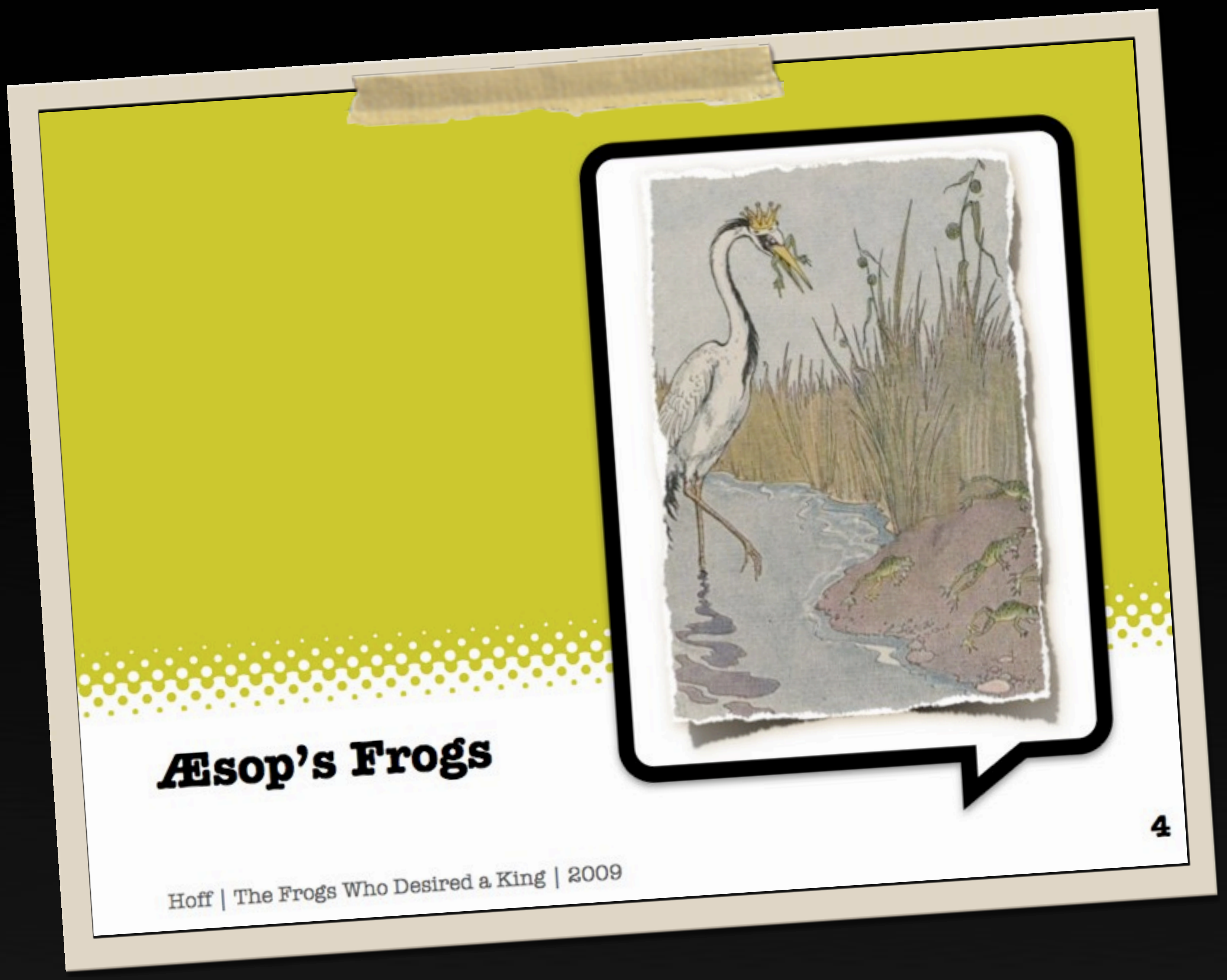
The Belgian Beer Lovers Guide to Cloud Security

BRUCON
September ‘09

Craig Balding cloudsecurity.org

Disclaimer

The views and opinions expressed here are those of Craig Balding only and in no way represent the views, positions or opinions – expressed or implied – of my employer or anyone else.



Æsop's Frogs

4

Hoff | The Frogs Who Desired a King | 2009

Sorry, No Frogs

Hoff is Busy

Takin’ down the Internet - well, through one it’s fathers ;-)

Free Beer Instead?

So instead I offer “free beer”. WIN!

Hacking for B33R!

HACKING FOR B33R
BRUCON
WWW.BRUCON.ORG

You’ll notice the black sun in the brucon logo

We are in the BruCON Beer Cloud…

Well here’s the cloud... the BruCON Beer Cloud

How are you enjoying the belgium beer so far?

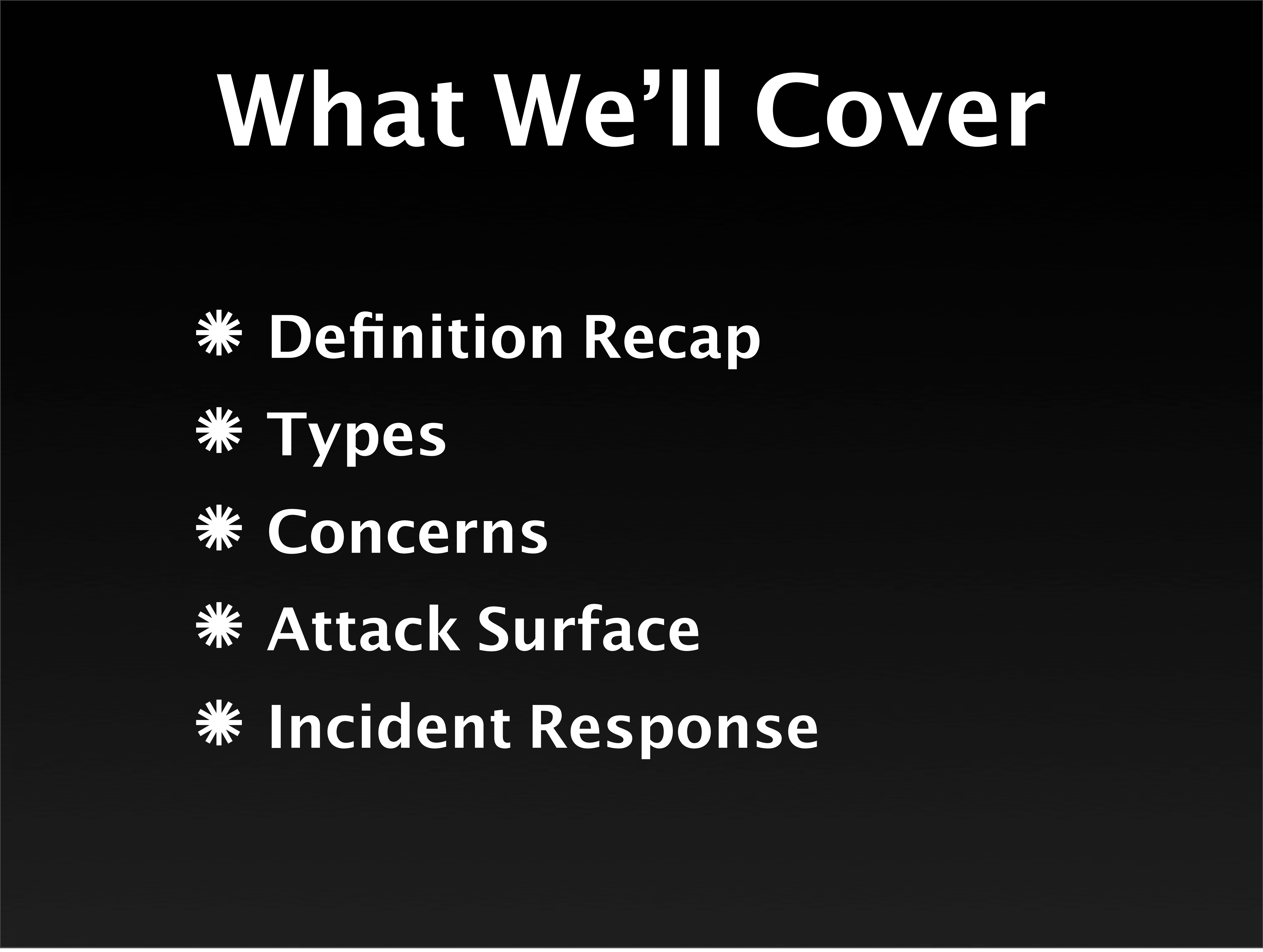
Win B33R!

Answer Questions for Beer!

Whenever you see this speech bubble it means you have a chance to win a beer if you can answer the question correctly.

Goal: Stimulate brains

This is not a 0h day talk
Nor is it terribly technical - in fact its quite high level
My day job is pen-testing, incident response etc...so this is me stepping out of the weeds.
My attempt to defluff the cloud
Separate out the issues
Encourage vuln research on cloud technologies
As a community we’re not matching our research to the pace of change
Cloud vuln research is much more than hypervisor research.



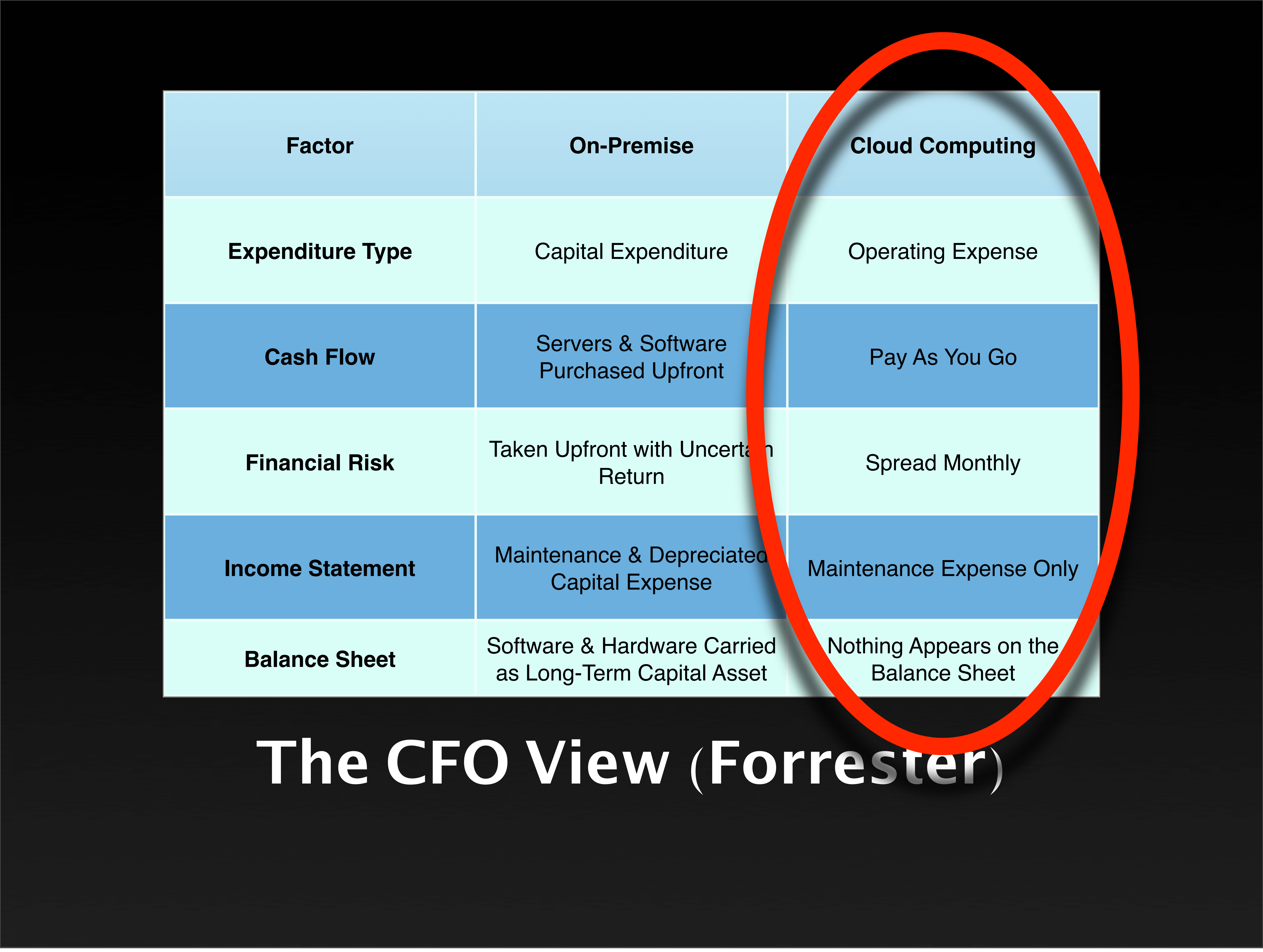
What We’ll Cover

- ❋ Definition Recap
- ❋ Types
- ❋ Concerns
- ❋ Attack Surface
- ❋ Incident Response

Here’s what we’ll cover.
<pause>
Before we do this, we should answer the “so what” question.

Cloud: Why Bother?

Why bother using the cloud?
If our job is to guide management around risk
we need to understand the other side of the equation - the promised reward
what are the benefits of cloud?
as infosec professionals we need to understand this to avoid trying to push water uphill



Factor	On-Premise	Cloud Computing
Expenditure Type	Capital Expenditure	Operating Expense
Cash Flow	Servers & Software Purchased Upfront	Pay As You Go
Financial Risk	Taken Upfront with Uncertain Return	Spread Monthly
Income Statement	Maintenance & Depreciated Capital Expense	Maintenance Expense Only
Balance Sheet	Software & Hardware Carried as Long-Term Capital Asset	Nothing Appears on the Balance Sheet

The CFO View (Forrester)

Or, why a CFO might love cloud
- pay as you go
- nothing on the balance sheet
- the opex/capex argument tends to be overplayed btw

The CEO View?

Agility: react faster to market conditions - beating competitors

Cloud Goggles

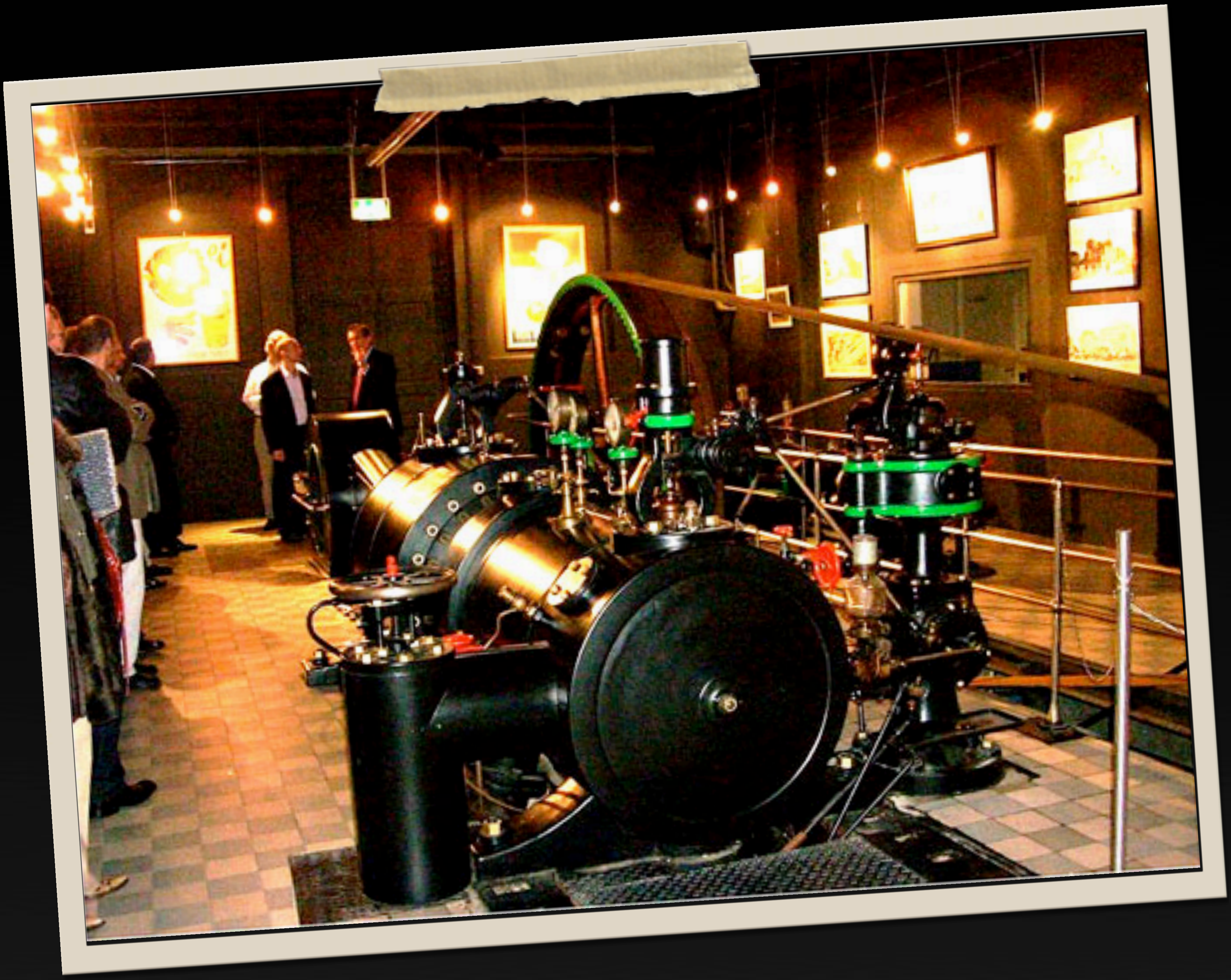
But the cloud juice is toxic and if you drink too much you wear the cloud goggles
Let’s be clear: Cloud isn’t “all or nothing”...
Not all workloads will go to a public cloud - that would be ridiculous
Don’t get taken in by the hype
Figuring out whats old and whats new
Use Common Sense
Do Good Due Diligence

Not Everyone Is Happy

For infosec people, cloud is immediately annoying for a number of reasons:
- hijacks an existing term (i.e. our network)
- its buzzword bingo (but really, what’s new)
- its “trendy” - everyone talks about at the moment - even at security conferences!
- it seems to mean anything a provider wants it to mean

Who Is This?

But some people are very happy



The Real Cloud Story

This is an electricity generator from a Belgium Brewery.
Nick Carr’s seminal Big Switch book used the generator as an analogy for delivering computing “as a service”
If books are food for the mind, beer is food for the soul.

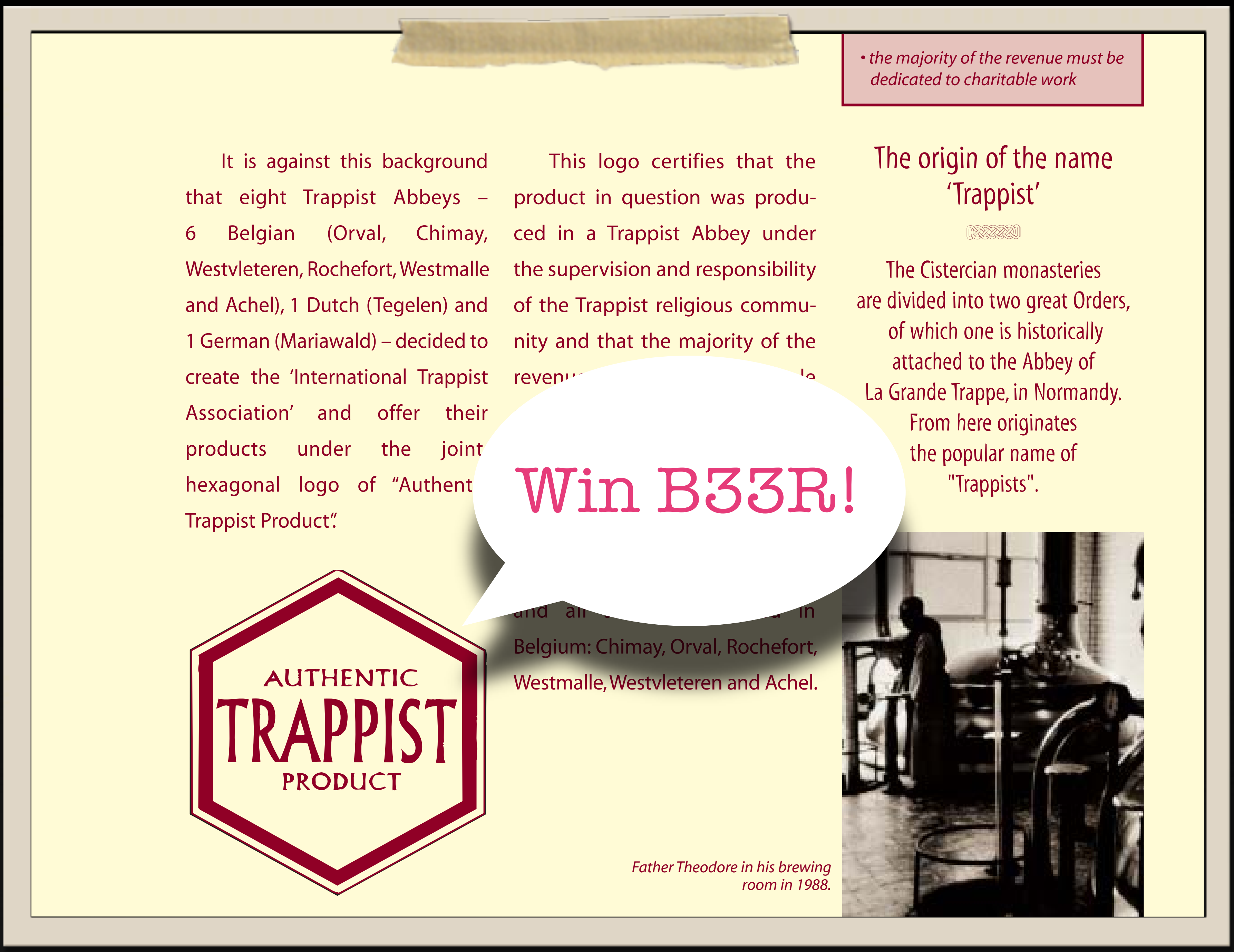
Definition Recap

Marketecture

Cloud has become a vehicle for terrible marketing
An avalanche of Cloud-powered “services”
PCI Compliant Cloud? Good luck with that
But we need to identify this for what it is and move on to the real cloud security conversation

“Give Me a Beer”

Saying ‘Cloud’ is a lot like walking into a belgium bar and asking for beer
The Barmaid’s smile is likely to wipe off her face rather quickly
Same with cloud - we can’t have a meaningful security conversation about “cloud”
its too vague



• the majority of the revenue must be dedicated to charitable work

It is against this background that eight Trappist Abbeys – 6 Belgian (Orval, Chimay, Westvleteren, Rochefort, Westmalle and Achel), 1 Dutch (Tegelen) and 1 German (Mariawald) – decided to create the 'International Trappist Association' and offer their products under the joint hexagonal logo of "Authent Trappist Product".

AUTHENTIC
TRAPPIST
PRODUCT

This logo certifies that the product in question was produced in a Trappist Abbey under the supervision and responsibility of the Trappist religious community and that the majority of the revenu le

and all in Belgium: Chimay, Orval, Rochefort, Westmalle, Westvleteren and Achel.

The origin of the name 'Trappist'

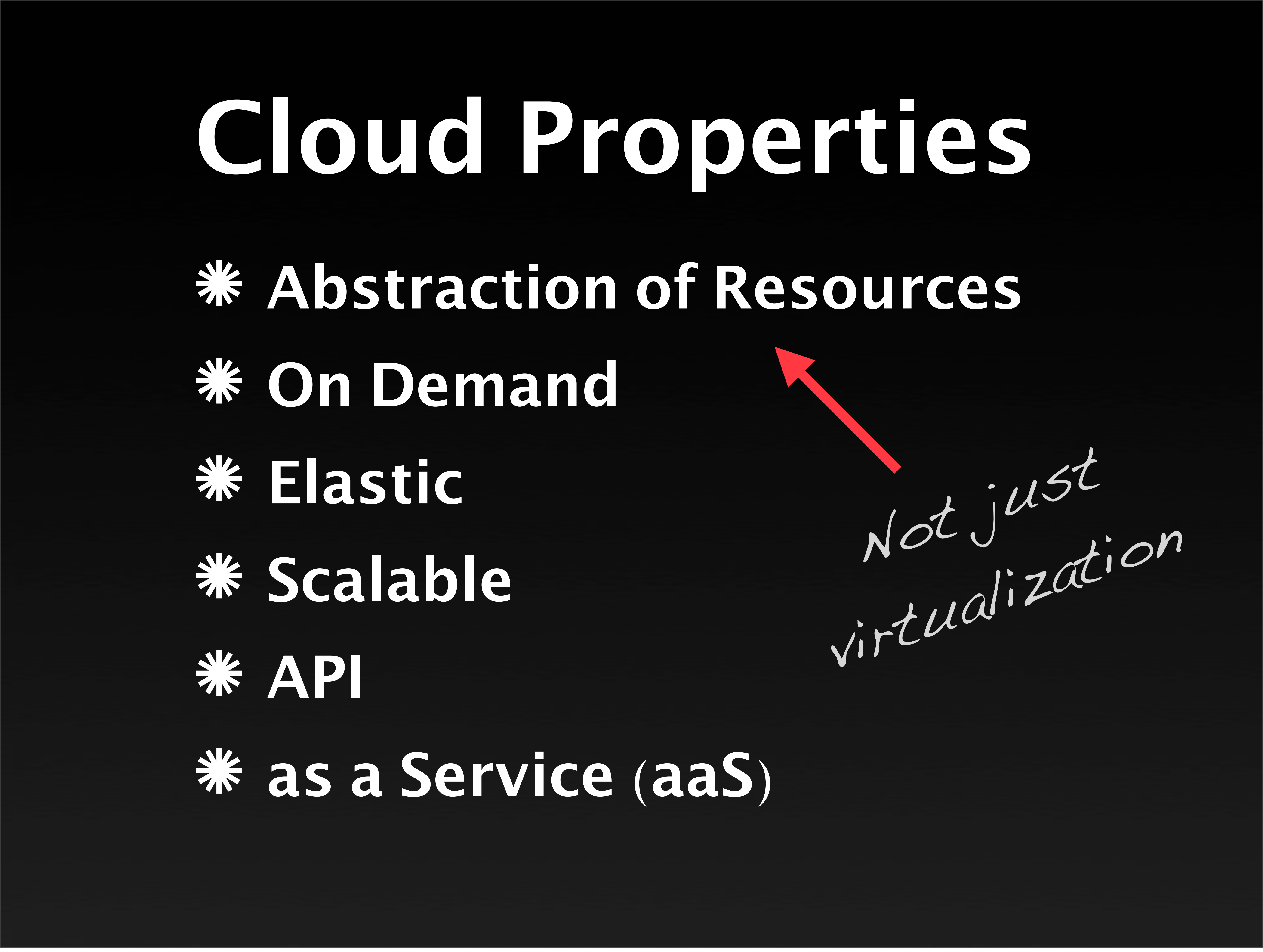
The Cistercian monasteries are divided into two great Orders, of which one is historically attached to the Abbey of La Grande Trappe, in Normandy. From here originates the popular name of "Trappists".

Father Theodore in his brewing room in 1988.

Certifiable

What is the significance of this logo? Free Beer

So with cloud, IBM and other consulting companies are already inventing certifications....



Cloud Properties

- Abstraction of Resources
- On Demand
- Elastic
- Scalable
- API
- as a Service (aaS)

Not just virtualization

Is it a bird, is it a plane, is it a cloud?
These are tangible properties of clouds
Contemplate this next time someone says ‘Its a cloud’
Each has security considerations and fundamentally that is what makes cloud a different deployment model
There’s been quite a bit of research on hypervisors:

- finding a vuln is the holy grail of virtsec vulnerability research
- however attack surface is shrinking
- low hanging fruit has gone
- where did that attack surface go to? the middleware and management tools
- hypervisor security is obviously very important but obsessing over this means we miss the bigger picture & other attack surfaces go untouched

Dynamic Meets Static Security

“Don’t land with the brakes on”

Cloud is dynamic, its a complex distributed system.

Clouds based on virtualization need to capture security state prior to motioning and adapt for the differing network position (new IP, route tables etc). IDS/FWs need to reflect these changes. This is not a trivial problem to solve but something VMware seems to be trying to figure out.

“Its Just Outsourcing”

Does anyone know why Cloud Computing isn’t just like traditional outsourcing?

For every solid reason you give, I’ll buy you a beer.

When I’m up in the clouds in an airplane, all the cars on the motorway below look the same...this is what happens when you look at everything at 50000ft

No Cloud Magic

It may be tempting to assume that cloud providers have solved the “security problem”
After all, clouds were built from the ground up...or were they?
More like a stichted quilt, lots of primarily open source code welded together
Vulns in underlying libraries are hidden time-bombs.
We all know about keeping OpenSSL libs up to date, what of image manipulation etc etc?
We’re relying on the cloud provider to write secure “glue code” and quickly update underlying code as vulns are discovered. Someone bring me a beer ;-).

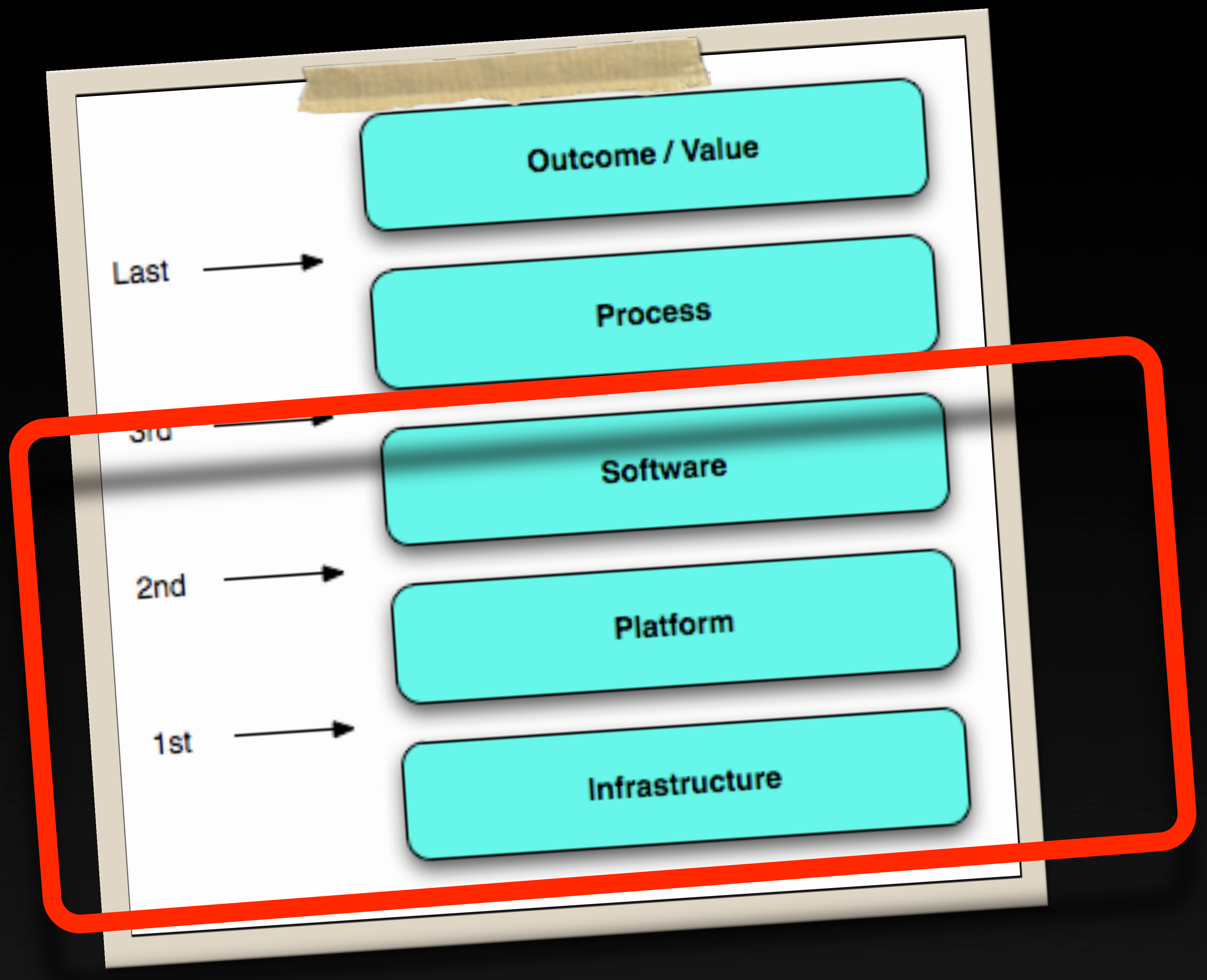
Types

Cloud Platforms

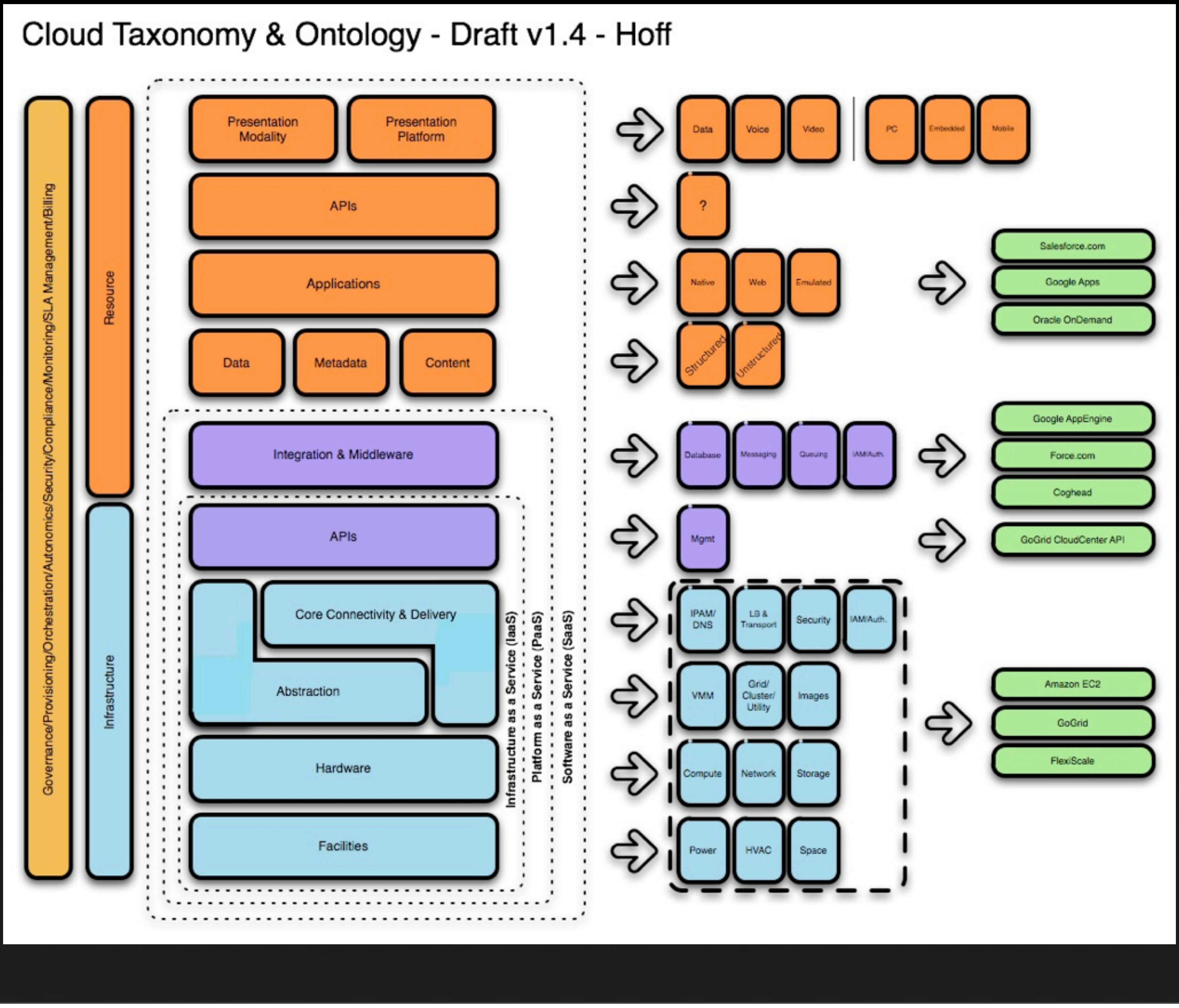
Cloud providers deliver their services on cloud platforms.

Summarise what we mean by “platform”

So where do the cloud providers go to buy “a platform” - I don’t recall seeing any TV commercials
Ecosystem of providers building platforms
Selling platforms to private companies, webhosting providers etc
Example of an open-source cloud (Ubuntu/Canonical) - you can download it and play with it
Cloud providers run services on cloud platforms


Outcome / Value
Last
Process
3rd
Software
2nd
Platform
1st
Infrastructure

…as a Service



Cloud Taxonomy & Ontology - Draft v1.4 - Hoff

Governance/Provisioning/Orchestration/Autonomics/Security/Compliance/Monitoring/SLA Management/Billing

Resource

Infrastructure

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)

Data

Voice

Video

PC

Embedded

Mobile

?

Native

Web

Emulated

Structured

Unstructured

Database

Messaging

Queuing

IAM/Auth.

Mgmt

IPAM/ DNS

LB & Transport

Security

IAM/Auth.

VMM

Grid/ Cluster/ Utility

Images

Compute

Network

Storage

Power

HVAC

Space

Salesforce.com

Google Apps

Oracle OnDemand

Google AppEngine

Force.com

Coghead

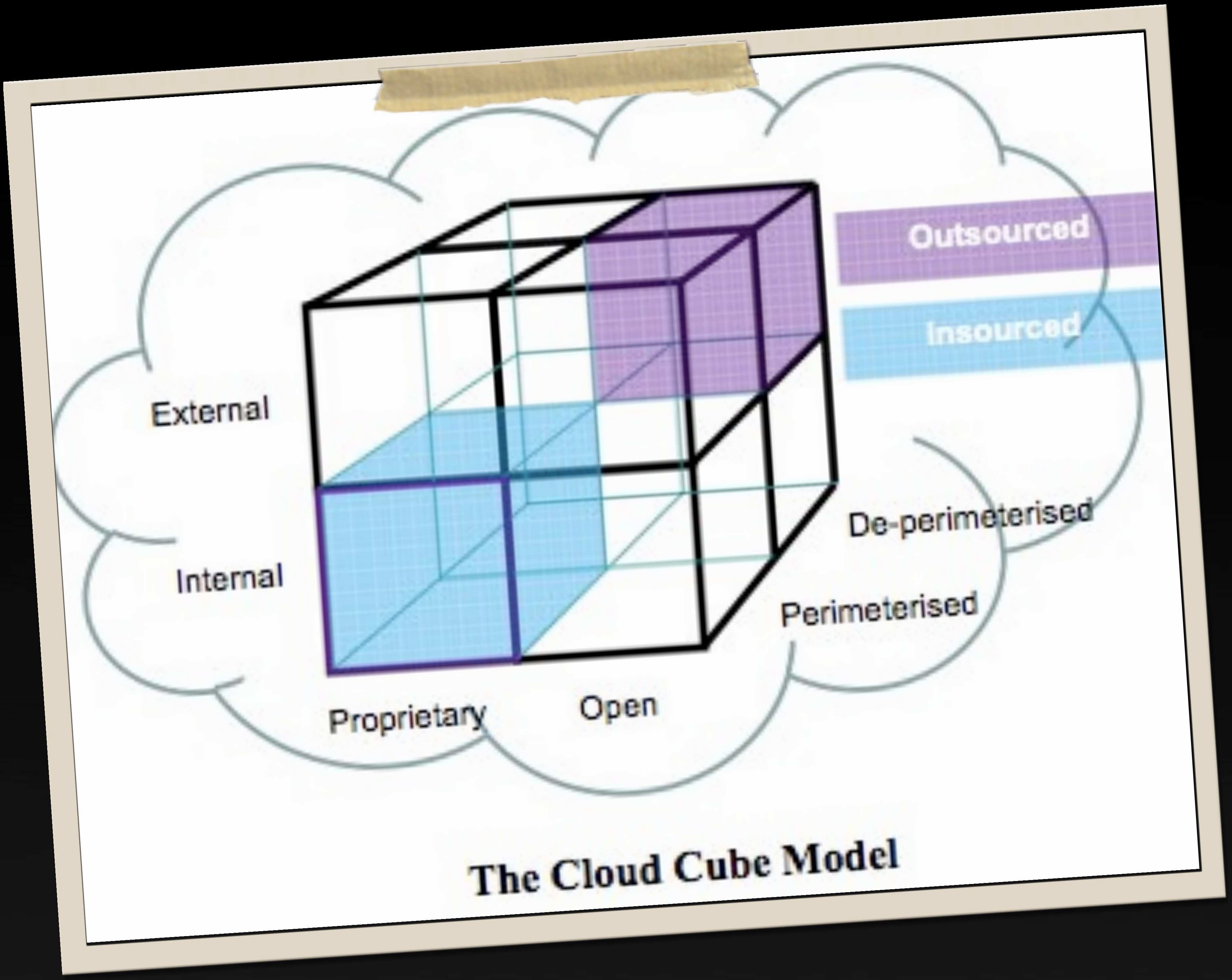
GoGrid CloudCenter API

Amazon EC2

GoGrid

FlexiScale

Shows the components that make up each layer of the stack
Very useful reference - not going through this now
Recommend reviewing when the slide deck is up or visit Hoff’s blog and search for ‘cloud model’

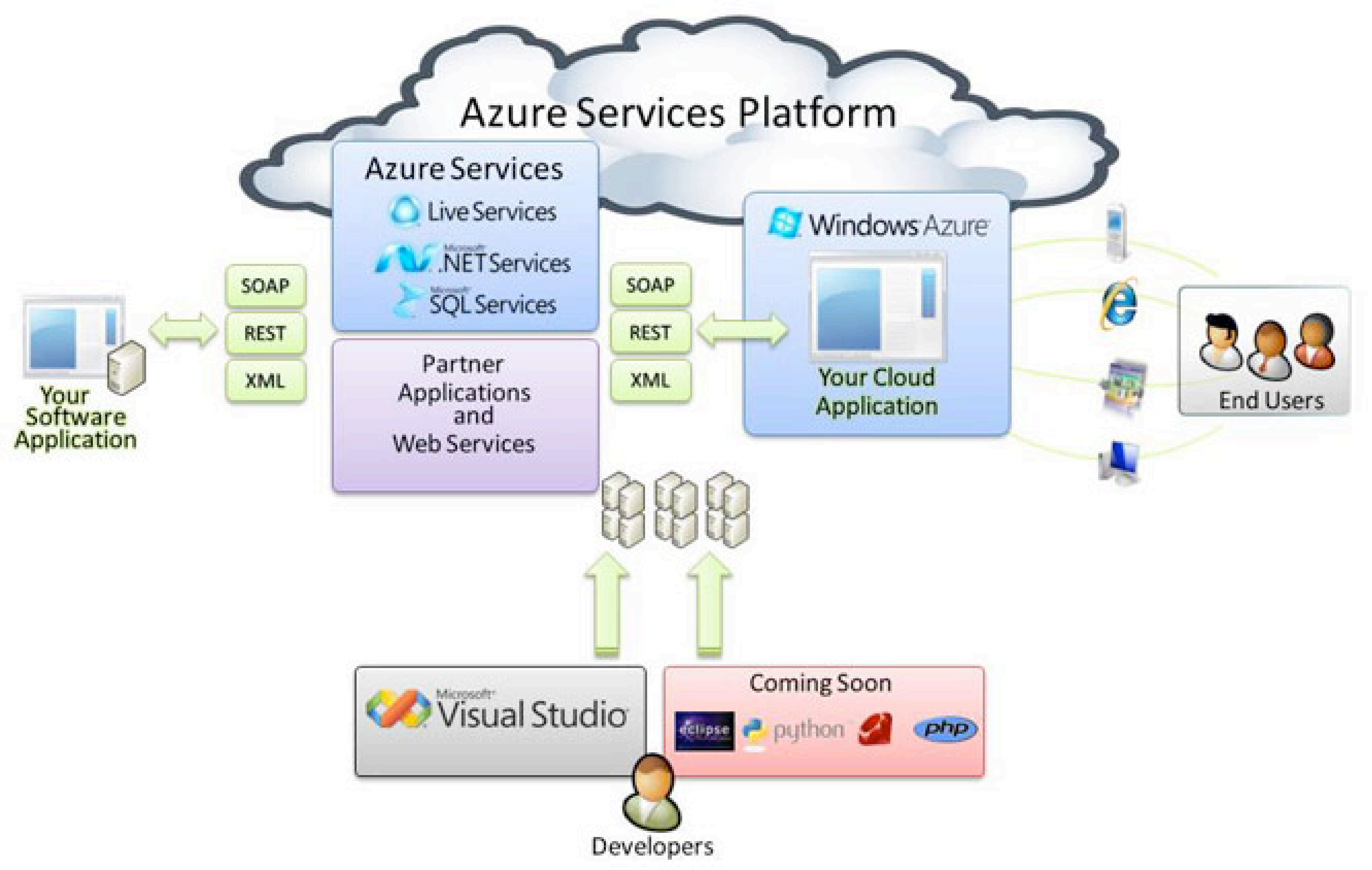


Jericho Cloud Cube

This graphic helps us understand cloud deployment options
3 dimensions
- external/internal
- propietary/open
- de-perimeterised/peremitised

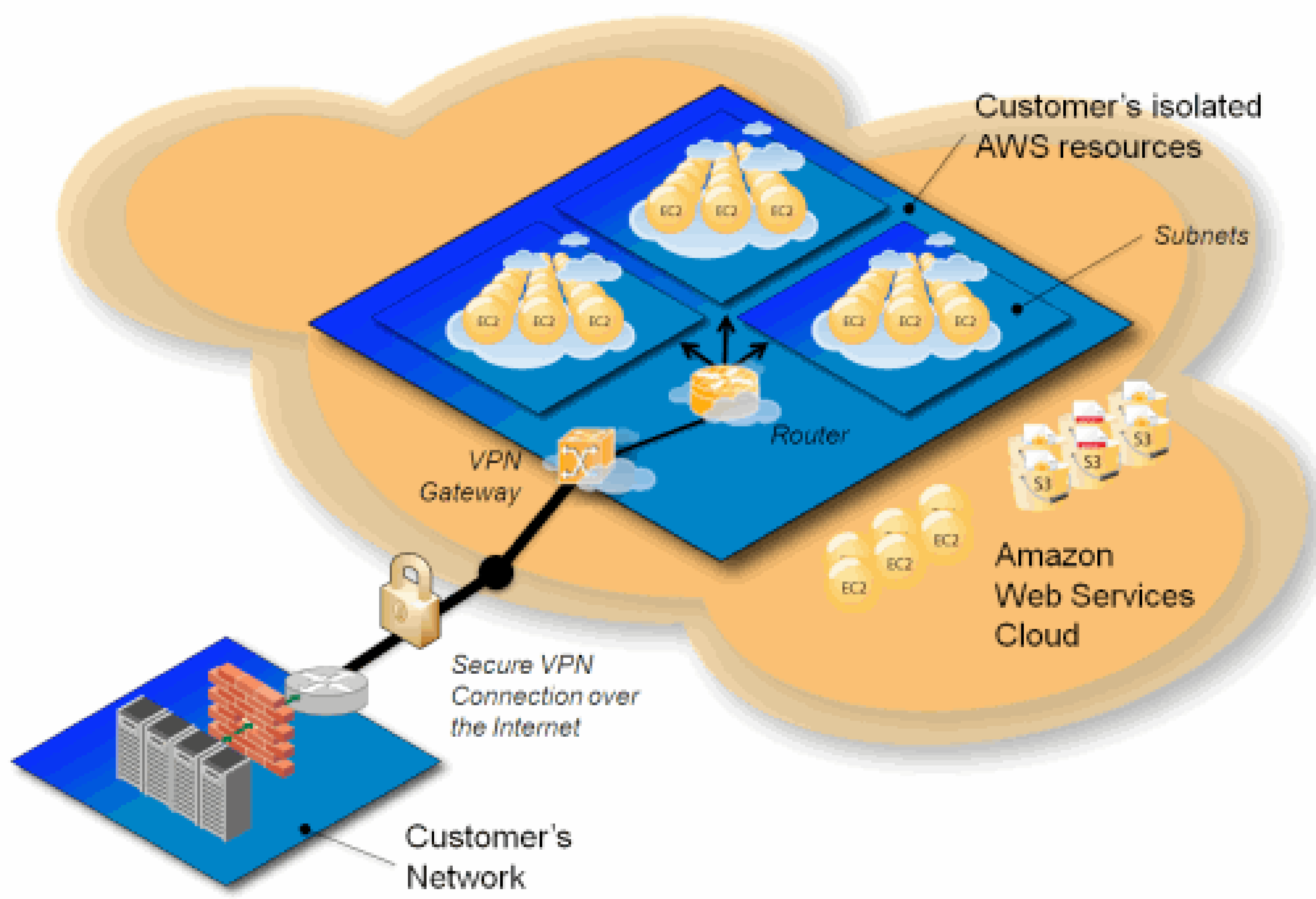
Note the outsourced/insourced factor: you could have an internal cloud run by a 3rd party

Public Cloud



Microsoft Azure software and services
- write software locally, upload to cloud et voila
- support for multiple languages coming soon
- all interfaces are publicly exposed to entire net
- administration performed via API call
- all the usual website and webservices security concerns

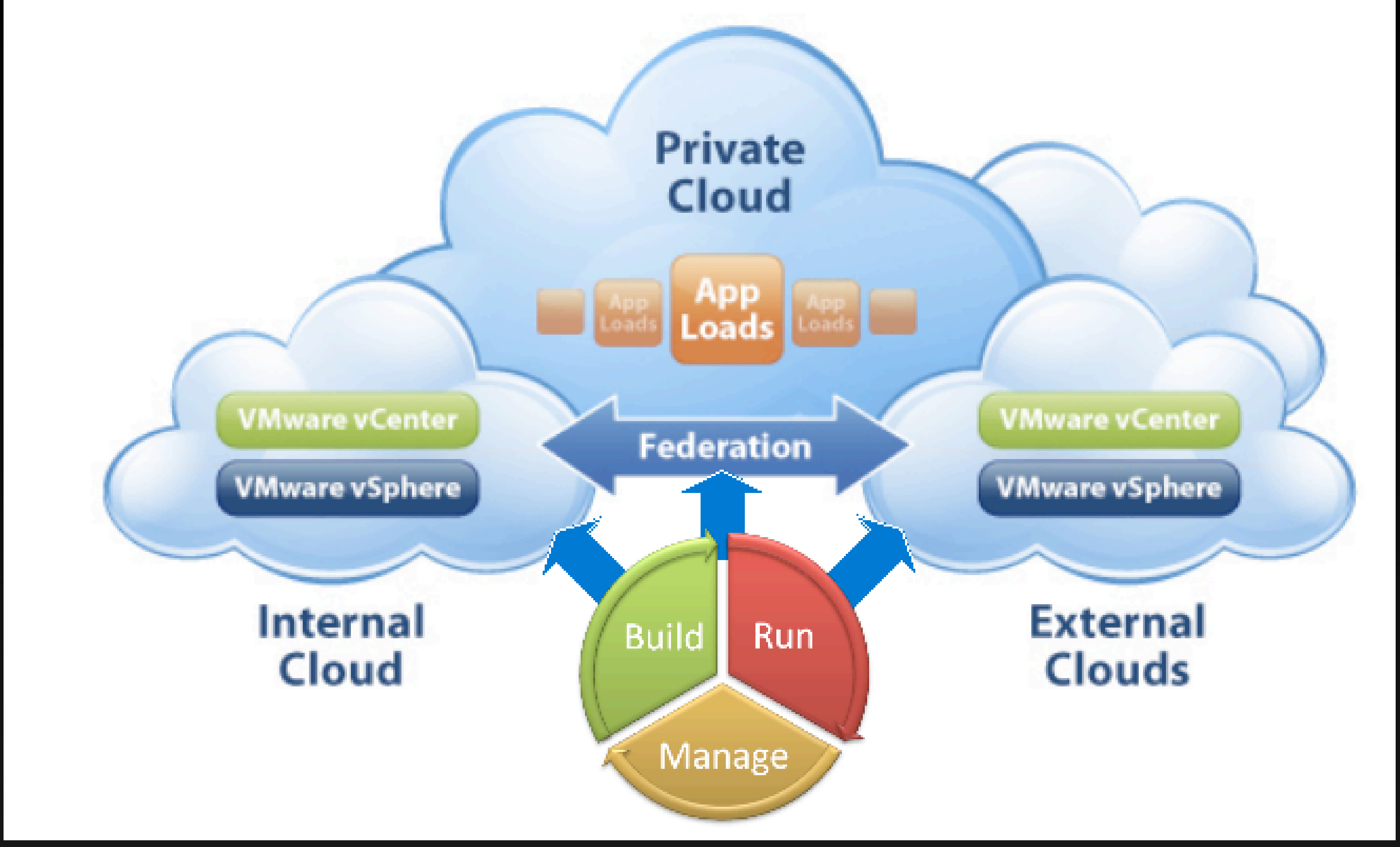
Virtual Private Cloud



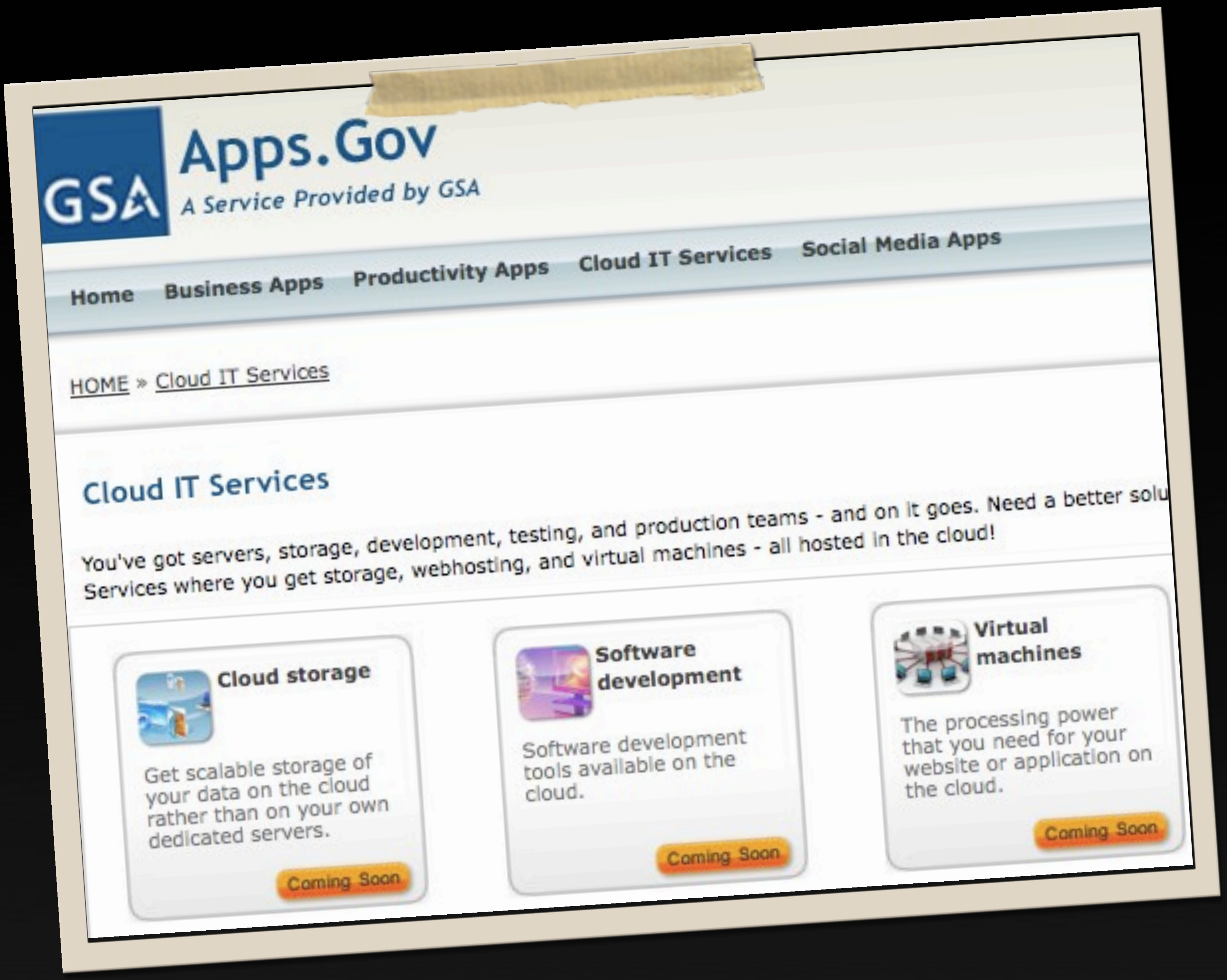
Amazon just introduced a Virtual Private Cloud offering
- EC2 only supports a single NIC
- usually this is attached to the public EC2
- VPC switches this to a ‘private’ network address space
- your org connects via a standard VPN tunnel
- currently VPC hosts cannot connect direct to internet (coming soon!)

The attack surface is the virtualized NIC driver...? Hard to tell as Amazon haven’t published any decent technical details...

Private Cloud



Attractive for those with existing data centers/investment
VMware, Cisco & EMC making a strategic play for your private cloud business
Note; can exist in your DC or a 3rd party provider with private VPN connection
Appropriate for workloads that need more security than offered by public clouds
Some will have hooks to public clouds for test/dev workloads
The attack surface is considerable – new products, new protocols, new networking technologies
Plus all the usual OS bugs above the hypervisor.



Apps.Gov

A Service Provided by GSA

HOME » Cloud IT Services

Cloud IT Services

You've got servers, storage, development, testing, and production teams - and on it goes. Need a better solu
Services where you get storage, webhosting, and virtual machines - all hosted in the cloud!

Cloud storage

Get scalable storage of your data on the cloud rather than on your own dedicated servers.

Software development

Software development tools available on the cloud.

Virtual machines

The processing power that you need for your website or application on the cloud.

Government Clouds

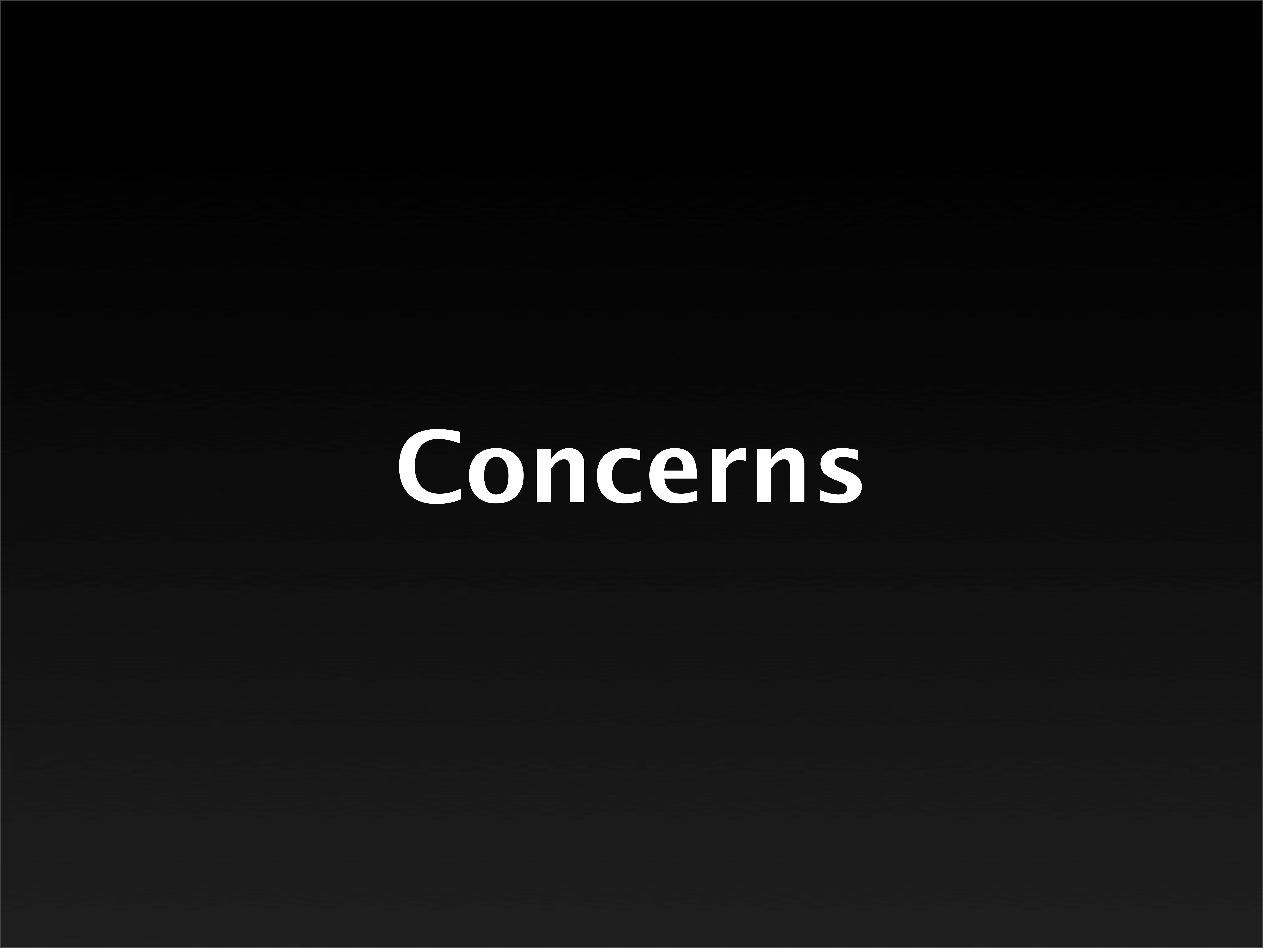
how about citizens data in the cloud?
what are the privacy implications?
example: US gov just announced an AppStore so federal departments can quickly gain access to cloud enabled apps.
Back to europe - what is your government doing?
Who is looking at the privacy aspects?

Home-brew Cloud

This is a purely gratuitous slide - showing one guys home brew arrangement ;-)

A Wise Man Once Said…

A wise Douglas once said ‘Don’t Panic’
As a security person considering cloud platforms, services and models - its easy to have an allergic reaction.
But use the cloud layers and the cube model as a kind of lens to scope your thinking about cloud.



Concerns

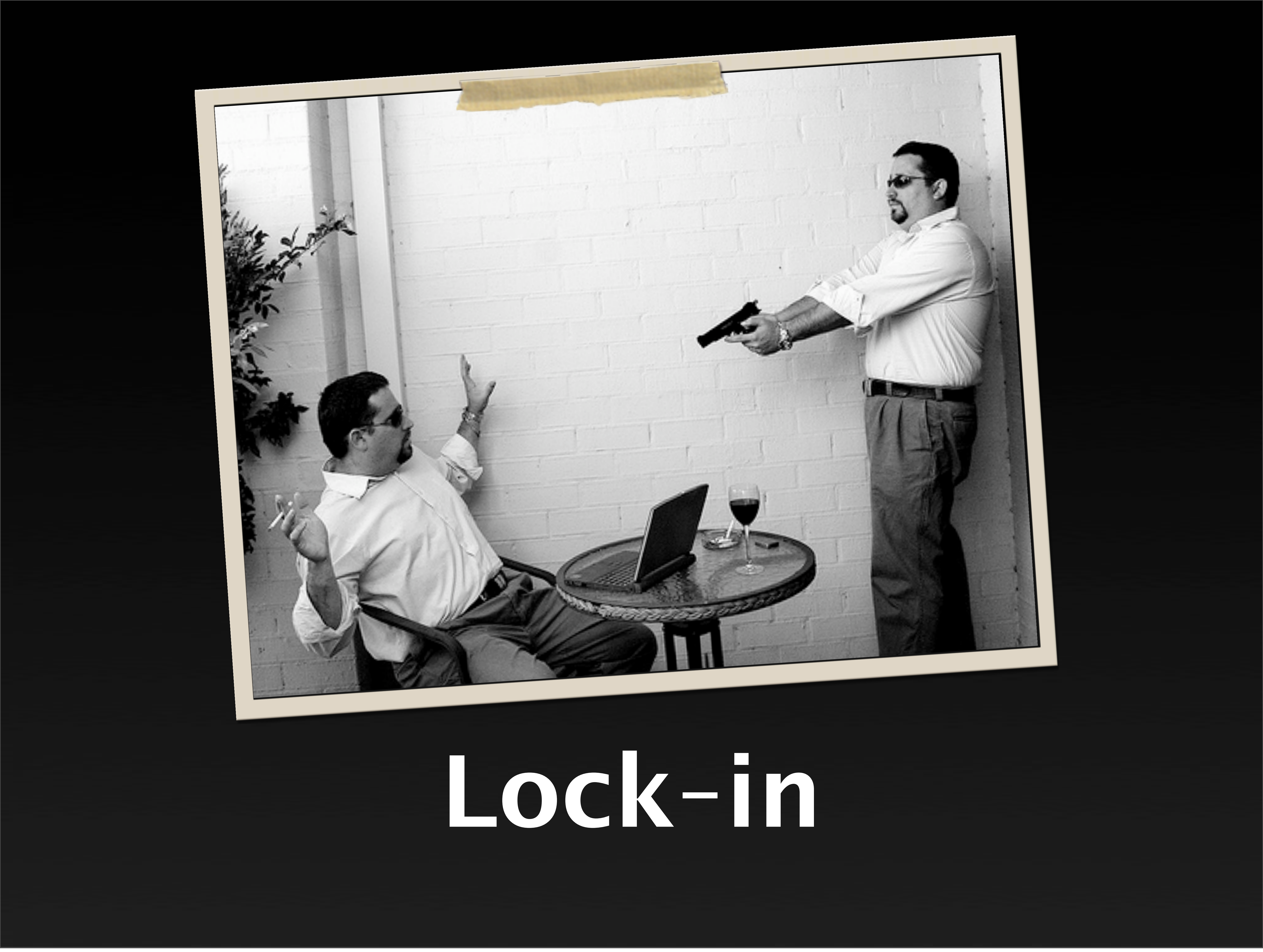
My advice: evaluate these concerns in the context of the layer you are considering and the workload you are looking to "put into the cloud"
Some concerns may not exist at certain layers but be overwhelming at other layers.

What Are They Hiding in the Basement?

In fact, lets ask a seemingly simpler question: where are they hiding their data centers?
Some make a sport out of locating Google DC’s for example
Unless you’re a very large customer, don’t expect a DC tour anytime soon, let alone going down to the basement

Uptime

This is pretty self-explanatory
Clouds are complex distributed systems with considerable ‘state’.
When state goes bad, clouds crash (ask Amazon, google etc)
Or perhaps uptime is affected by your neighbours?
Will come onto hypervisor stalking later.



Lock-in

This one varies considerably depending on what layer we’re talking about

Examples:
- IaaS = VM portability/format
- PaaS= application portability + data portability + API compatibility (e.g. Google BigTable)

The antidote to data lock in is simply to use multiple providers to store the same data - provides DR capability too

Multi Tenancy

Multi-tenancy can be implemented in different ways.
Why is this interesting?
Consider how customer data is stored and hence accessed at the backend
Separate database vs separate database schema vs separate rows in a single table
Even simple SQL Injection holes can land you other customers rows of data...

Change Control

*"…someone once likened the process of upgrading our core websearch infrastructure to "**changing the tires on a car while you're going at 60 down the freeway.** "*

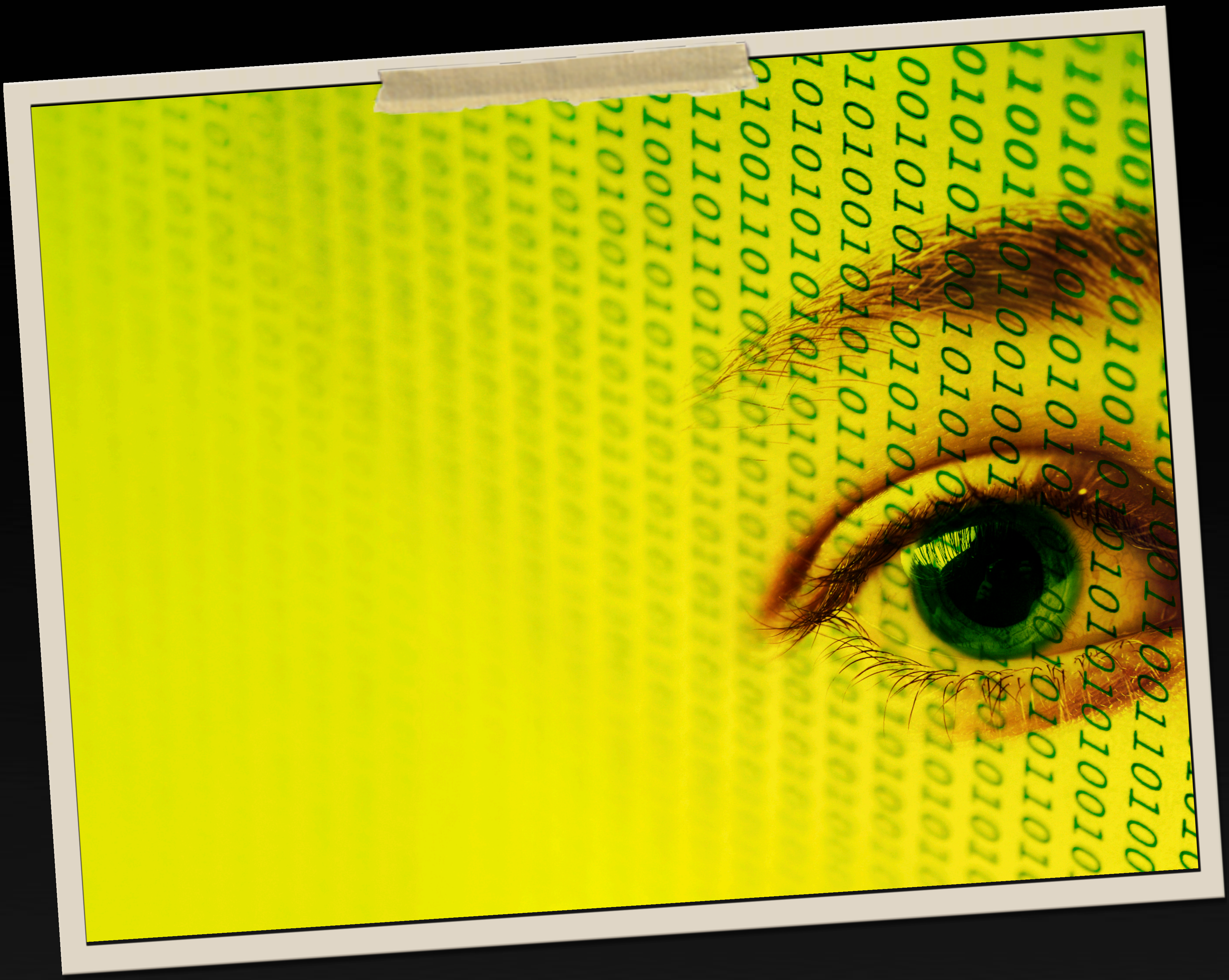
Urs Holzle – SVP Operations, Google

Oh and no changelog ;-)

Stuff changes in mid-flight and you may or may not be informed beforehand

What does this mean for data integrity?

Or more importantly for service assurance? The version you had pen-tested yesterday is not the same version today...



Visibility

Cloud Layers

Some cloud services are built atop other cloud services
This introduces dependancies
What is one cloud provider goes bust, or gets hacked or is DDoSed.
From an attack perspective:
- use documentation and/or Maltego to discover dependancies
- footprint & attack weakest
- yup, this is about protecting the cloud supply chain

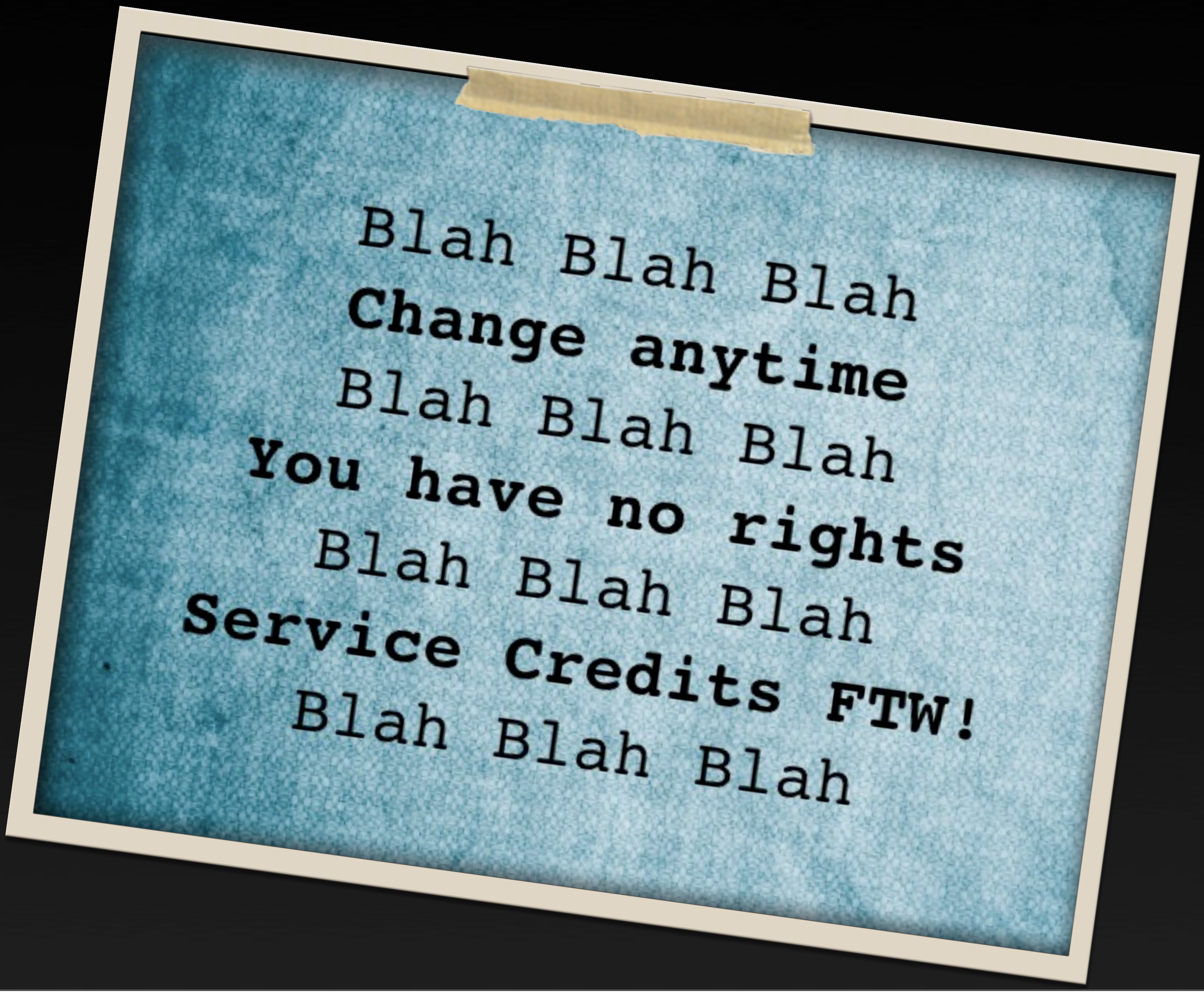
Identity

We haven’t fixed identify, access and management in the enterprise.
Nor have we done so on the Internet
Now the two worlds all colliding.
This is a complex issue - if you’re interested in it, check out project Geneva
MS Azure tackles this problem for MS shops with AD adapters etc.
Has anyone installed an AD Adapter in your environment on your DC?
Would you know?

SLAs

The Promises of Tomorrow Written in Ink for You to sign up to today.

Terms of Service



Blah Blah Blah

Change anytime

Blah Blah Blah

You have no rights

Blah Blah Blah

Service Credits FTW!

Blah Blah Blah

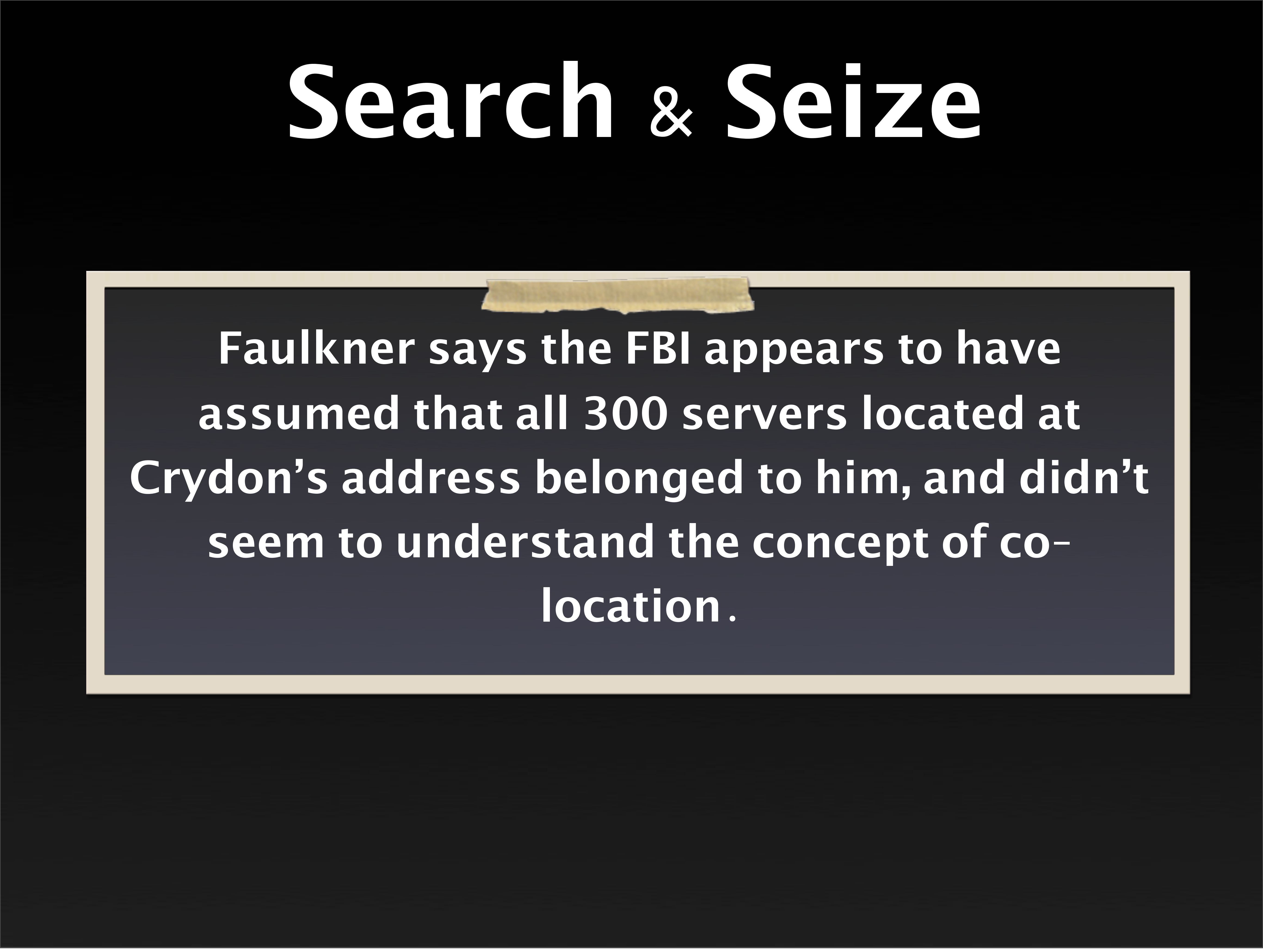
Legal Issues

Cross border data transfer
regulated entities are familiar with the issues
BUT your cloud provider may be shuffling bits all over the place for resiliency..

Search & Seize

> The FBI on Tuesday defended its raids on at least two data centers in Texas, in which agents carted out equipment and disrupted service to hundreds of businesses....
>
> These customers essentially lost connectivity to the U.S. after the raid, Faulkner says.

Search & Seizure is not a cloud specific concern by any means
BUT cloud deployments span multiple data centers, potentially jurisdictions or even multiple countries
Um, has anyone got a guide to how this should be handled?



Search & Seize

Faulkner says the FBI appears to have assumed that all 300 servers located at Crydon’s address belonged to him, and didn’t seem to understand the concept of co-location.

co-location. Cloud *is* the new co-lo.
But ultimately the issue for law enforcement is: how do you seize a cloud? (dynamism, hypervisor migration).
Would they even get what they were seeking if they only had access to a single DC?
How well are the authorities doing today with cross-border collaboration?

The Auditor

For regulated entities, public cloud will only be viable in the short-medium term for non-regulated workloads.
The regulated stuff will either stay put, or end up in a private cloud - self hosted or by a 3rd party.

Auditors are only just coming to terms with virtualization.
Expect a long, slow learning curve where the risk is on your shoulders if you go cloud too early

Pay As You Go

Can anyone say DoS? That could get expensive fast...
Or whatever credit card theft & fraud?
What *real-time* anti-fraud controls does your cloud provider use?
What happens if you don’t pay for whatever reason? (see ToS)

Data Wiping

Public cloud providers don’t offer secure wipe options for their object stores
Amazon BETA issue

Distributed Programming

Distributed programming isn’t new - nor is it specific to cloud BUT
this is distributed computing on a HUGE scale with sequences of interactions that the providers themselves don’t predict (see last Google outage)

I argue this is a mindset change for programmers used to client/server

Race conditions, Time-to-check-to-time-of-use style issues

State that isn’t replicated

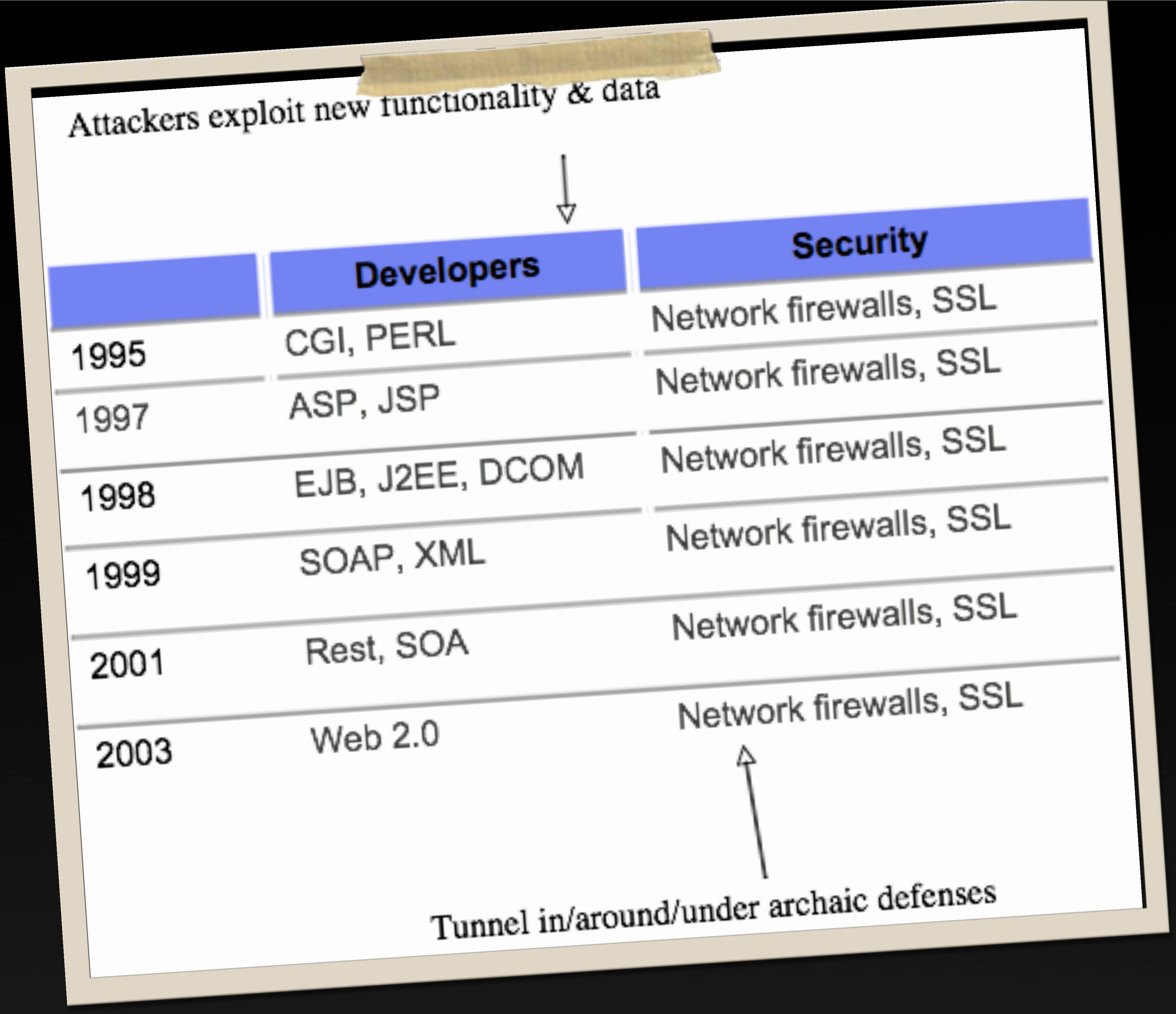
Data that hasn’t been committed to all shards

Eventually consistent is the name of the game in the cloud.

Since your apps will make business decisions on whatever copy of the data your provider returned, your app needs to handle this gracefully!

Cloud APIs

How you consume cloud services
Web Services - aka WS* etc
Has anyone used any? What for?
What Security did you notice?



Attackers exploit new functionality & data

	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

Tunnel in/around/under archaic defenses

When's the Revolution?

Gunnar Peterson's take on the evolution of security....comparing the technologies developers were using vs. what security people were using to protect their orgs

Hmmm, we're not exactly progressive are we? We seem to rely on SSL a lot...

SSLmo

Anyone know who this is?
SSLMo, he appears whenever anyone mentions security and cloud in the same sentence...but he has some issues

Where is Tin Tin?

POP QUIZ: anyone know the name of the building Tin Tin is visiting?

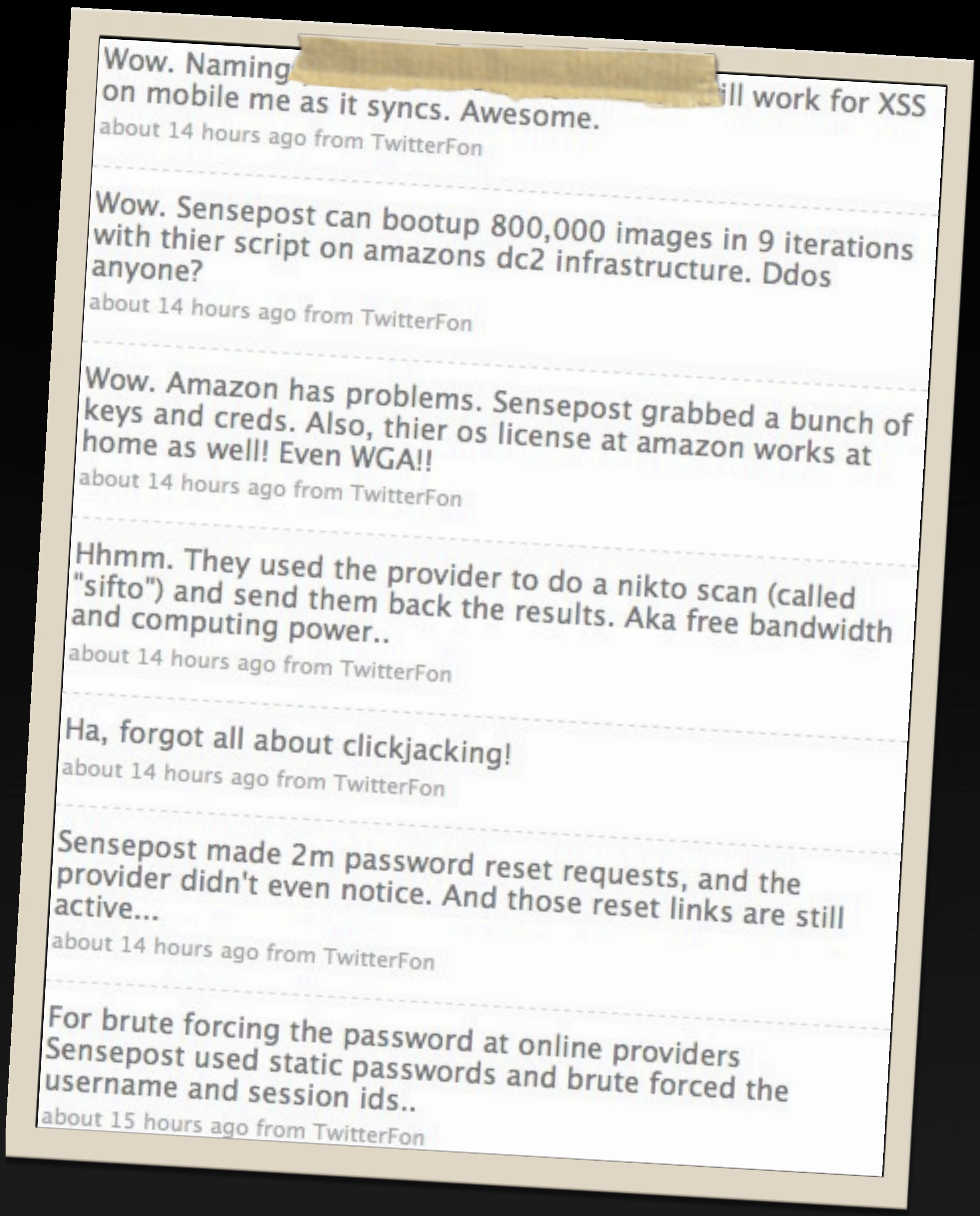
All Your SSL...

Moxie Marlinspike already owns us 10 billion ways with SSL. Who has read his papers? Tempting to say SSL is dead after reading them. OCSP - scary stuff, revocation doesn't really work...but this is primarily about browser implementations

BUT WAIT! Aren't we relying on browser management interfaces to manage some of our cloud stuff? Oh...

Back to the real-world: Online banks, stores etc didn't flinch. Business as usual. Vulns are there but threat may be small (but devastating when it happens).

Vuln Research



Wow. Naming [redacted] ill work for XSS on mobile me as it syncs. Awesome.
about 14 hours ago from TwitterFon

Wow. Sensepost can bootup 800,000 images in 9 iterations with thier script on amazons dc2 infrastructure. Ddos anyone?
about 14 hours ago from TwitterFon

Wow. Amazon has problems. Sensepost grabbed a bunch of keys and creds. Also, thier os license at amazon works at home as well! Even WGA!!
about 14 hours ago from TwitterFon

Hhmm. They used the provider to do a nikto scan (called "sifto") and send them back the results. Aka free bandwidth and computing power..
about 14 hours ago from TwitterFon

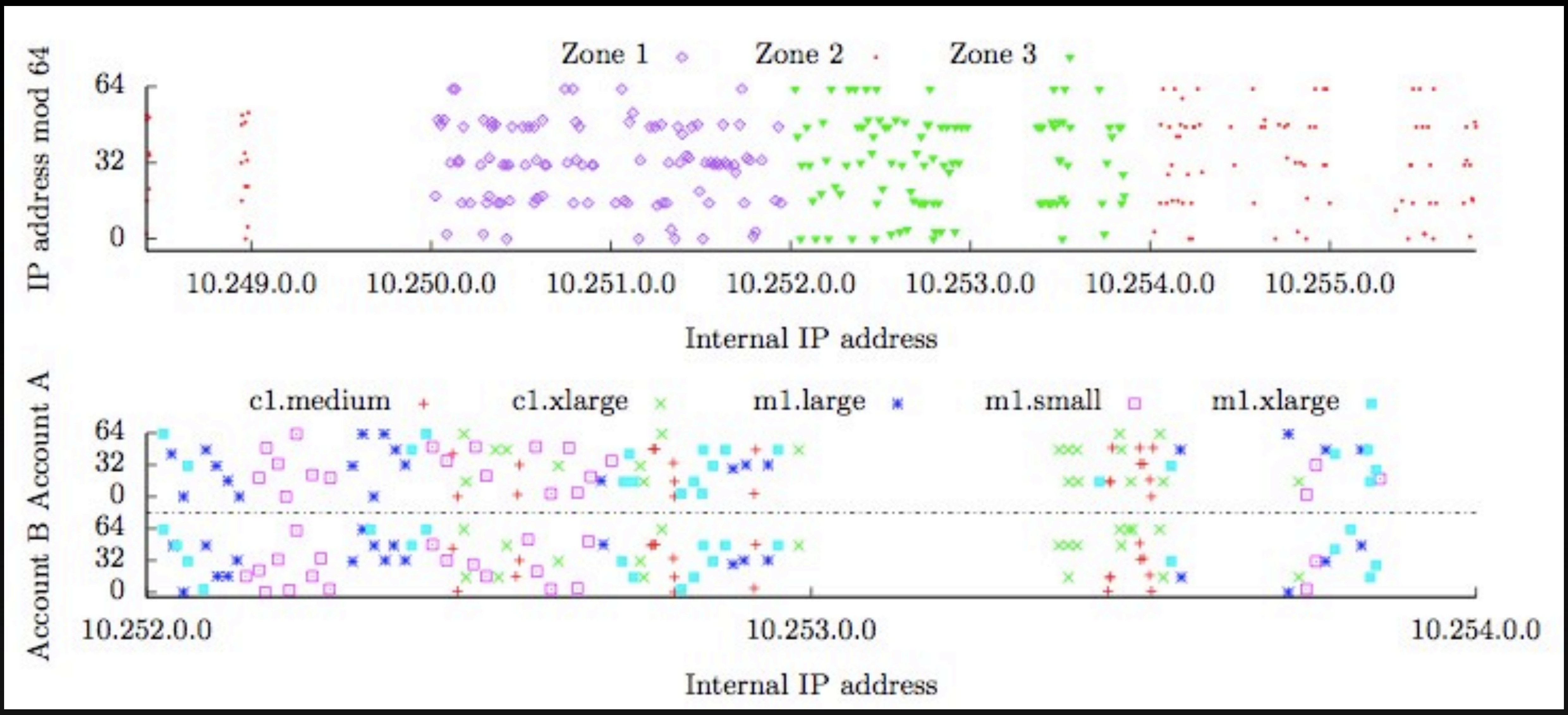
Ha, forgot all about clickjacking!
about 14 hours ago from TwitterFon

Sensepost made 2m password reset requests, and the provider didn't even notice. And those reset links are still active...
about 14 hours ago from TwitterFon

For brute forcing the password at online providers Sensepost used static passwords and brute forced the username and session ids..
about 15 hours ago from TwitterFon

Sensepost kicking the tyres.

weaknesses in processes & procedures

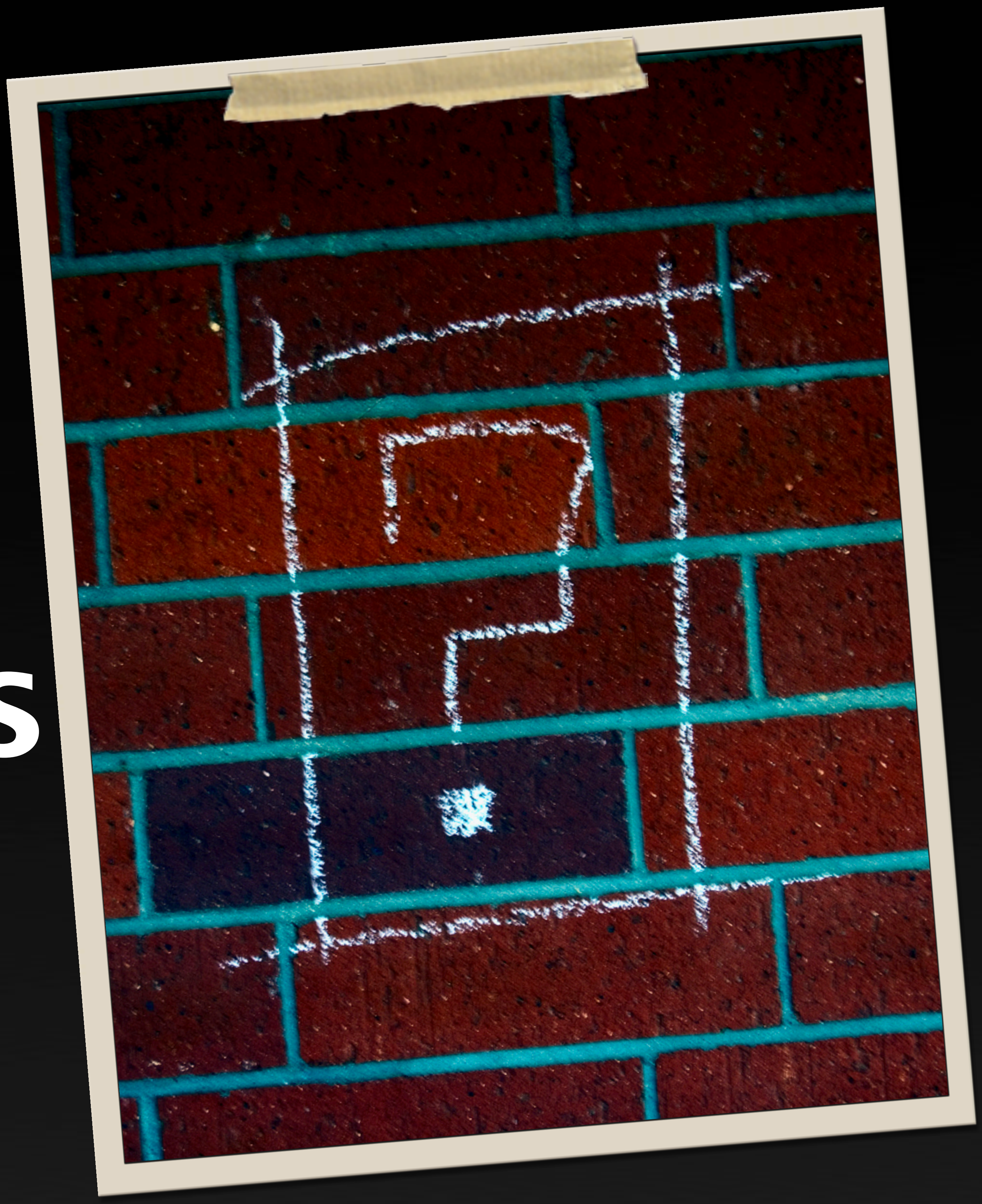


Hypervisor Stalking

In IaaS, how close can you get to your target?
Researchers explored Amazon EC2
Found you could reliably get on same physical hardware as target reliably
Also: side channel attacks

weaknesses in processes & procedures

Call for Researchers



This is a call to vuln researchers
Take your head out of your hypervisor and look around
- Cloud API fuzzing
- Stateful analysis of cloud architectures to find weaknesses
- orchestration & management layers
-

salesforce.com Success. Not Software.

Win B33R!

xyz.com pledges not to initiate legal action against security researchers for penetrating or attempting to penetrate our systems as long as they adhere to the conditions below…
‹snip›

Enlighted Providers

Which enlighted provider recently published this vulnerability disclosure policy?

Resources

cloud security alliance℠

Security Guidance for Critical Areas of Focus in Cloud Computing

Prepared by the Cloud Security Alliance

April 2009

Bedtime Reading

Version 2 is out shortly from http://cloudsecurityalliance.org. Grab this and read it - best advice available.

Consider joining the CSA to join in the conversation and improve the guidance.

Non-profit, open to vendors, customers and anyone else (e.g. vulnerability researchers)

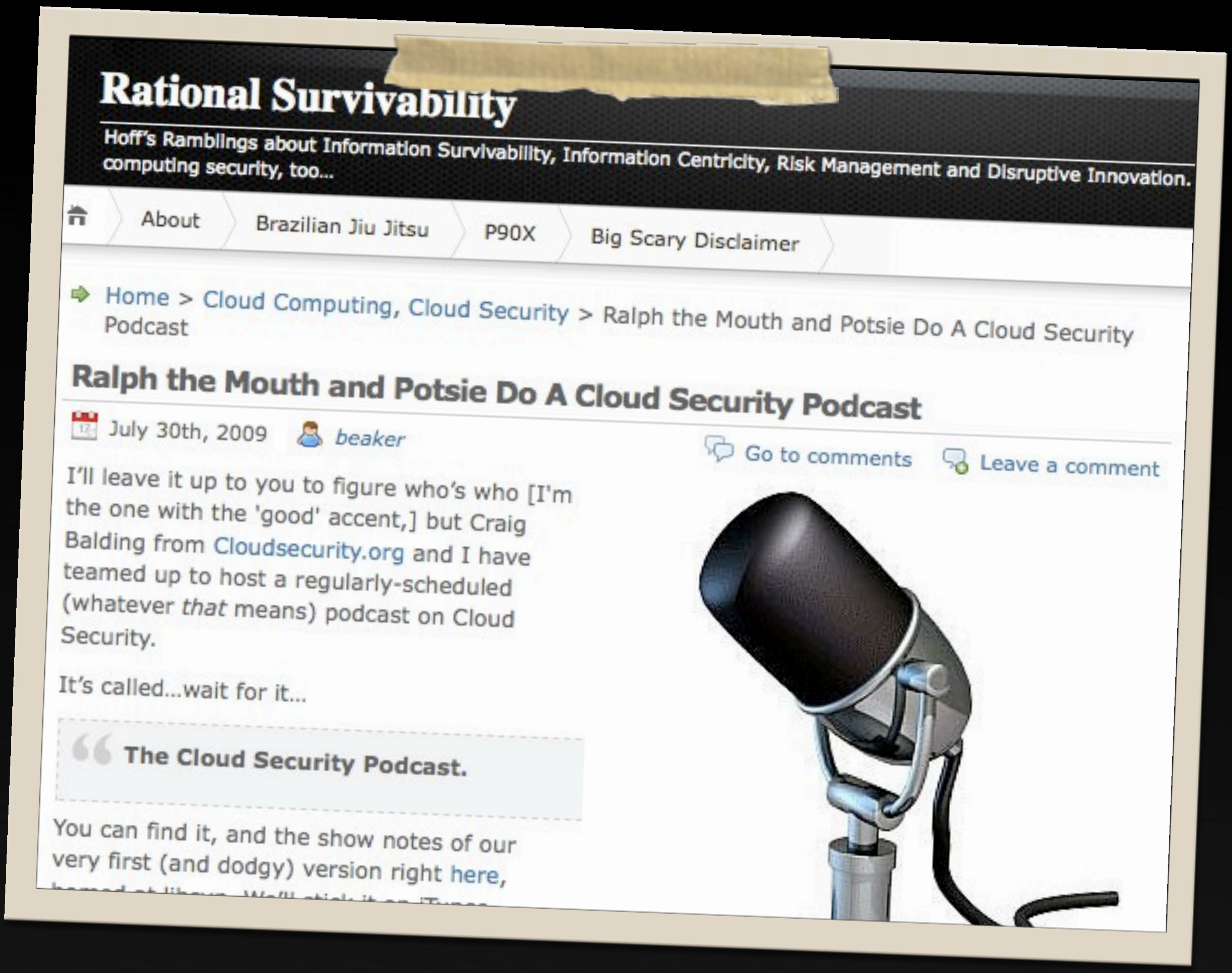
Cloud Computing and Security For The Masses: Interview on NPR

What Does PCI Compliance in the Cloud Really Mean?

Cloudsecurity.org Interviews Guido van Rossum: Google App Engine, Python and Security

cloudsecurity.org

My blog
Check the “Resources” page for a list of other non-security specific cloud blogs



Rational Survivability

Hoff's Ramblings about Information Survivability, Information Centricity, Risk Management and Disruptive Innovation.
computing security, too...

Home > Cloud Computing, Cloud Security > Ralph the Mouth and Potsie Do A Cloud Security Podcast

Ralph the Mouth and Potsie Do A Cloud Security Podcast

July 30th, 2009 beaker

I'll leave it up to you to figure who's who [I'm the one with the 'good' accent,] but Craig Balding from Cloudsecurity.org and I have teamed up to host a regularly-scheduled (whatever *that* means) podcast on Cloud Security.

It's called...wait for it...

> The Cloud Security Podcast.

You can find it, and the show notes of our very first (and dodgy) version right here,

rationalsurvivability.com/blog

Chris Hoffs' blog.

Very smart + good sense of humour makes for an interesting read.

Subscribe!

Too Much Cloud?

If this has all been too much cloud for you, you'll like the next slide...

EOF

cloudsecurity.org

craig.balding@gmail.com

Thanks for listening.

Meet me in the bar if you won a beer :-)

Questions?