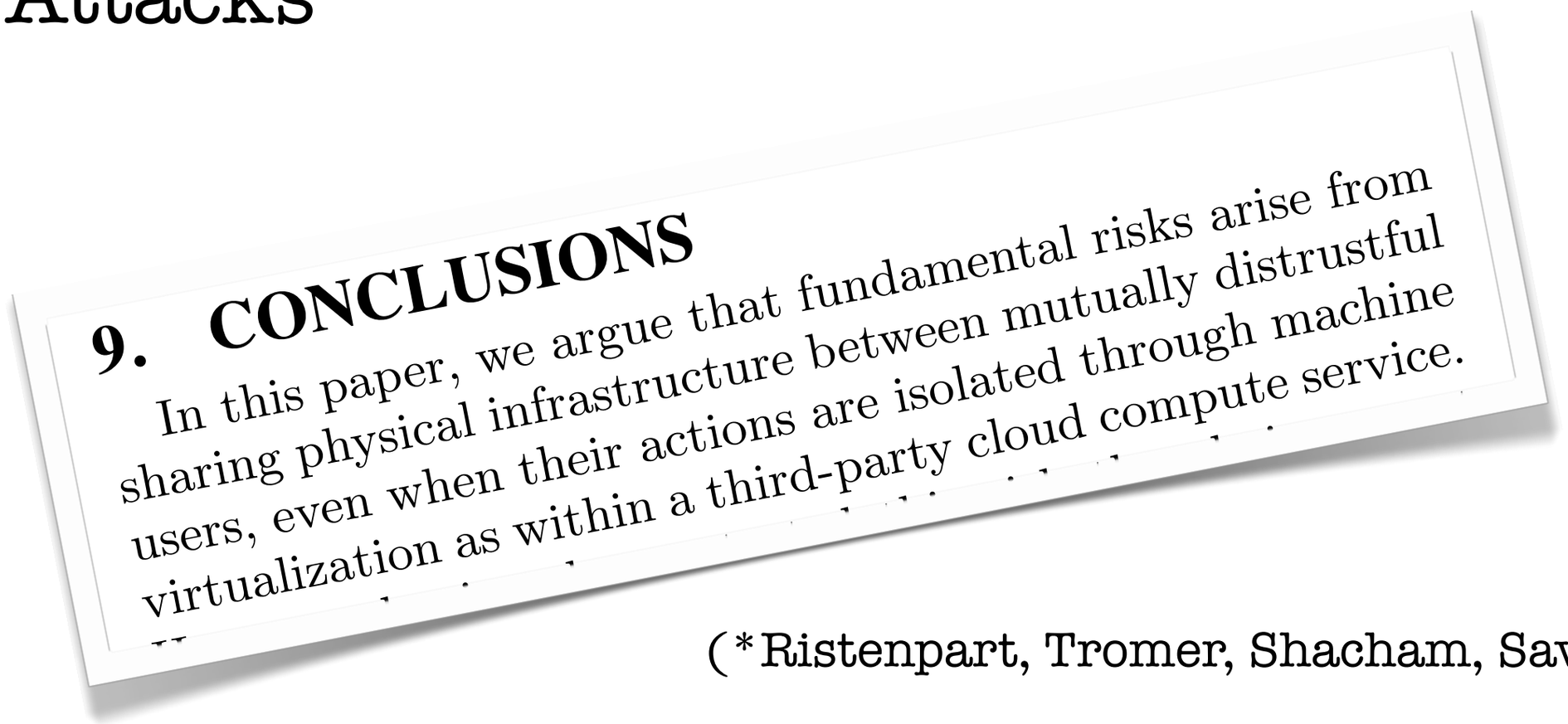
Live By the Cloud, Die By the Cloud...

Cloud-Specific Stuff Emerging

- Organizational & Operational Misalignment
- Monoculture of Operating Systems, Virtualized Components & Platforms
- Privacy Of Data/Metadata, Exfiltration and Leakage
- Inability to Deploy Compensating or Detective Controls
- Segmentation & Isolation In Multi-tenant environments...

A Very Cool Example...

- **Cloud Cartography*** - Mapping Cloud Infrastructure & Brute Forcing Co-Resident EC2 AMI 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)

And Another...

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

(*Kostya Kortchinsky - Immunity)

All Your Clouds Are Belong To Us...

- **MeatCloud**: Using the Mechanical Turk to be a Maniacal Jerk
- **CloudFlux** - Using FastFlux Botnets in the Cloud
- **LeapFrog** - (Ab)using VPN tunnels across Clouds
- Cloud-based **vMotion Poison Potion**
- Economic Denial Of Sustainability (**EDoS**)

New Solutions To Old Problems

The Realities of Today's CloudSec Solutions Landscape:

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

Look for extensions of management and visibility solutions to lead - LOTS of APIs on the horizon

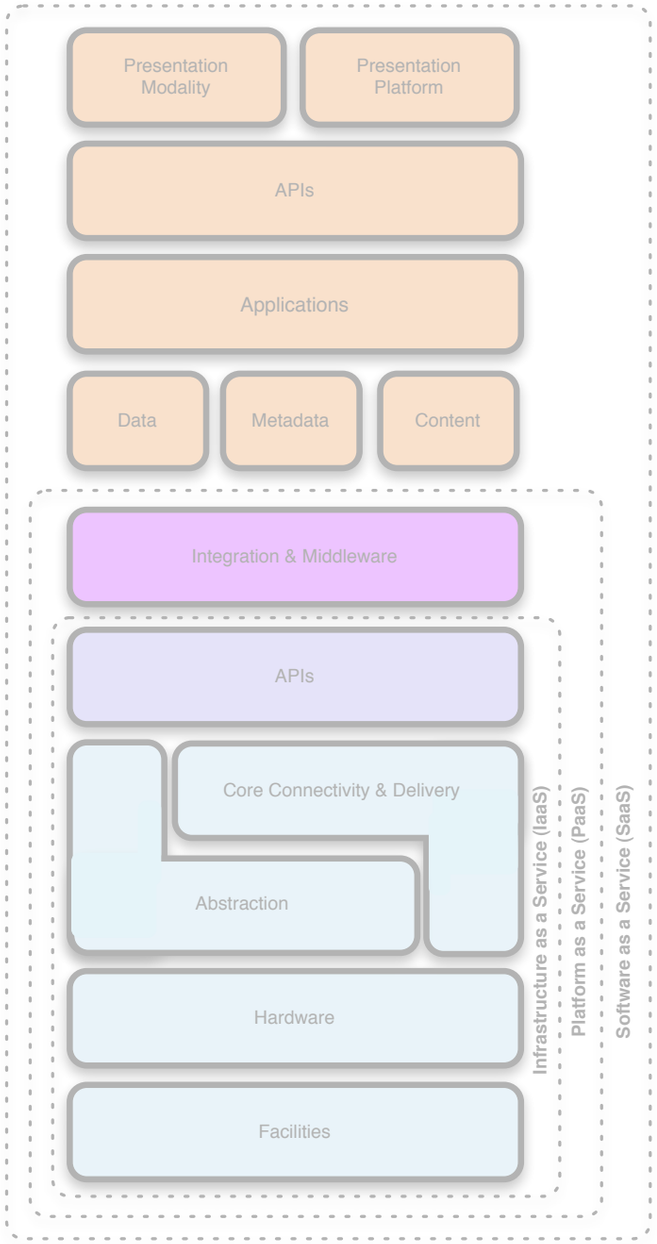
Look for standardized policy language and enforcement capabilities with VM's as the de facto atomic unit of the Cloud

Let's Revisit Our Examples : Public Clouds

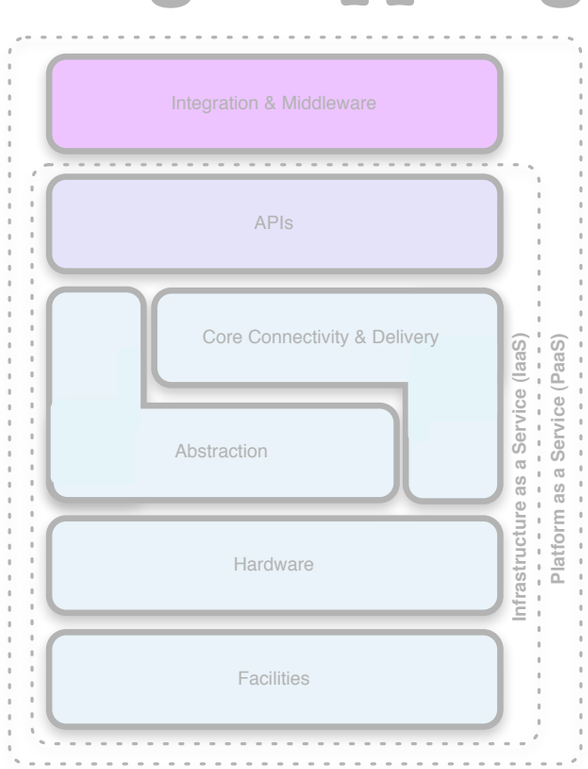
Q: How do I take my catalog of compensating controls/best practices and apply them/integrate them in each of these environments?

A: You may not be able to (or need to)

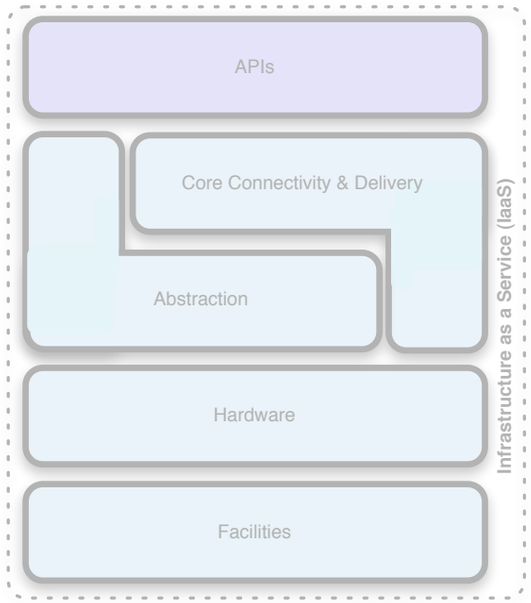
Salesforce - SaaS



Google AppEngine - PaaS



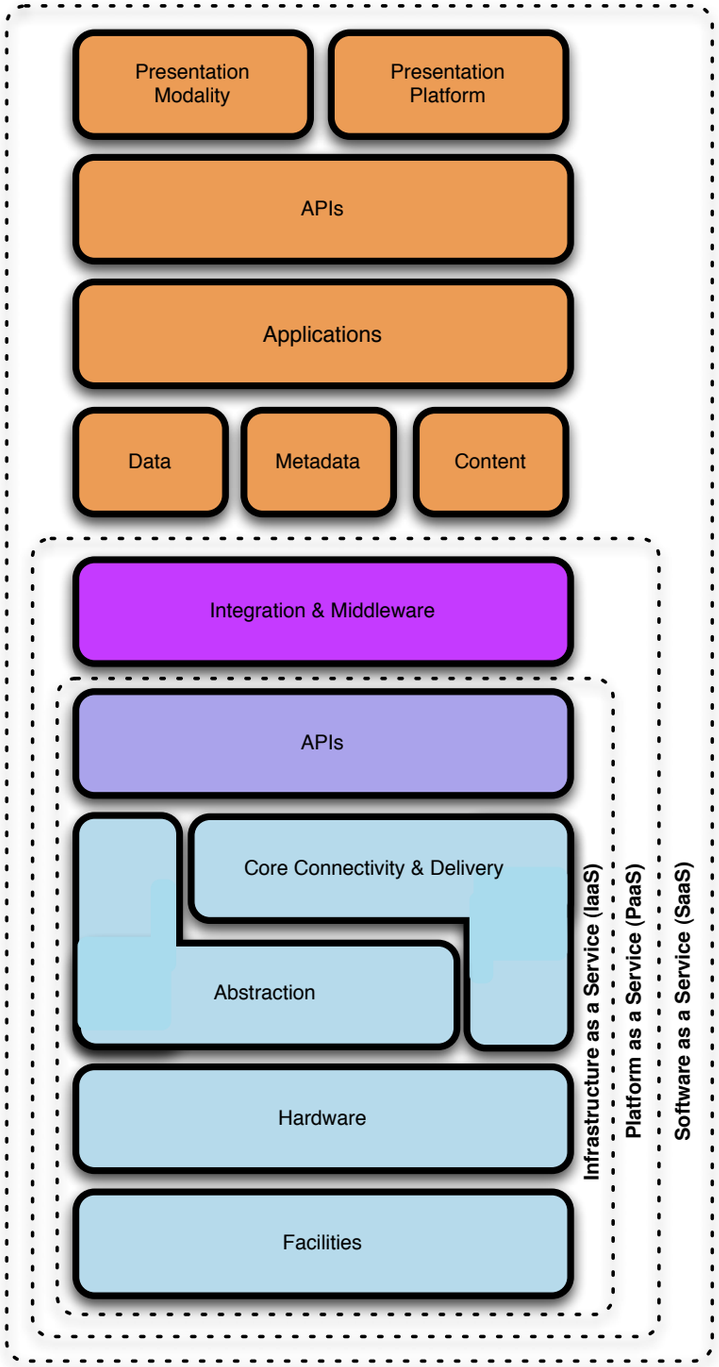
Amazon EC2 - IaaS



Hoff | The Frogs Who Desired a King | 2009

Mapping the Model to the Metal

Cloud Model



Find the Gaps!

Security Control Model

Applications	SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec.
Information	DLP, CMF, Database Activity Monitoring, Encryption
Management	GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
Network	NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
Trusted Computing	Hardware & Software RoT & API's
Compute & Storage	Host-based Firewalls, HIDS/HIPS, Integrity & File/log Management, Encryption, Masking
Physical	Physical Plant Security, CCTV, Guards

Compliance Model

PCI

- ☑ Firewalls
- ☑ Code Review
- ☑ WAF
- ☑ Encryption
- ☑ Unique User IDs
- ☑ Anti-Virus
- ☑ Monitoring/IDS/IPS
- ☑ Patch/Vulnerability Management
- ☑ Physical Access Control
- ☑ Two-Factor Authentication...

HIPAA

GLBA

SOX

Cloud Happiness :: Warm & Fuzzies

The Cloud <u>can</u> 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.

Deal With It

Hoff | The Frogs Who Desired a King | 2009

So You Said Something About a Fable?

fa•ble |ˈfābəl|
noun
a short story, typically with animals as characters, conveying a moral.
• a story, typically a supernatural one incorporating elements of myth and legend.
See note at FICTION .
• myth and legend : *the unnatural monsters of fable.*
• a false statement or belief.

verb [intrans.] archaic
tell fictitious tales : *I do not dream nor fable.*
• [trans.] fabricate or invent (an incident, person, or story).

DERIVATIVES
fa•bler |ˈfāb(ə)lər| |ˈfeɪb(ə)lər| |ˈfeɪblə| noun

ORIGIN Middle English : from Old French ***fable*** (noun), from Latin ***fabula 'story,'*** from ***fari 'speak.'***

- The **fable** is that we're screwed
- The **reality** is that we're not...
- **Actually**, we are (and will be) just as insecure as we've always been*

Hoff | The Frogs Who Desired a King | 2009

*Ranum

The Velocity Of Cloud Is Driving Change In Security

- This is actually something to be really happy about; 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

Break Glass, Apply Common Sense

- We already have most of what you need to make an informed set of decisions, but I'm afraid Cloud Security comes down to the basics…
- You have a risk assessment methodology, right? You classify assets and data and segment already, right?
- Interrogate vendors and providers; use the same diligence that you would for outsourced services today; focus on resilience/recovery, SLA's, confidentiality, privacy and segmentation. See how they twitch.
- The challenge is to match business/security requirements against the various *aaS model(s) and perform the gap analysis
- Each of the *aaS models provides a delicate balance of openness, flexibility, control, security and extensibility
- Go back & look at the "Right For the Cloud?" criteria
- REGARDLESS of the model, **you** are still responsible for some element of security

Cloud Security Alliance - Guidance

Critical Areas Of Focus For Cloud Computing
15 Domains – Architecture, Governance & Operations*

1. Architecture & Framework

Governing in the Cloud

2. Governance & Risk Mgt
3. Legal
4. Electronic Discovery
5. Compliance & Audit
6. Information Lifecycle Mgt
7. Portability & Interoperability

Operating in the Cloud

8. Traditional, BCM, DR
9. Data Center Operations
10. Incident Response
11. Application Security
12. Encryption & Key Mgt
13. Identity & Access Mgt
14. Storage
15. Virtualization

**Cloud Security Alliance*

Get Involved & Edumacated

- Cloud Computing Google Groups:
  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**
- Join the Cloud Security Alliance...

Join The Cloud Security Alliance

The CSA is a non-profit organization formed to promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing.

The Cloud Security Alliance is comprised of many subject matter experts from a wide variety disciplines, united in our objectives:

- **Promote a common level of understanding between the consumers and providers of cloud computing regarding the necessary security requirements and attestation of assurance.**

- **Promote independent research into best practices for cloud computing security.**

- **Launch awareness campaigns and educational programs on the appropriate uses of cloud computing and cloud security solutions.**

- **Create consensus lists of issues and guidance for cloud security assurance.**

The Cloud Security Alliance was launched at the RSA Conference 2009 in San Francisco, April 24, 2009.

Never “Misunderestimate” the Power Of the Cloud

Name: Christofer Hoff

Twitter: @Beaker

Email: choff@packetfilter.com

Blog: www.rationalsurvivability.com

Phone: +1.978.631.0302

Cloud Location: 9

“It’s Good To Be King”