A Cloud Security Ghost Story

Craig Balding cloudsecurity.org

Disclaimer

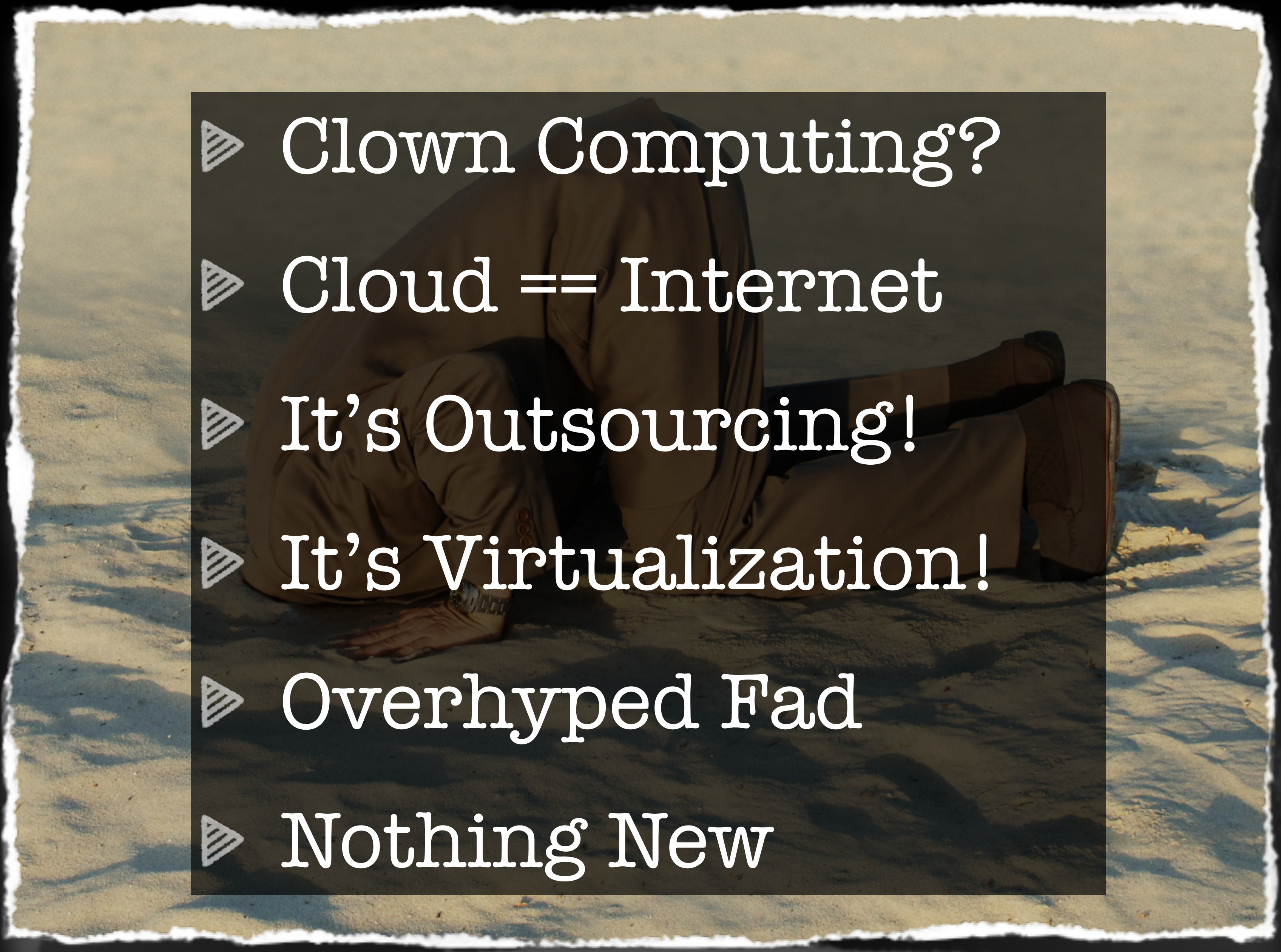
The views and opinions expressed here are those of Craig Balding only and in no way represent the views, positions or opinions - expressed or implied - of my employer or anyone else.

- Happy to take questions as we go
- Will limit in-flight answers to 2 minutes…
- …to allow time for Q&A at end
- If you want SAP Pwnage, other track ;-)

Tweeting/Blogging?

Please add the tag:

cloudsec



- Clown Computing?
- Cloud == Internet
- It’s Outsourcing!
- It’s Virtualization!
- Overhyped Fad
- Nothing New

Don’t Believe in Clouds?

- A Service Model
- *aaS: ...as a Service
- On-Demand
- Pay As You Go (CC)
- Elastic
- Abstracted Resource

What Is “Cloud”?

Cloud Security

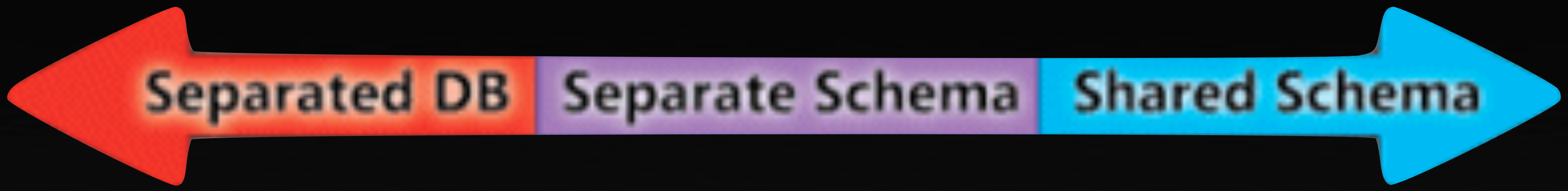
vs.

Security in the Cloud

Avoid the Facepalm

- This is not ASP
- Shared Hardware
- Shared Fabric / Host
- Scalability / Cost

Multi Tenancy

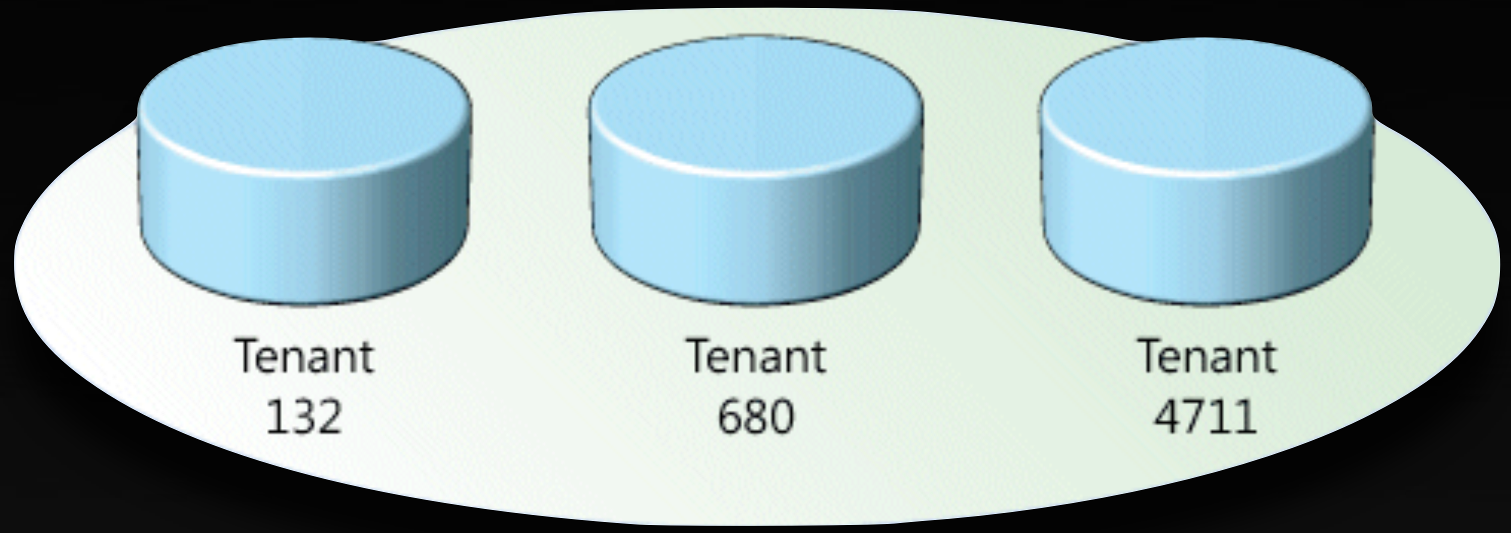


Separated DB

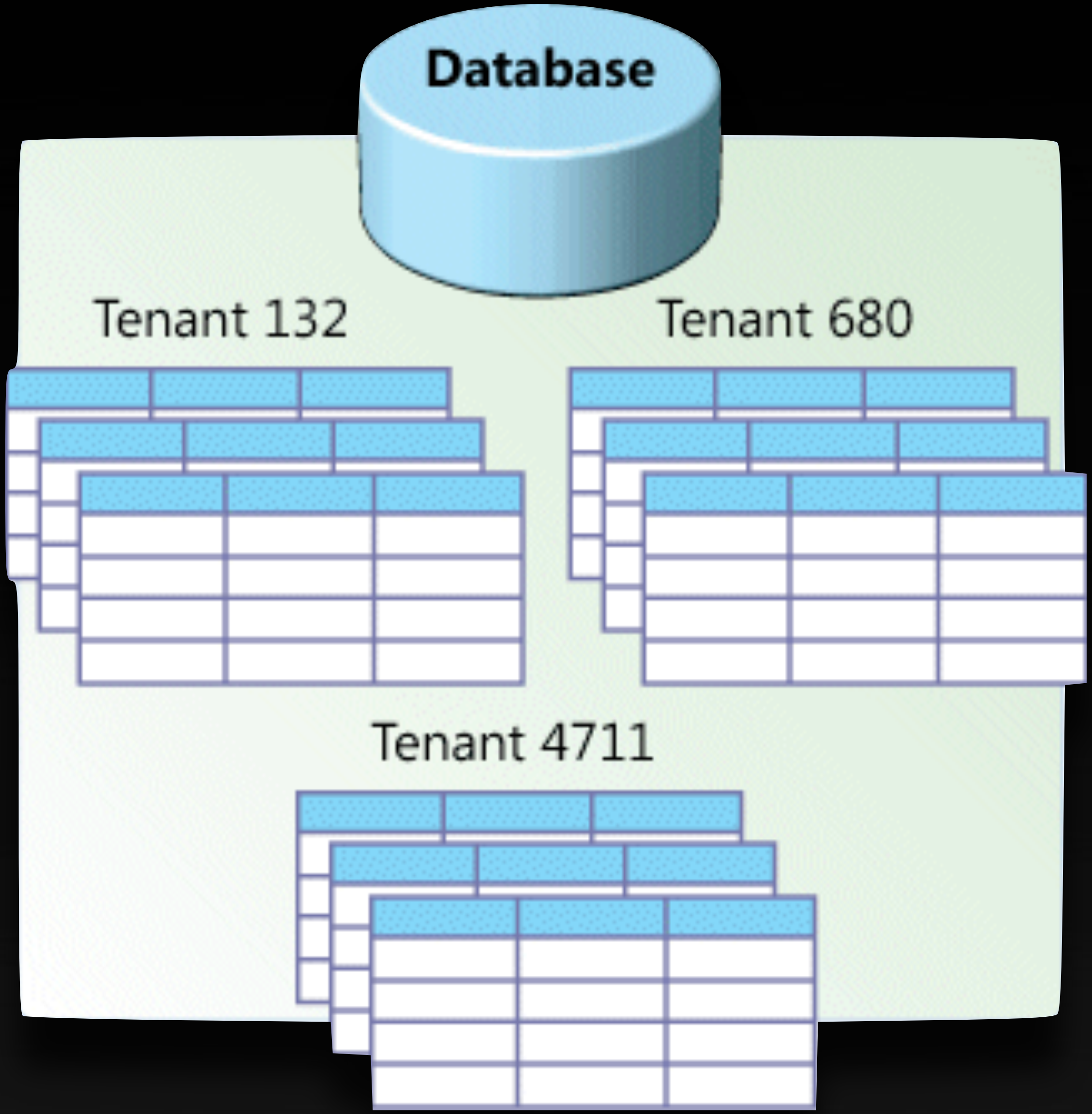
Separate Schema

Shared Schema

DB Security Model



DB == Tenant



DB == Tenant 1..n

- Engineering Feat
- Scalability
- Availability
- New techniques
- 1000:1
- Green

“It’s Only Day 1”

Cloud Magic: Just Say No

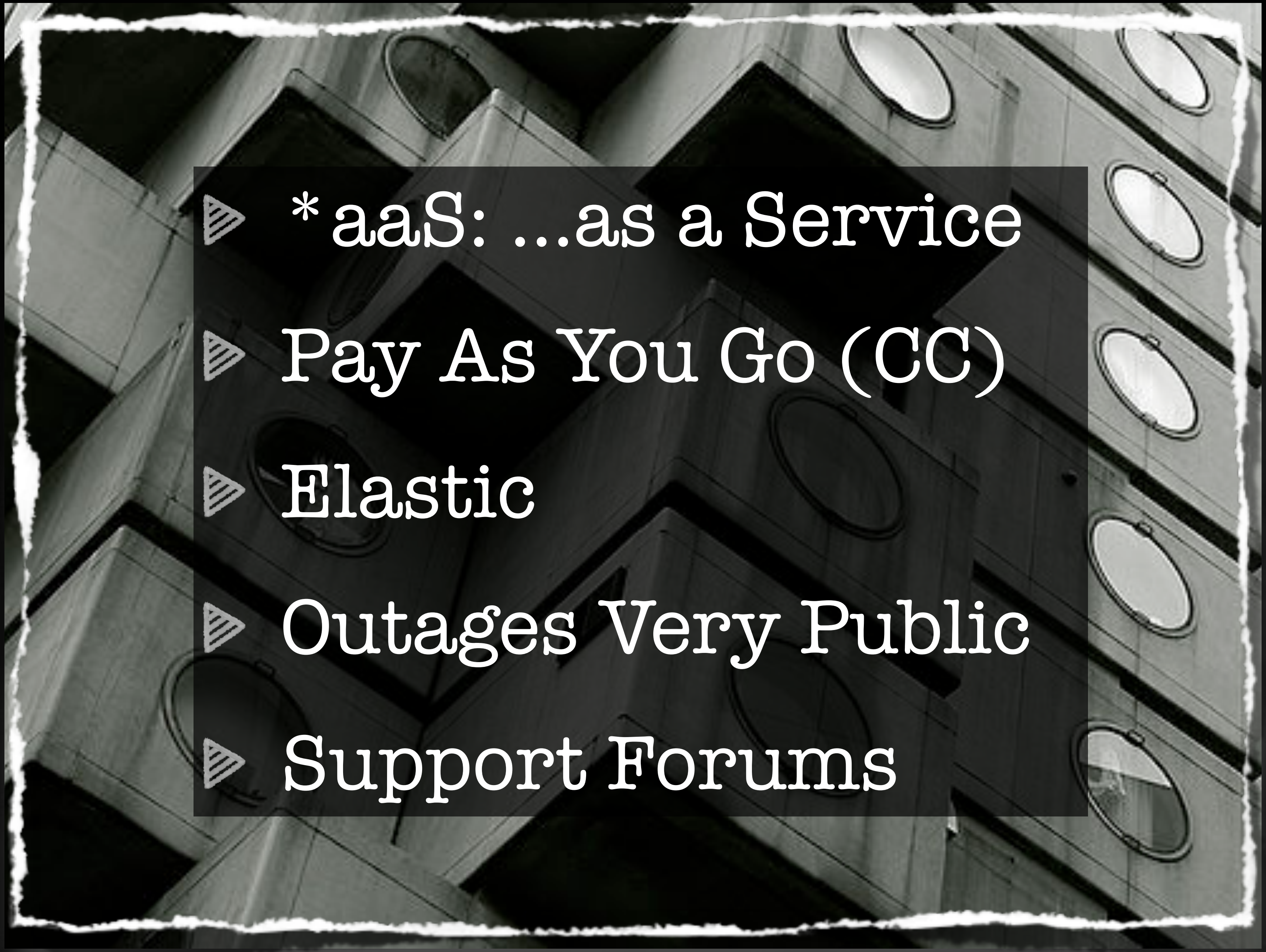
- Evil State
- Replication Woes
- Patching Devils
- Insidious Integrity
- Funding

Cloud FAIL

- Risk Management
- Your Liable
- Compensating Controls
- Plan for Failure
- Trust but Verify
- Web Services Security
- Browsers Are Brittle

Security Givens

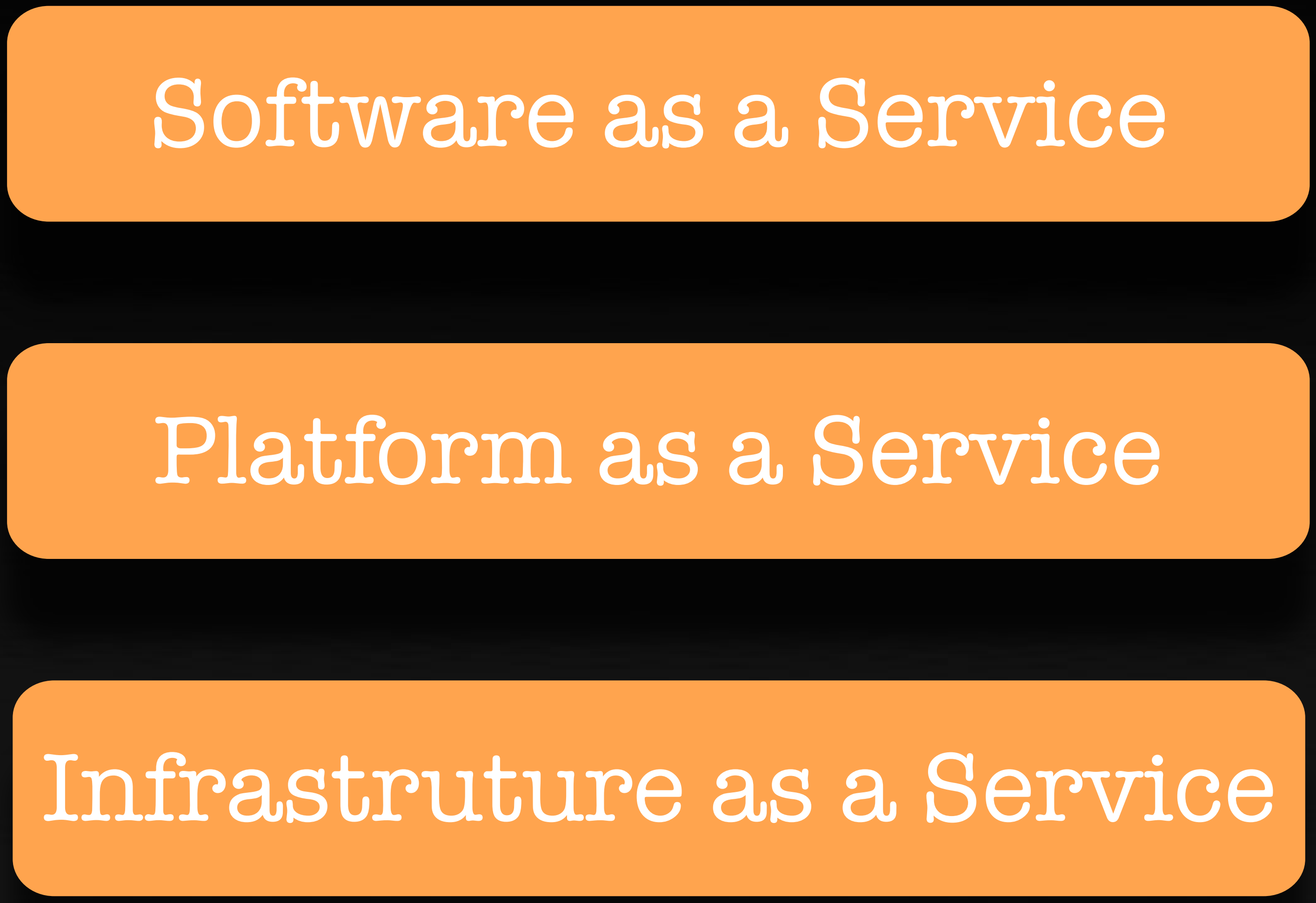
Ghost Central



- *aaS: ...as a Service
- Pay As You Go (CC)
- Elastic
- Outages Very Public
- Support Forums

Public Clouds

Classic SPI Model

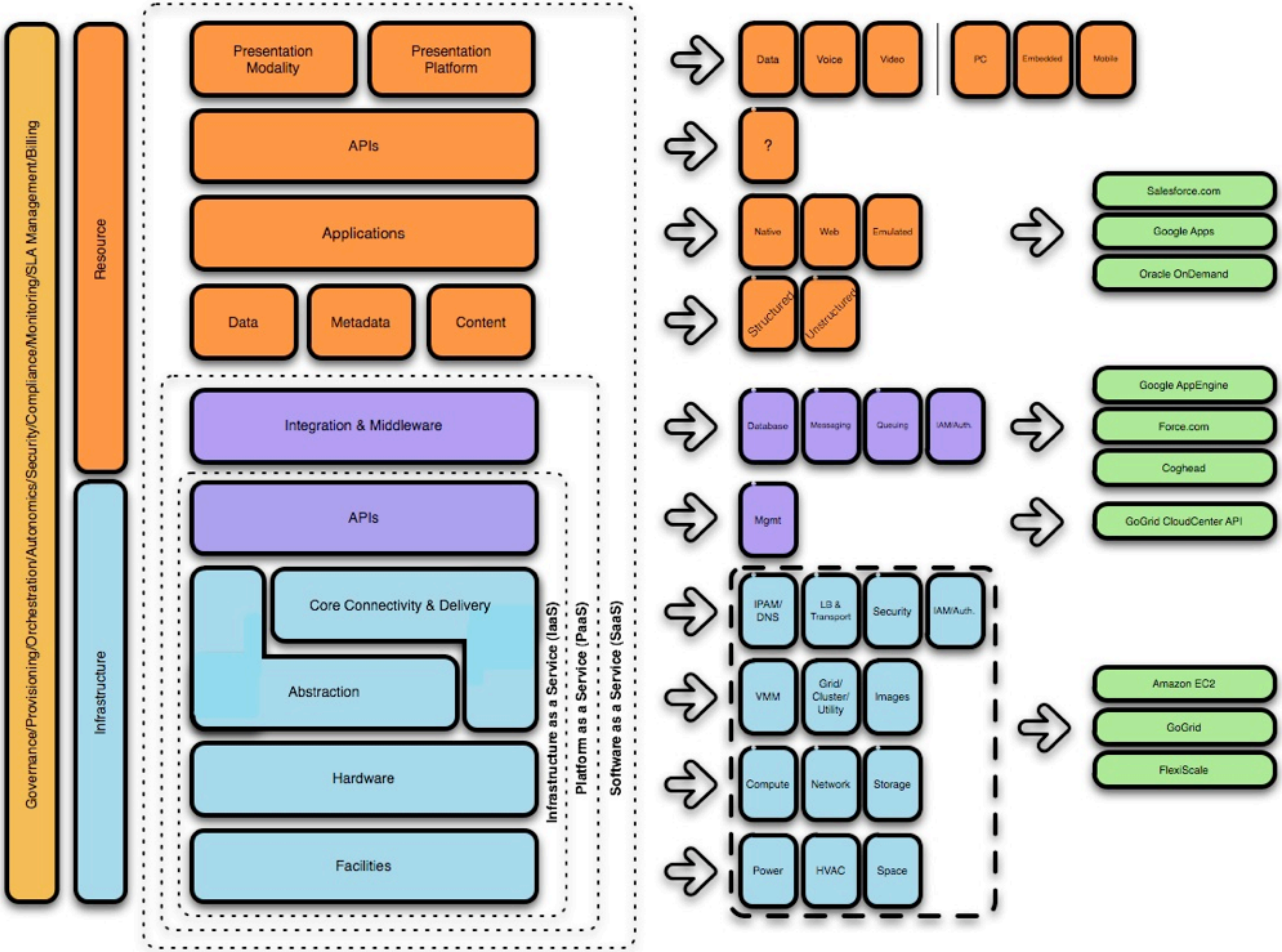


Software as a Service

Platform as a Service

Infrastruture 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

CLOUD TAXONOMY

Infrastructure Services

Storage

- Amazon S3
- InfoBright
- Amazon SimpleDB
- Vertica
- Microsoft SSDS
- CTERA
- Rackspace Mosso CloudFS
- Google BigTable
- Nirvanix

Compute

- Amazon EC2
- Serve Path GoGrid
- Elastra
- Rackspace Mosso Cloud
- Joyent Accelerators
- AppNexus
- Flexiscale
- Elastichosts
- Hosting.com CloudNine
- Terramark
- GridLayer
- iTRiCiTY
- LayeredTech

Services Management

- RightScale
- enStratus
- Scalr
- CohesiveFT
- Kaavo
- CloudStatus
- Ylastic
- Dynect
- CloudFoundry
- NewRelic

Cloud Software

Data

- 10Gen MongoDB
- Oracle Coherence
- Gemstone Gemfire
- Apache CouchDb
- Apache HBase
- Hyperbase
- TerraCotta

Appliances

- PingIdentity
- Symplified
- rPath
- Vordel

Compute

- Globus Toolkit
- Xeround
- Beowulf
- Sun Grid Engine
- Hadoop
- OpenCloud
- IBM eXtreme Scale
- Gigaspaces
- DataSynapse
- Xeround

File Storage

- EMC Atmos
- ParaScale
- Zmamda
- CTERA

Cloud Management

- 3Tera App Logic
- OpenNebula
- Cassatt Active Response
- Open.ControlTier
- Catbird
- Enomaly Enomalism
- Altor NEtworks
- VMware Ops
- Ops-Scorecard
- CohesiveFT VPN Cubed
- Chef
- Hyperic
- Eucalyptus
- Reductive Lbs Puppet
- CollectD
- OpenQRM
- Appistry

Platform Services

General Purpose

- Force.com
- Etelos
- LongJump
- AppJet
- Rollbase
- Bungee Labs Connect
- Google App Engine
- Engine Yard
- Caspio
- Qrimp
- MS Azure Services Platform

Business Intelligence

- Aster DB
- Quantivo
- Cloud9 Analytics
- Blink Logic
- K2 Analytics
- LogiXML
- Oco
- Panorama
- PivotLink
- Sterna
- ColdLight Neuron
- Infobright

Integration

- Amazon SQS
- HubSpace
- MuleSource Mule OnDemand
- Boomi
- SnapLogic
- OpSource Connect
- Cast Iron
- Microsoft BizTalk Services
- gnip
- SnapLogic SaaS Solution Packs
- Appian Anywhere
- HubSpan
- Informatica On-Demand

Development & Testing

- Keynote Systems
- Mercury
- SOASTA
- SkyTap
- WhiteHat Sentinel
- LoadStorm
- BrowserMob
- Collabnet
- Dynamsoft

Authentication

- Ping Identity
- OpenID/OAuth
- Symplified

Software Services

Billing

- Aria Systems
- eVapt
- OpSource
- Redi2
- Zuora

Financials

- Concur
- Xero
- Workday
- Beam4d

Legal

- DirectLaw
- Advologix
- Fios
- Sertifi

Sales

- Xactly
- LucidEra
- StreetSmarts
- Success Metrics

Desktop Productivity

- Zoho
- IBM Lotus Live
- Google Apps
- Desktoptoo
- Parallels
- ClusterSeven

Human Resources

- Taleo
- Workday
- iCIMS

Content Management

- Clickability
- SpringCM
- CrownPoint

Backup & Recovery

- JungleDisk
- Mozy
- Zmanda Cloud Backup
- OpenRSM
- Syncplicity

CRM

- NetSuite
- Parature
- Responsys
- Rightnow
- Salesforce.com
- LiveOps
- MSDynamics
- Oracle On Demand

Document Management

- NetDocuments
- Questys
- DocLanding
- Aconex
- Xythos
- Knowledge TreeLive
- SpringCM

Collaboration

- Box.net
- DropBox

Social Networks

- Ning
- Zembly
- Amitive

OpenCrowd

Examples

- Software as a Service
- Platform as a Service
- Infrastruture as a Service

- SaaS
- CRM
- force.com == PaaS
- AppExchange
- Code Reviews
- Service Cloud

Salesforce

Examples

Software as a Service

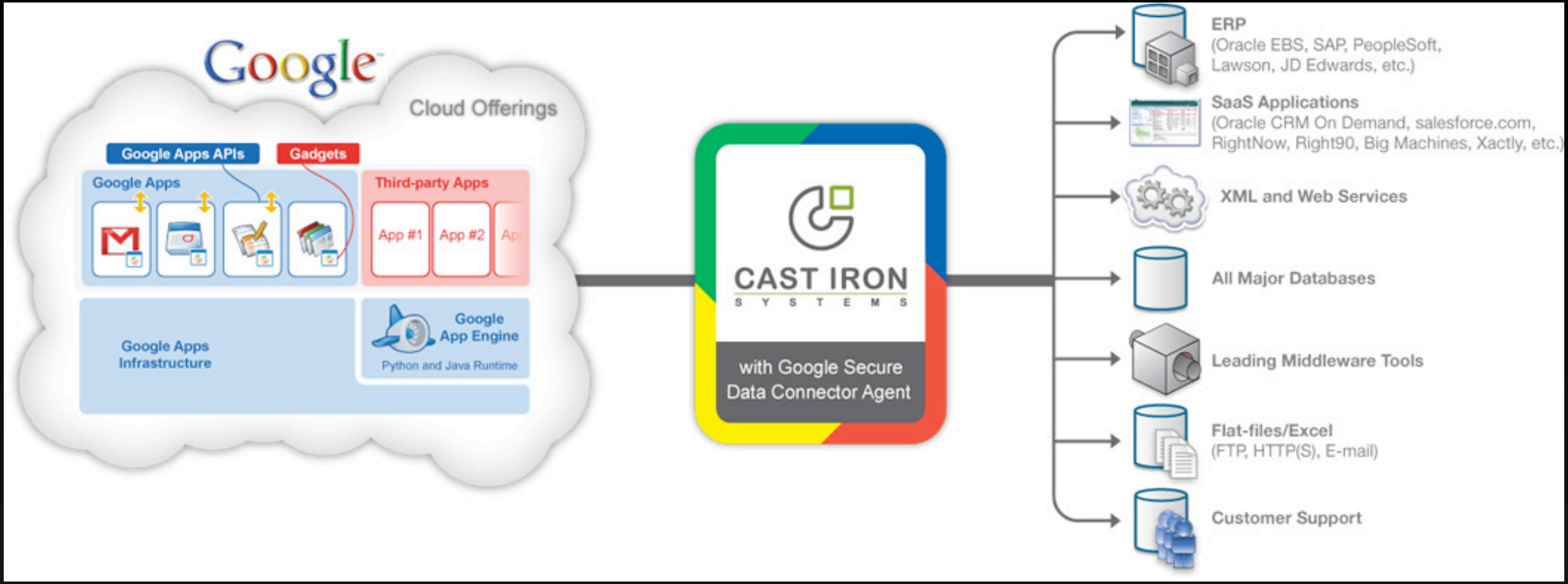
Platform as a Service

Infrastruture as a Service

Google App Engine

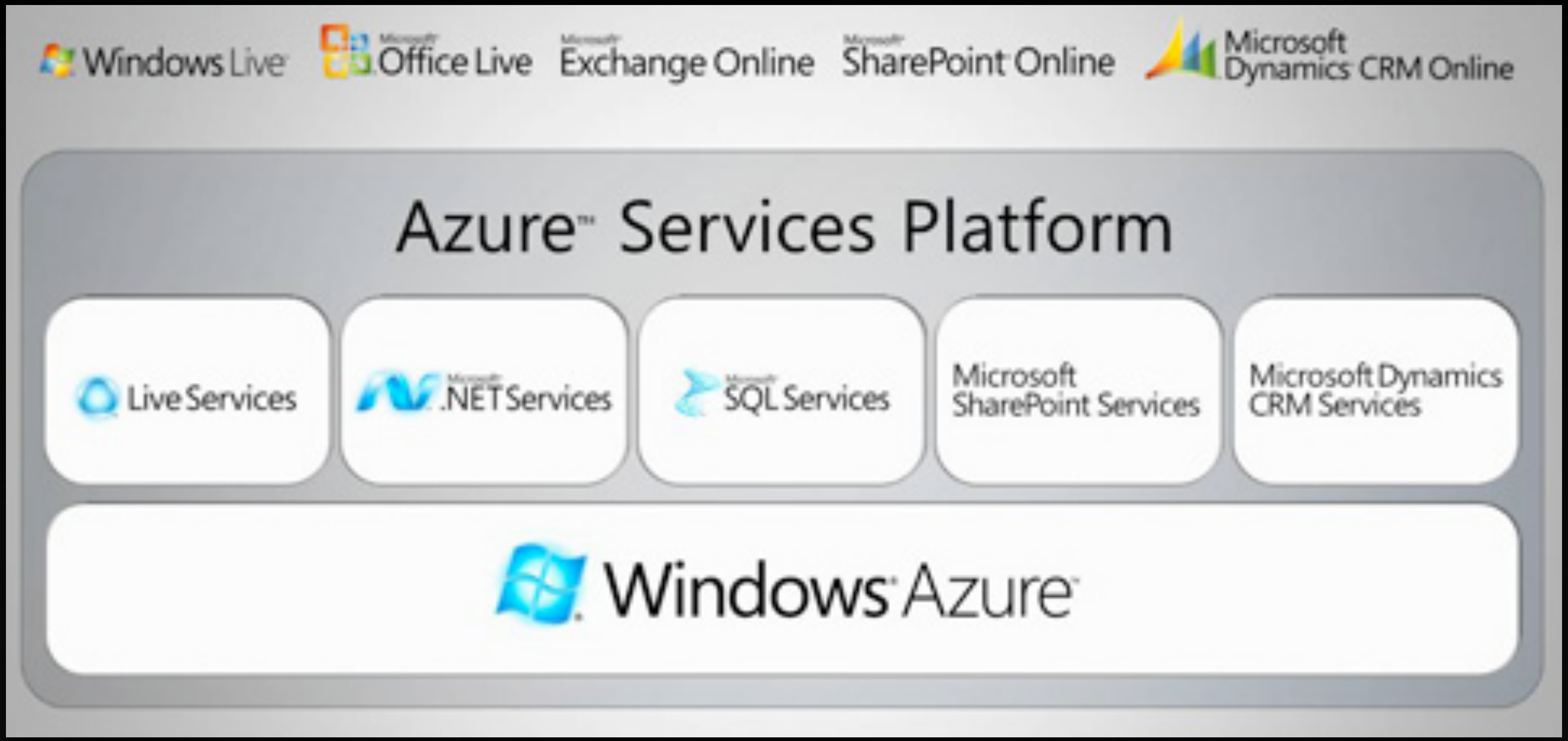
- PaaS
- Python VM
- Justin Ferguson
- Java VM
- Data Import/Export
- SDC

Google Secure Data Connector


Google
Cloud Offerings
Google Apps APIs
Gadgets
Google Apps
Third-party Apps
App #1
App #2
Google Apps Infrastructure
Google App Engine
Python and Java Runtime
CAST IRON SYSTEMS
with Google Secure Data Connector Agent
ERP (Oracle EBS, SAP, PeopleSoft, Lawson, JD Edwards, etc.)
SaaS Applications (Oracle CRM On Demand, salesforce.com, RightNow, Right90, Big Machines, Xactly, etc.)
XML and Web Services
All Major Databases
Leading Middleware Tools
Flat-files/Excel (FTP, HTTP(S), E-mail)
Customer Support

- Software & Services
- Technology Preview
- Identity (Cameron)

Microsoft Azure


Windows Live
Microsoft Office Live
Microsoft Exchange Online
Microsoft SharePoint Online
Microsoft Dynamics CRM Online
Azure™ Services Platform
Live Services
Microsoft .NET Services
Microsoft SQL Services
Microsoft SharePoint Services
Microsoft Dynamics CRM Services
Windows Azure

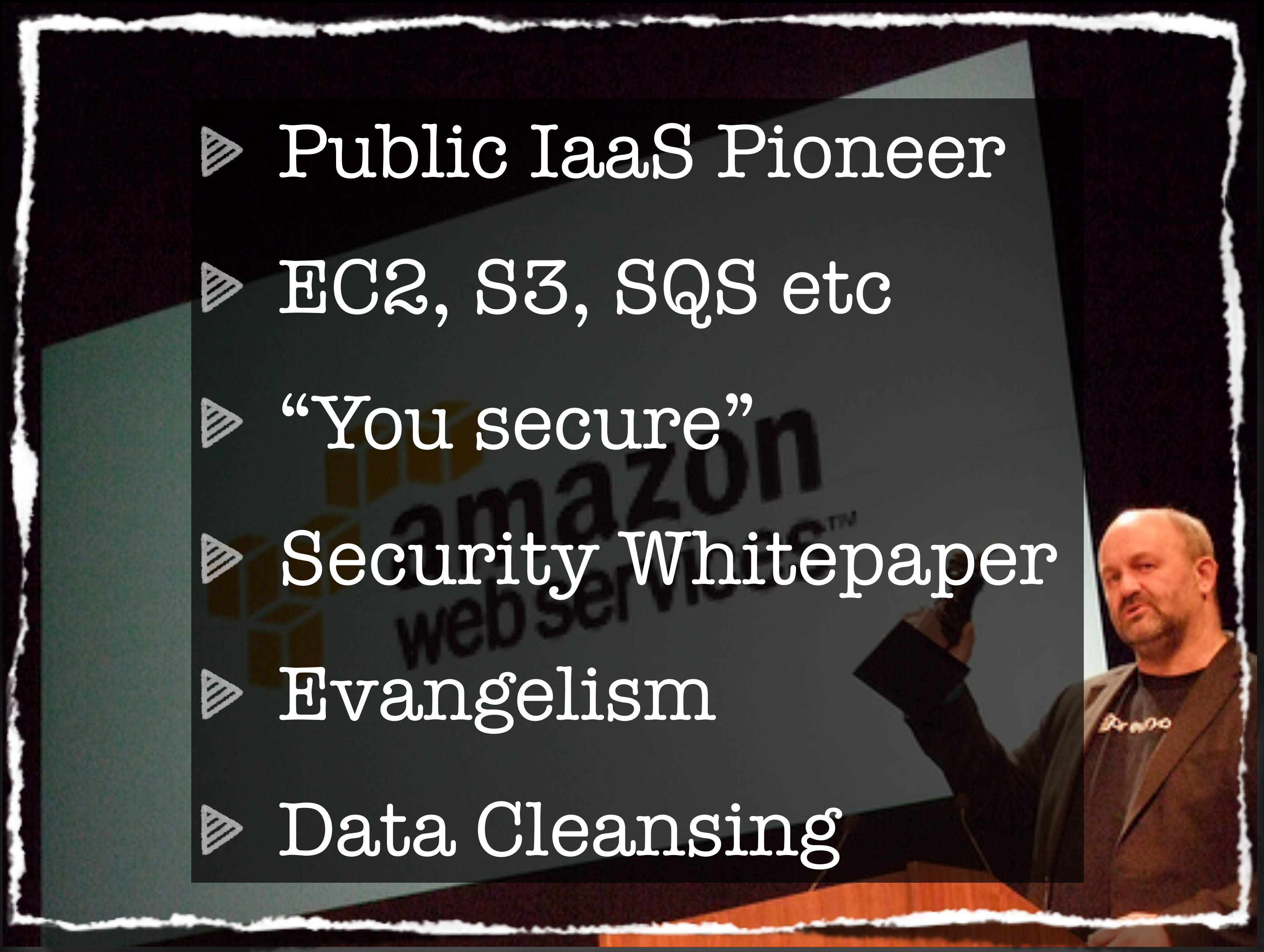
Software + Services

Examples

Software as a Service

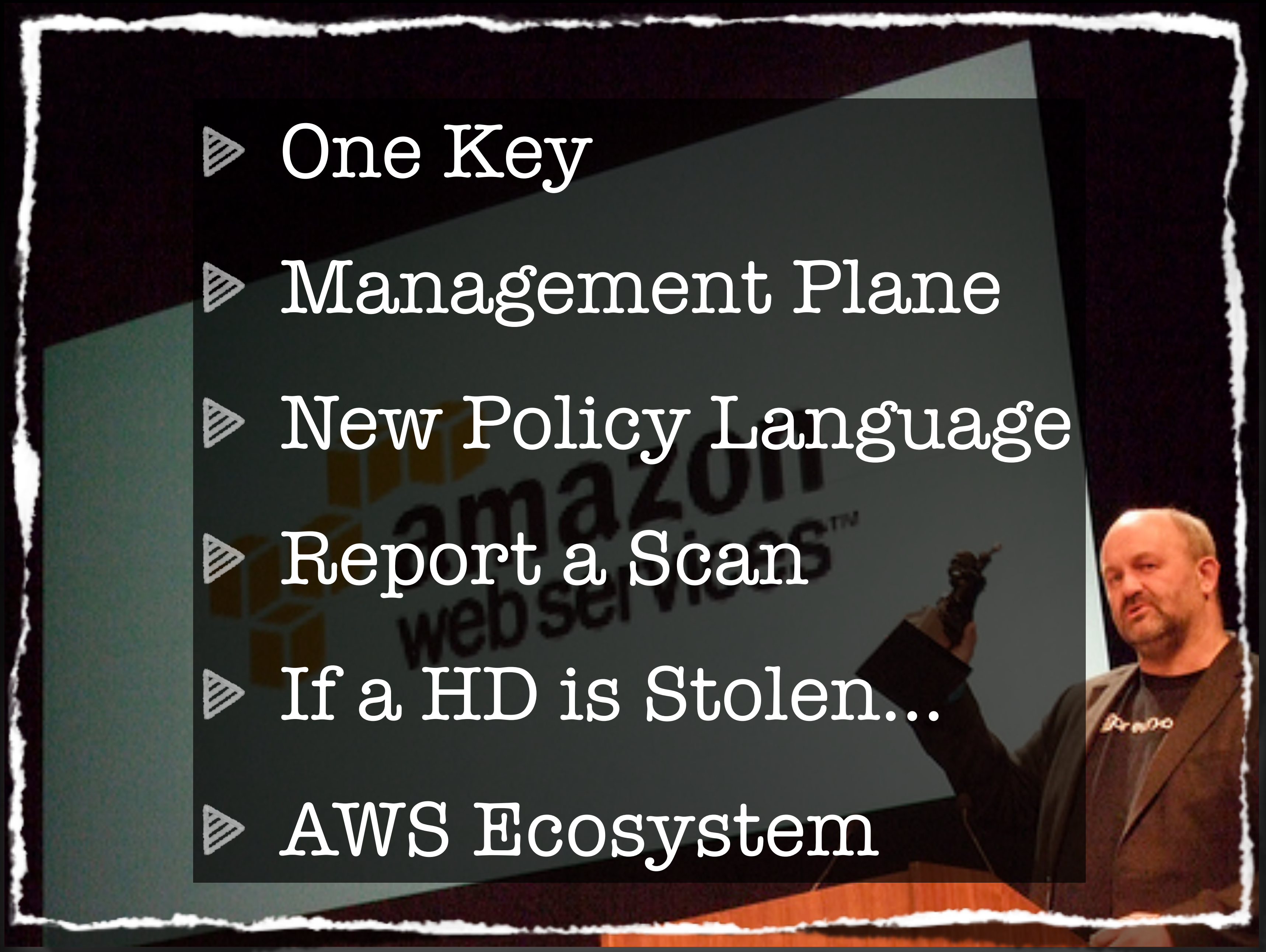
Platform as a Service

Infrastruture as a Service



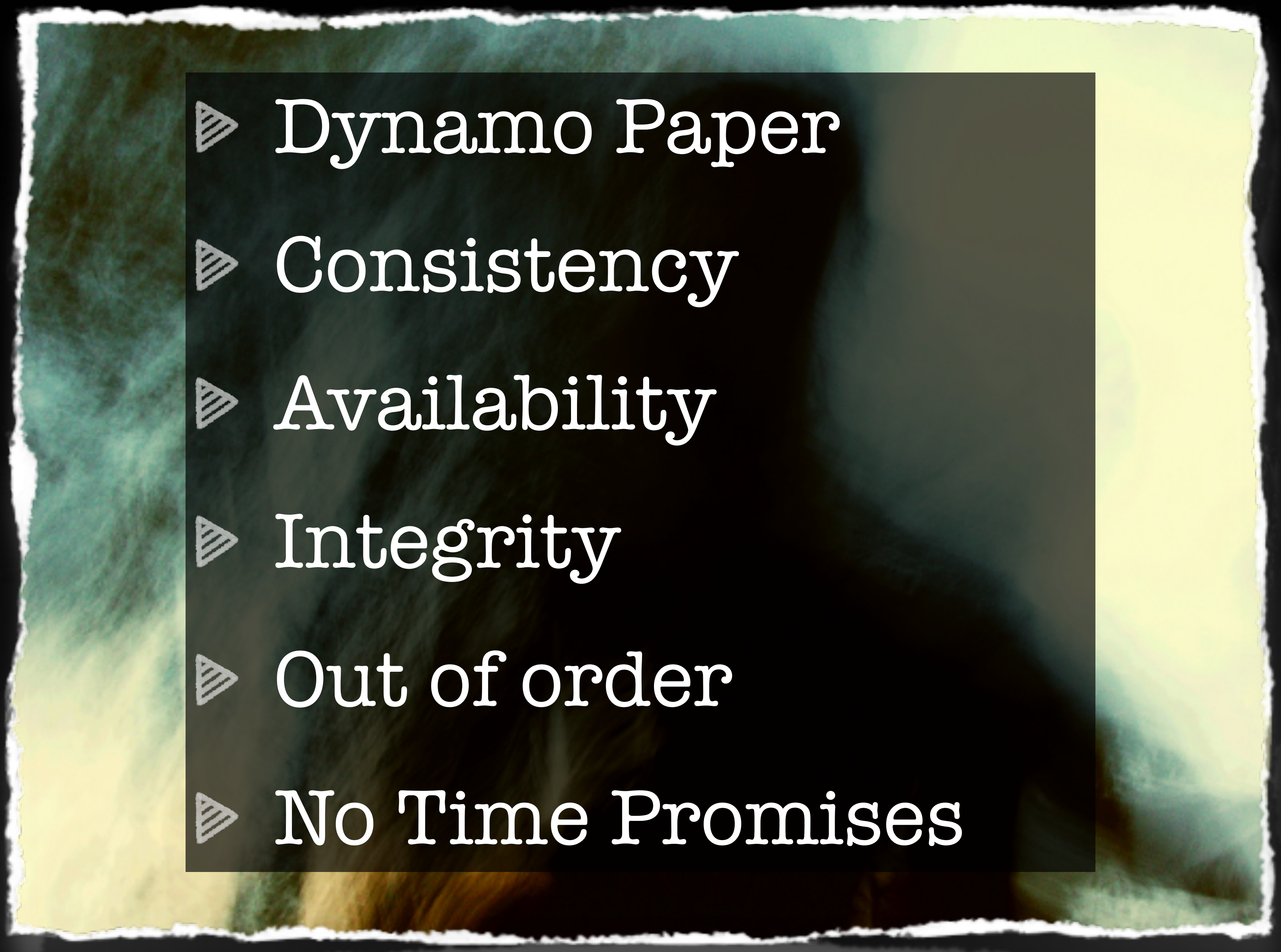
- Public IaaS Pioneer
- EC2, S3, SQS etc
- “You secure”
- Security Whitepaper
- Evangelism
- Data Cleansing

Amazon Web Services



- One Key
- Management Plane
- New Policy Language
- Report a Scan
- If a HD is Stolen...
- AWS Ecosystem

Amazon Web Services

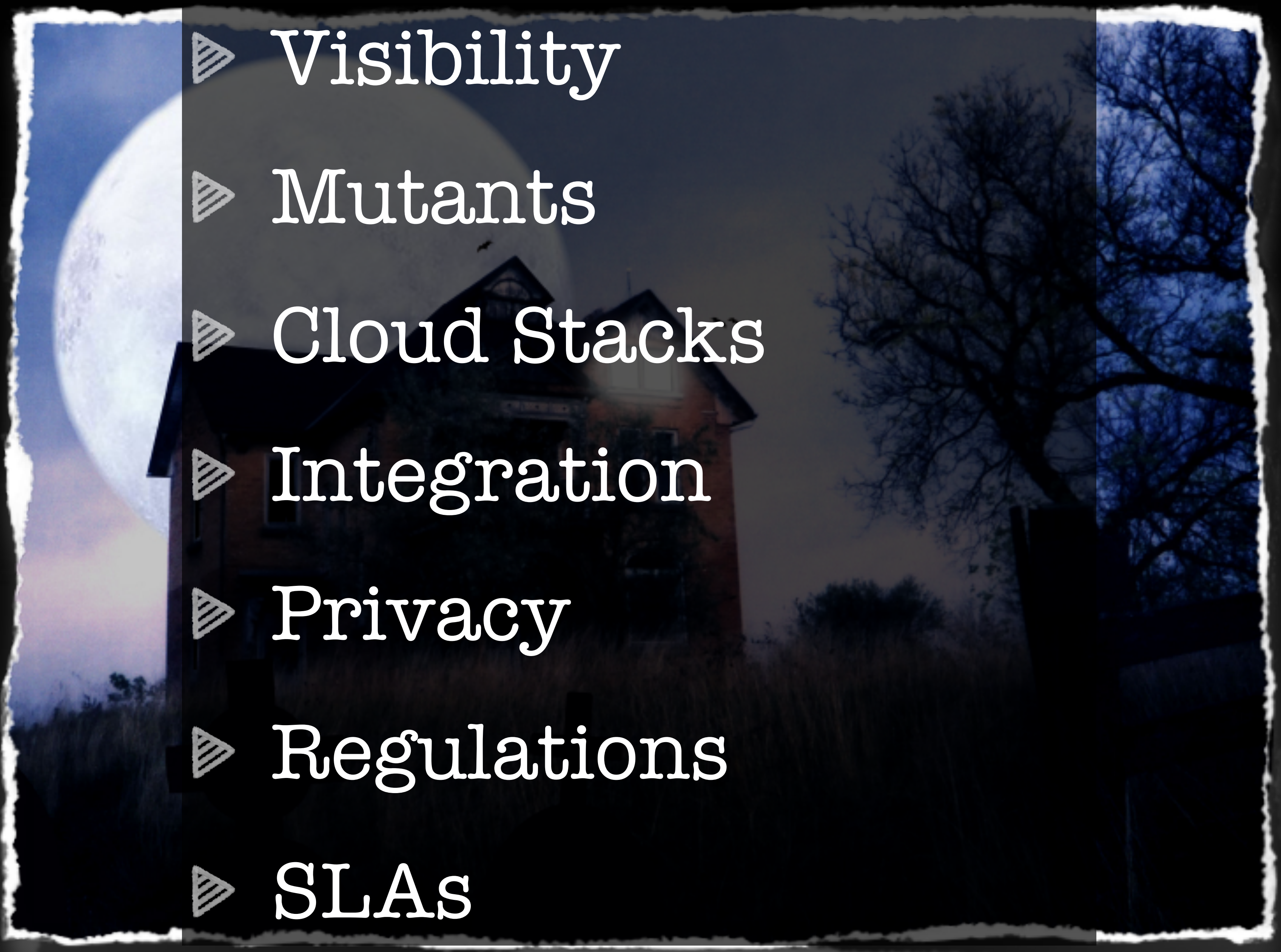


- Dynamo Paper
- Consistency
- Availability
- Integrity
- Out of order
- No Time Promises

Eventually Consistent

- AWS “Dev friendly”
- Dev Testimonials
- AMZN PMTS
- 866-216-1072
- AWS API endpoints
- POST/PUT/DELETE

Developers with Credit Cards



- Visibility
- Mutants
- Cloud Stacks
- Integration
- Privacy
- Regulations
- SLAs

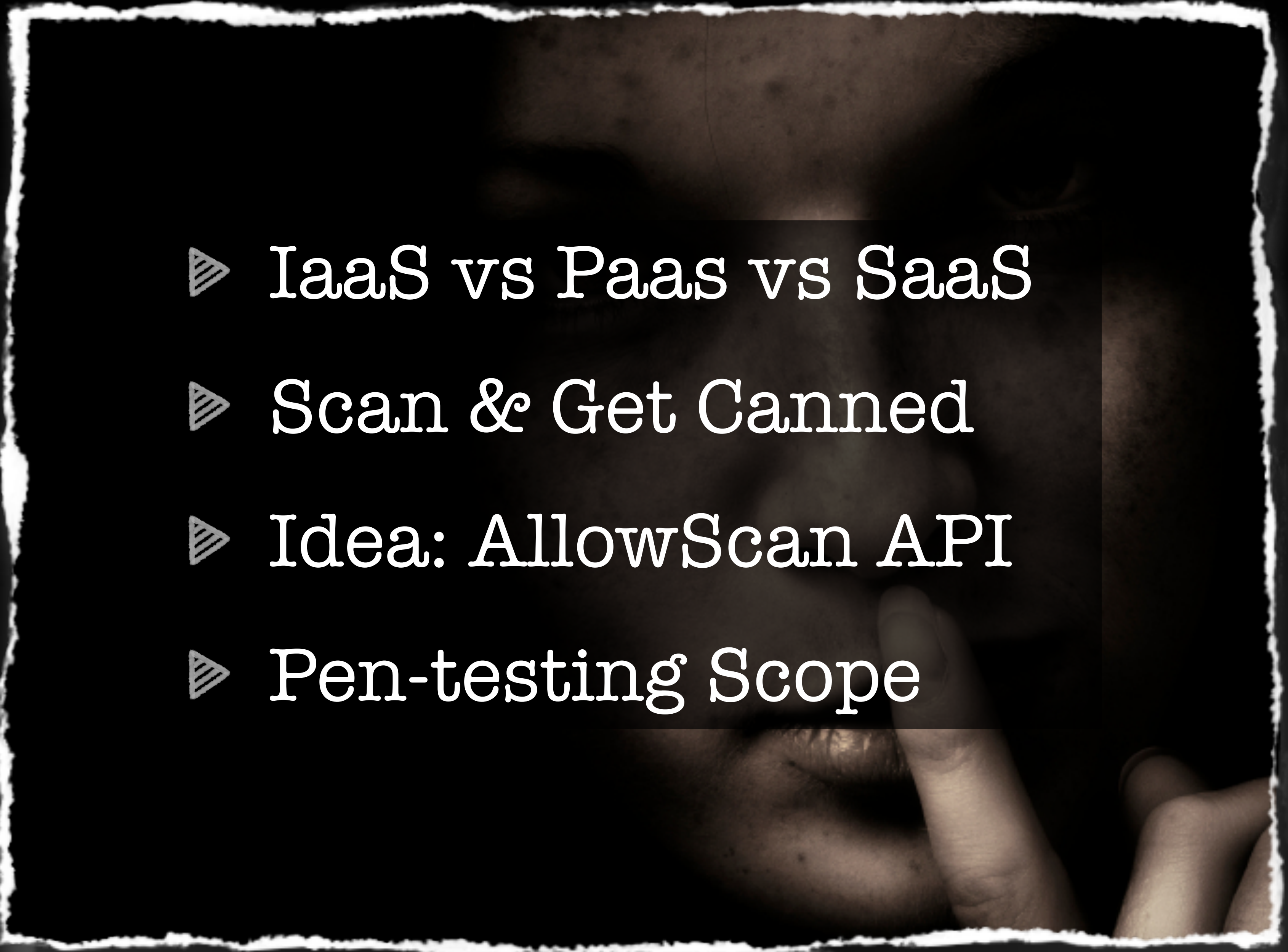
Haunted House of the Cloud

The Visibility Ghost Ship

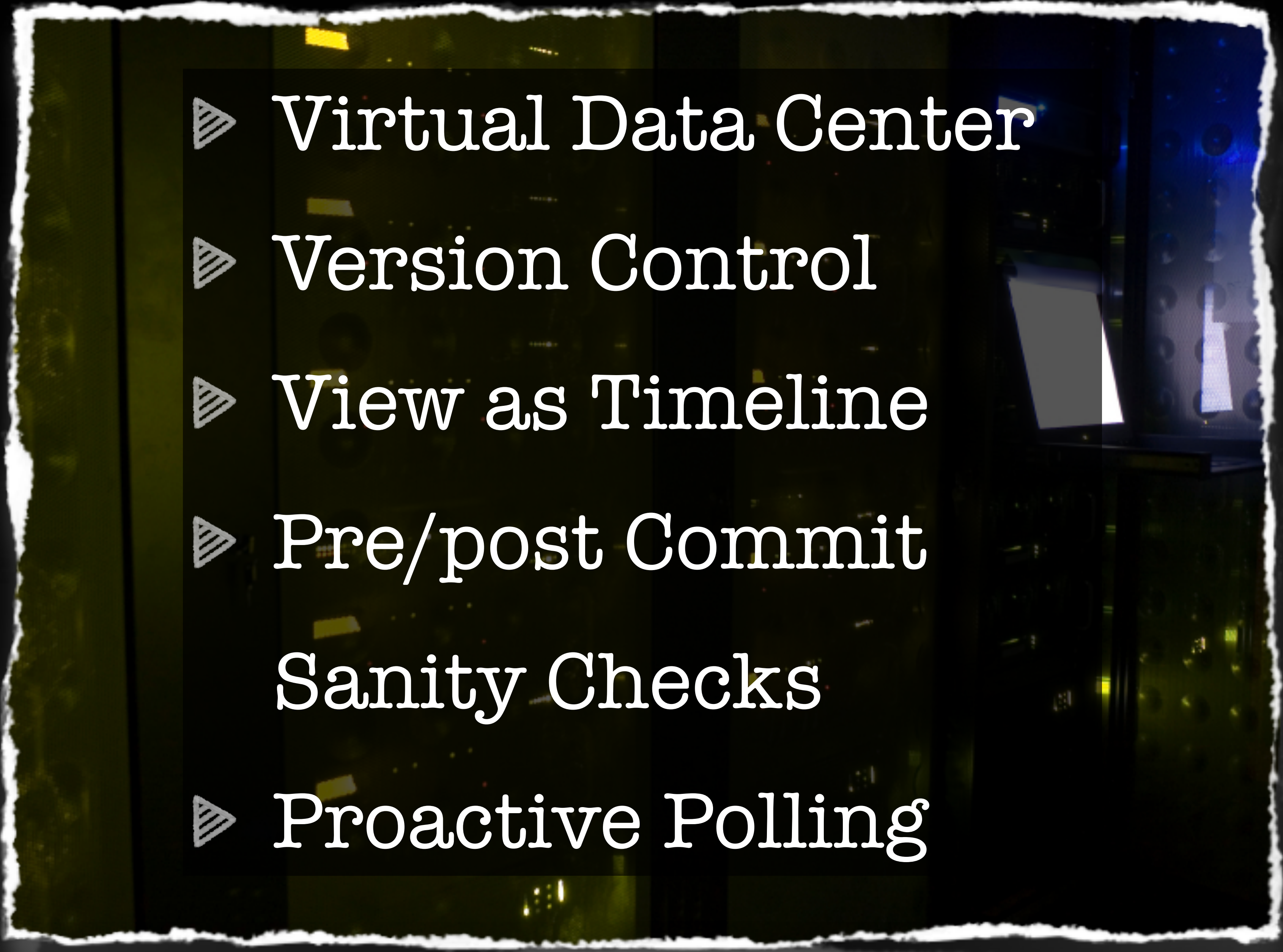
- When Controls Fail
- Lingua Franca: API
- Manage SSL
- EC2 vs NSM
- Immature logging
- DLP

The Visibility Ghostship

Assurance

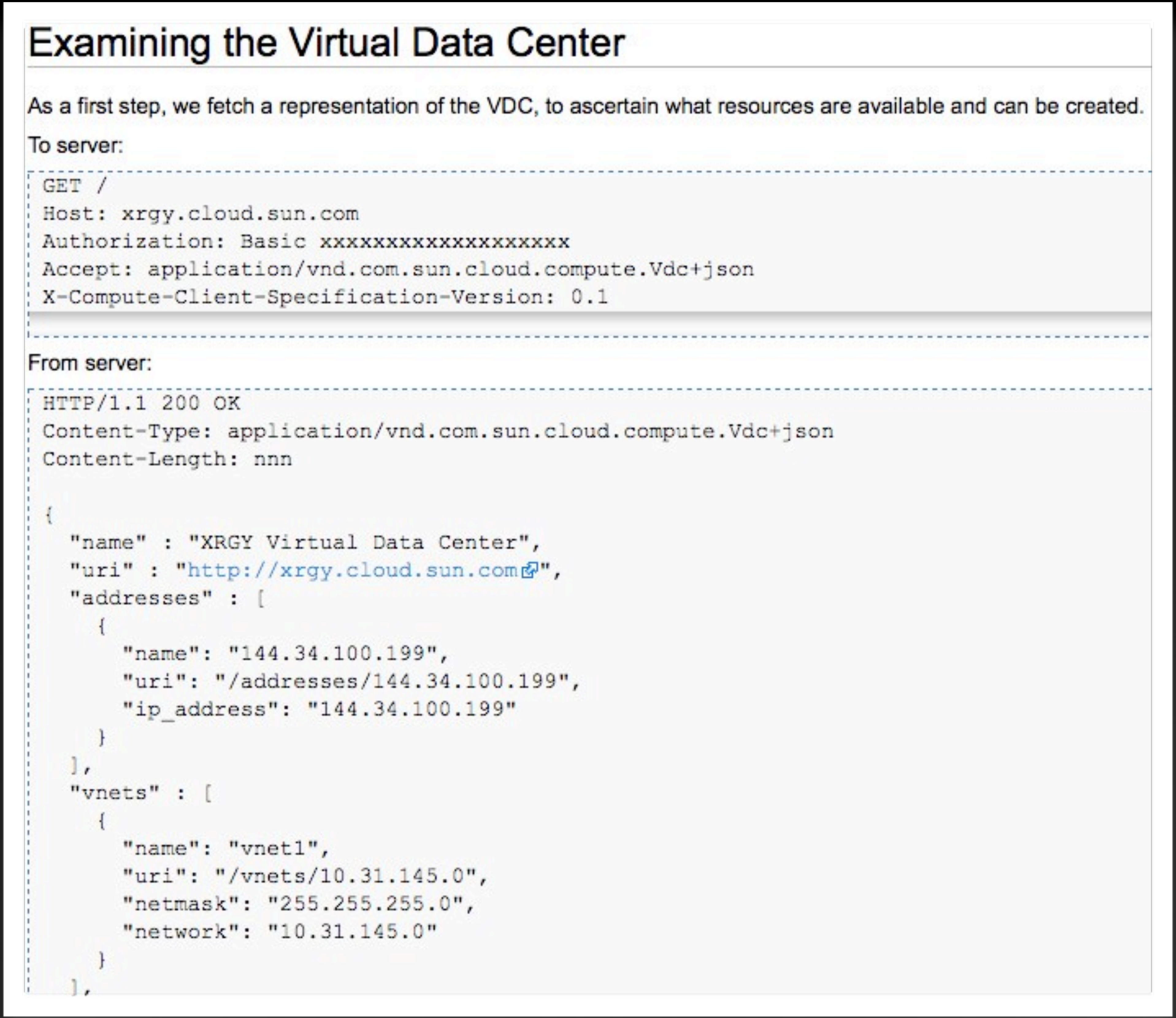


- IaaS vs Paas vs SaaS
- Scan & Get Canned
- Idea: AllowScan API
- Pen-testing Scope



- Virtual Data Center
- Version Control
- View as Timeline
- Pre/post Commit Sanity Checks
- Proactive Polling

Data Center Tripwire



Examining the Virtual Data Center

As a first step, we fetch a representation of the VDC, to ascertain what resources are available and can be created.

To server:

```
GET /
Host: xrgy.cloud.sun.com
Authorization: Basic xxxxxxxxxxxxxxxxxxx
Accept: application/vnd.com.sun.cloud.compute.Vdc+json
X-Compute-Client-Specification-Version: 0.1
```

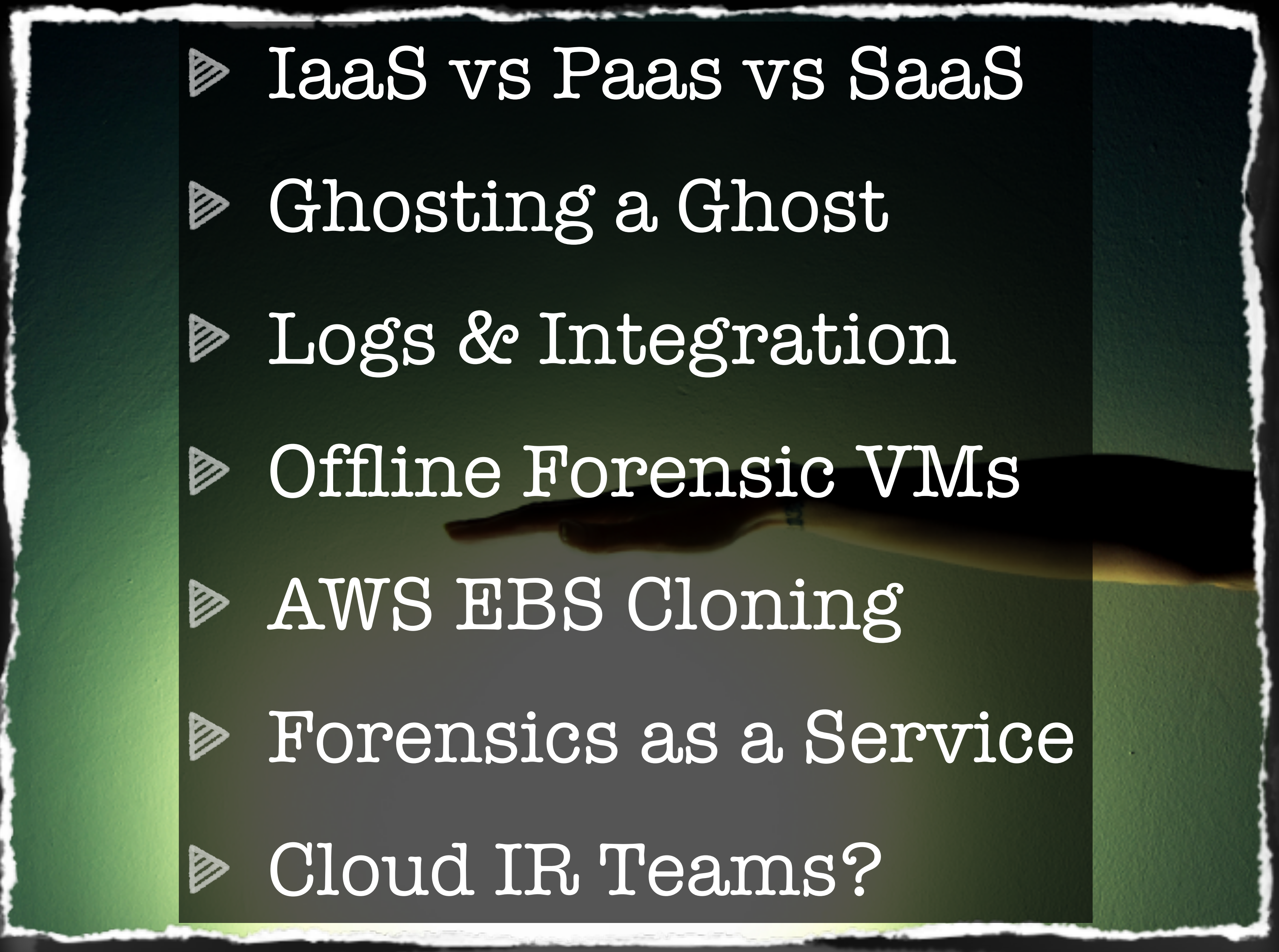
From server:

```
HTTP/1.1 200 OK
Content-Type: application/vnd.com.sun.cloud.compute.Vdc+json
Content-Length: nnn

{
  "name" : "XRGY Virtual Data Center",
  "uri" : "http://xrgy.cloud.sun.com",
  "addresses" : [
    {
      "name": "144.34.100.199",
      "uri": "/addresses/144.34.100.199",
      "ip_address": "144.34.100.199"
    }
  ],
  "vnets" : [
    {
      "name": "vnet1",
      "uri": "/vnets/10.31.145.0",
      "netmask": "255.255.255.0",
      "network": "10.31.145.0"
    }
  ],
```

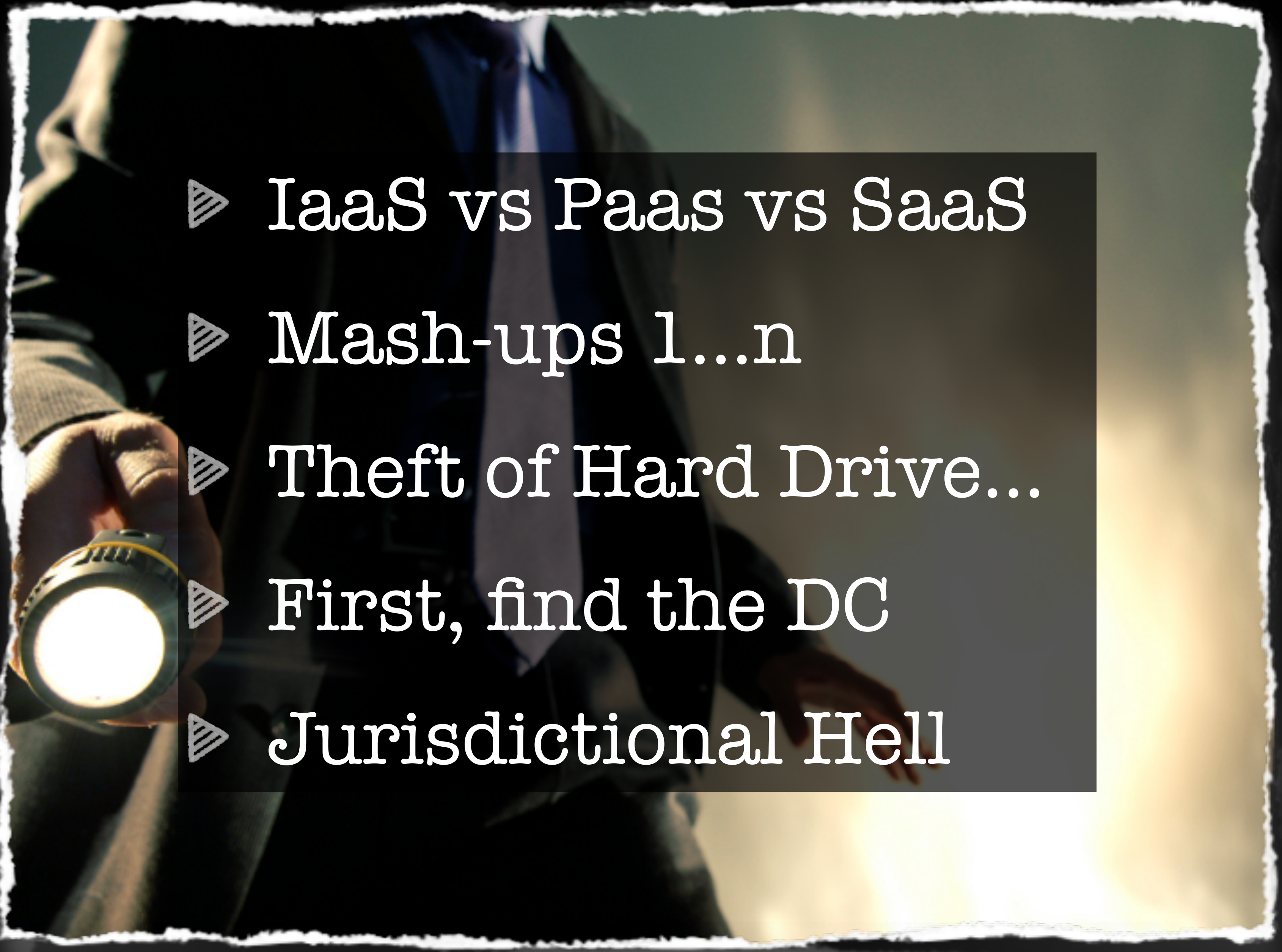
- Call Premium Support
- Cloud Clamour
- No Business Context

Incident Response



- IaaS vs Paas vs SaaS
- Ghosting a Ghost
- Logs & Integration
- Offline Forensic VMs
- AWS EBS Cloning
- Forensics as a Service
- Cloud IR Teams?

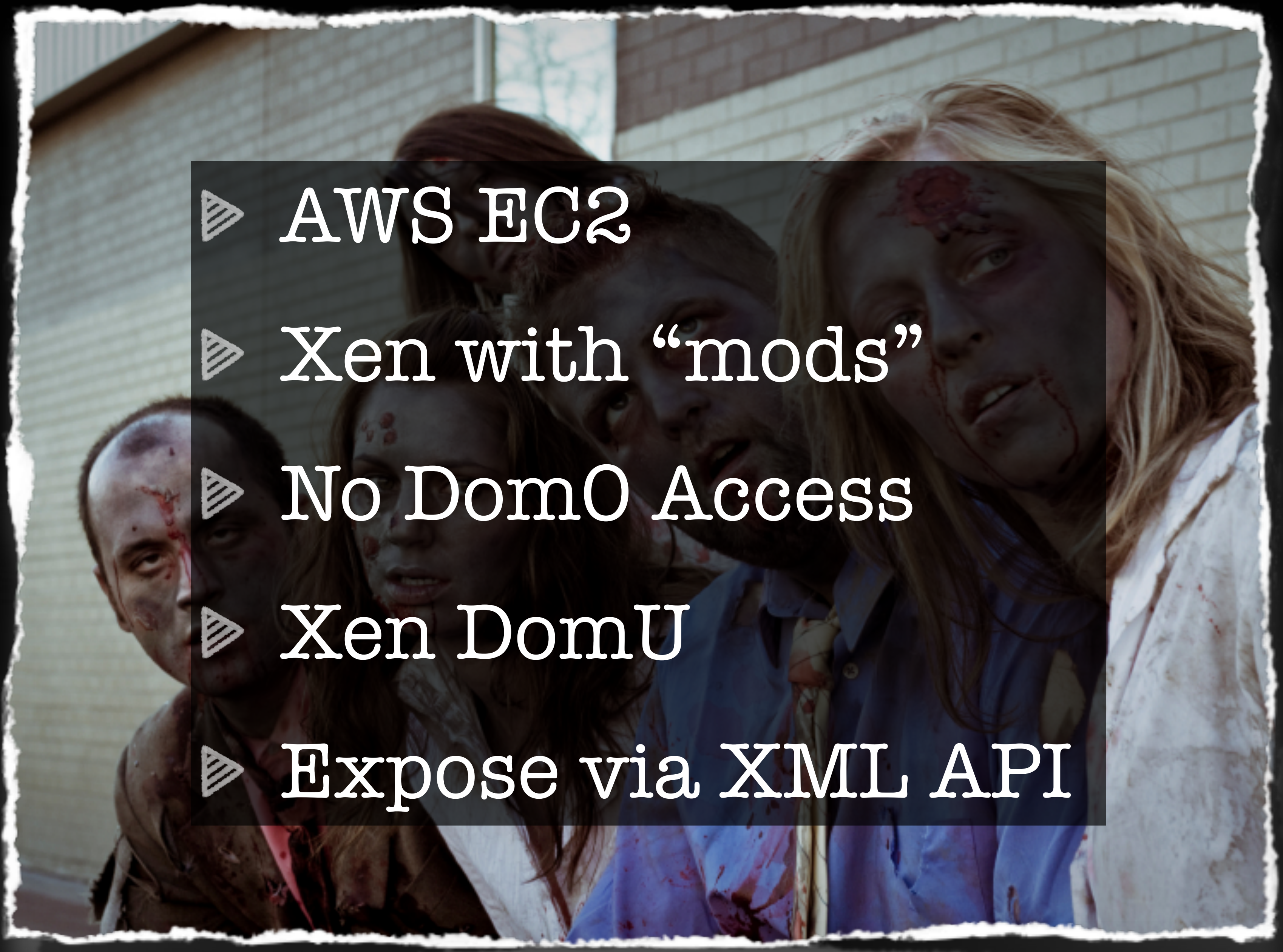
Forensics



- IaaS vs Paas vs SaaS
- Mash-ups 1...n
- Theft of Hard Drive...
- First, find the DC
- Jurisdictional Hell

Investigations

The March of the Mutated Hypervisor



- AWS EC2
- Xen with “mods”
- No Dom0 Access
- Xen DomU
- Expose via XML API

The March of the Mutated Hypervisor

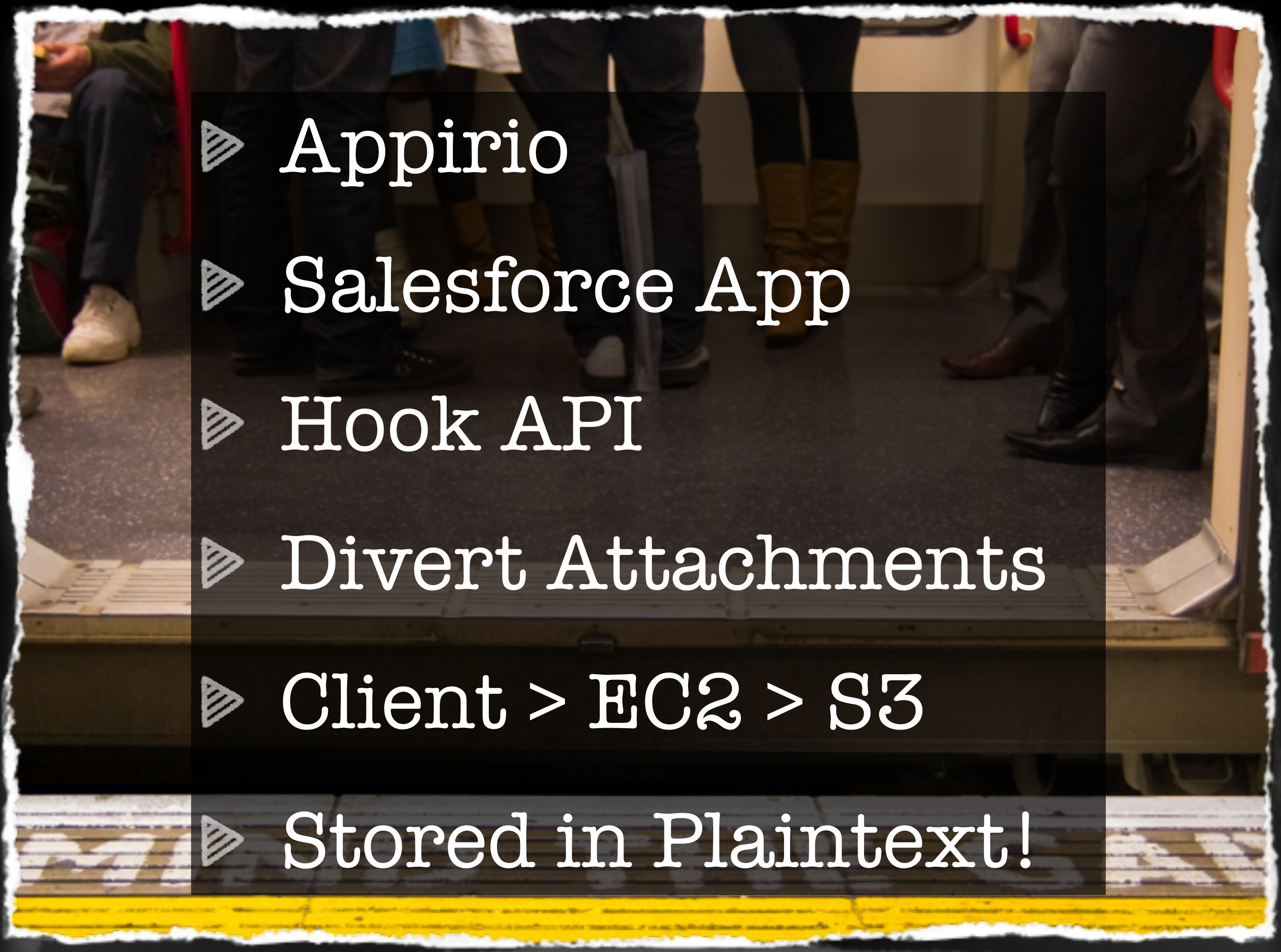
- BIOS Functionality++
- Research++
- Cache Snooping
- Hypervisor Attack
- Persistent Rootkits

The Vampire BIOS

Ghost in the Stacks

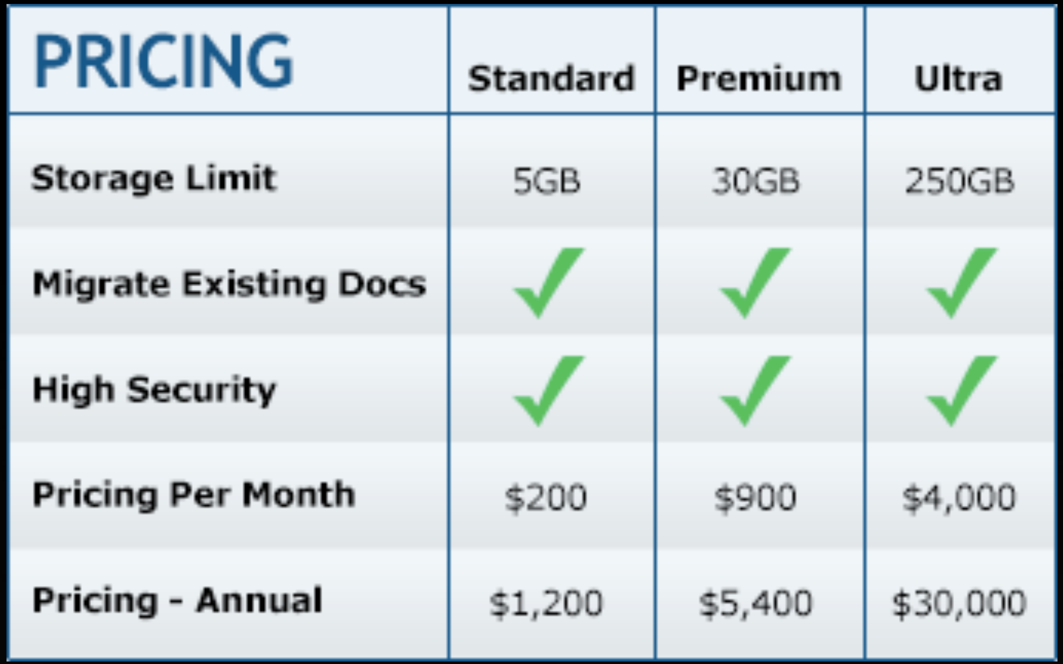
Cloud Stacks/Layers

- Dependent Services
- Consume & Provide
- Trust by Inheritence
- Mind the Gap
- Pass the Buck

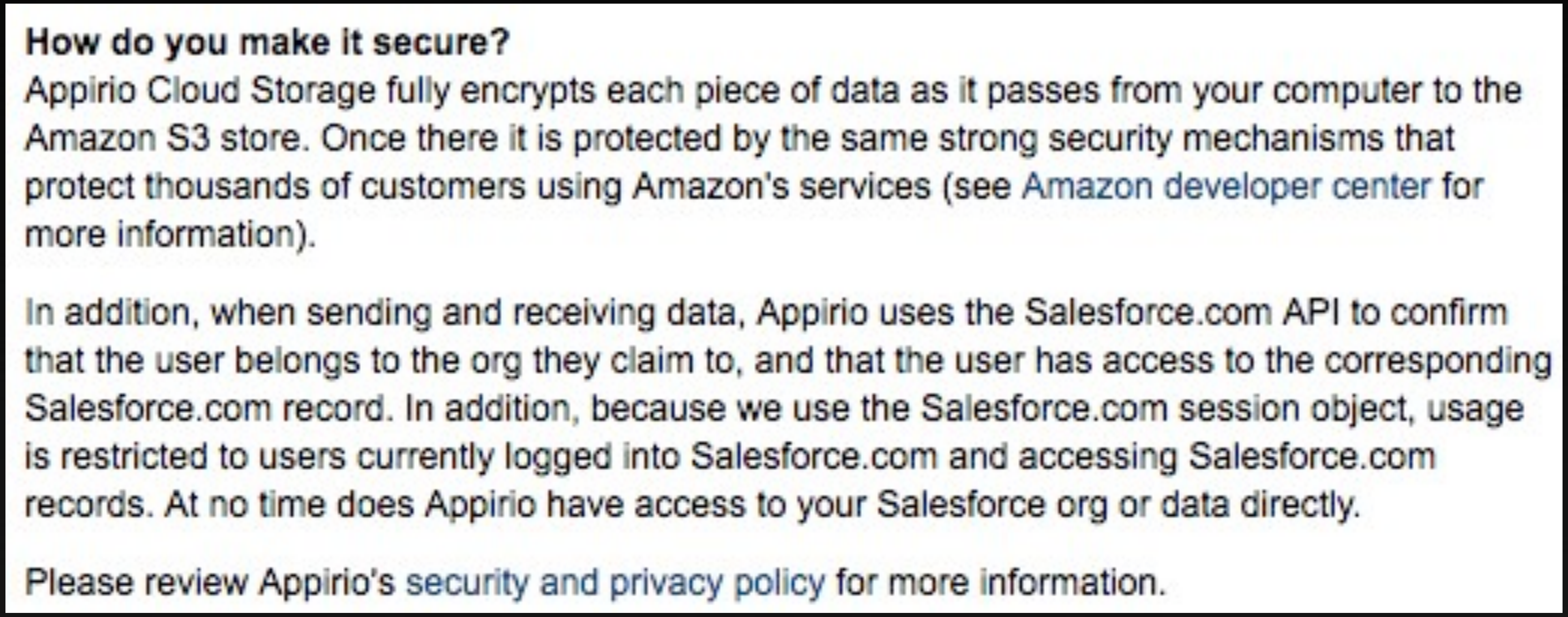


- Appirio
- Salesforce App
- Hook API
- Divert Attachments
- Client > EC2 > S3
- Stored in Plaintext!

Example



PRICING	Standard	Premium	Ultra
Storage Limit	5GB	30GB	250GB
Migrate Existing Docs	✓	✓	✓
High Security	✓	✓	✓
Pricing Per Month	$200	$900	$4,000
Pricing - Annual	$1,200	$5,400	$30,000



How do you make it secure?
Appirio Cloud Storage fully encrypts each piece of data as it passes from your computer to the Amazon S3 store. Once there it is protected by the same strong security mechanisms that protect thousands of customers using Amazon's services (see Amazon developer center for more information).

In addition, when sending and receiving data, Appirio uses the Salesforce.com API to confirm that the user belongs to the org they claim to, and that the user has access to the corresponding Salesforce.com record. In addition, because we use the Salesforce.com session object, usage is restricted to users currently logged into Salesforce.com and accessing Salesforce.com records. At no time does Appirio have access to your Salesforce org or data directly.

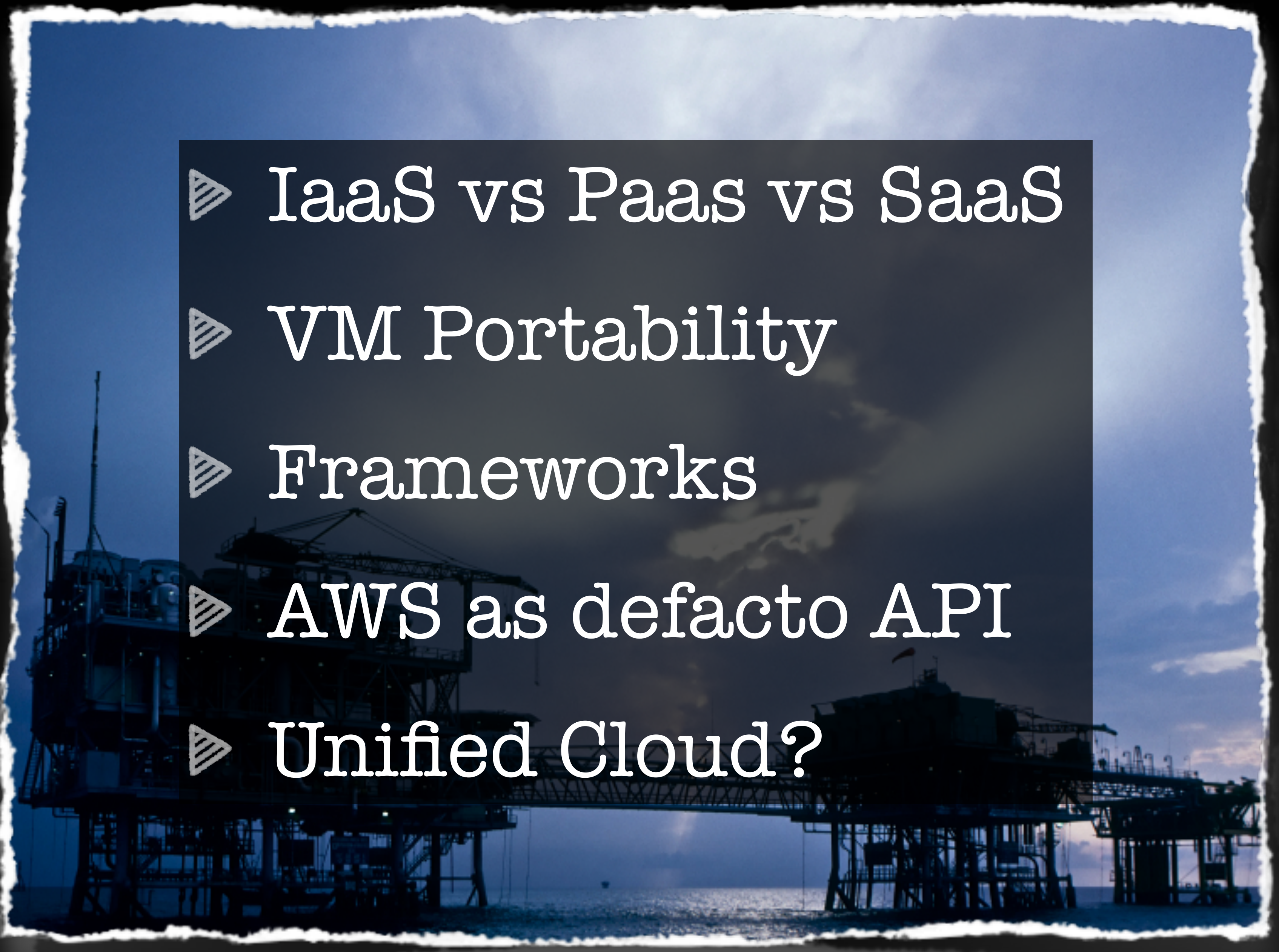
Please review Appirio's security and privacy policy for more information.

Net vs Storage Crypto

Enterprise Integration Road to Hell

- Identity is > People
- Federated Auth
- Visibility
- DLP
- Metrics
- Billing

Enterprise Integration



- IaaS vs Paas vs SaaS
- VM Portability
- Frameworks
- AWS as defacto API
- Unified Cloud?

Interoperability

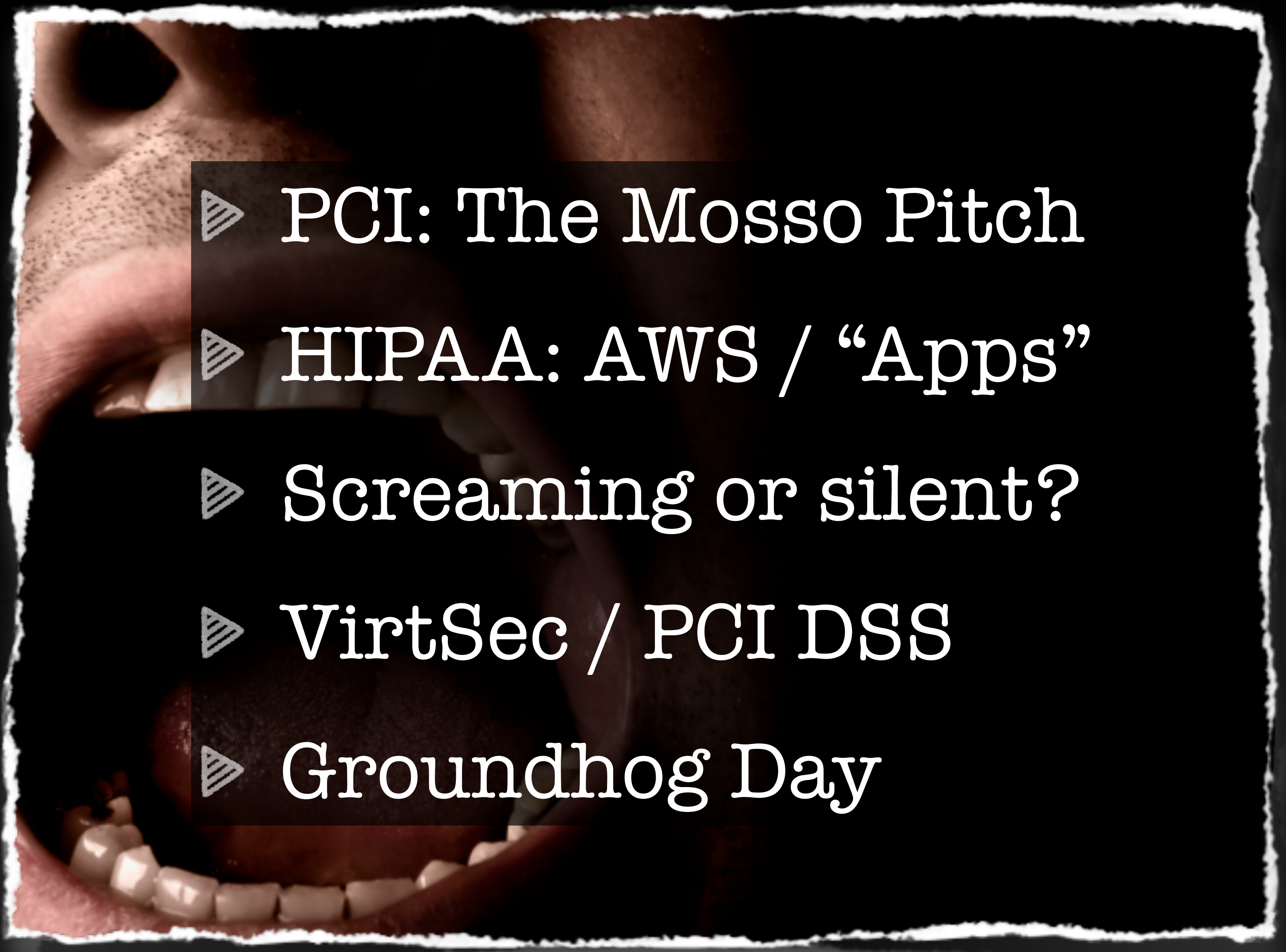
Cloud Lock-in

The Green Latern of Privacy

- EPIC Compliant
- Misstating Security
- Snafus & Vulns
- Lack of Crypto
- Bar of chocolate?
- $SOCIALNETWORKS

The Green Lantern of Privacy

The Screaming Regulator



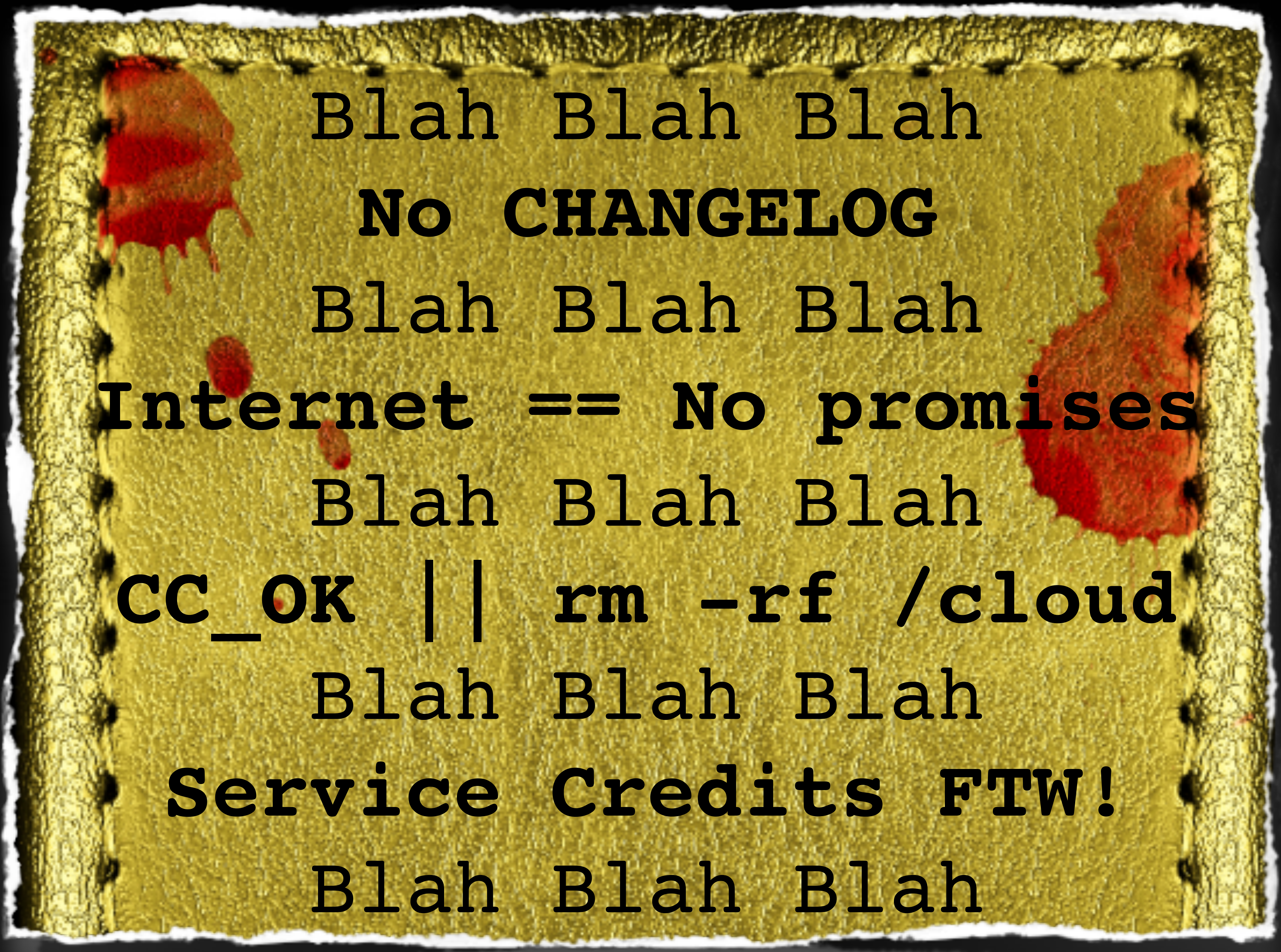
- PCI: The Mosso Pitch
- HIPAA: AWS / “Apps”
- Screaming or silent?
- VirtSec / PCI DSS
- Groundhog Day

The Screaming Regulator

- Jurisdiction
- IP rights
- Content ownership
- Contract Law Wins
- Licensing
- Raid 8

Legal Concerns

The Curse of the Bloodstained SLA



Blah Blah Blah

No CHANGELOG

Blah Blah Blah

Internet == No promises

Blah Blah Blah

CC_OK || rm -rf /cloud

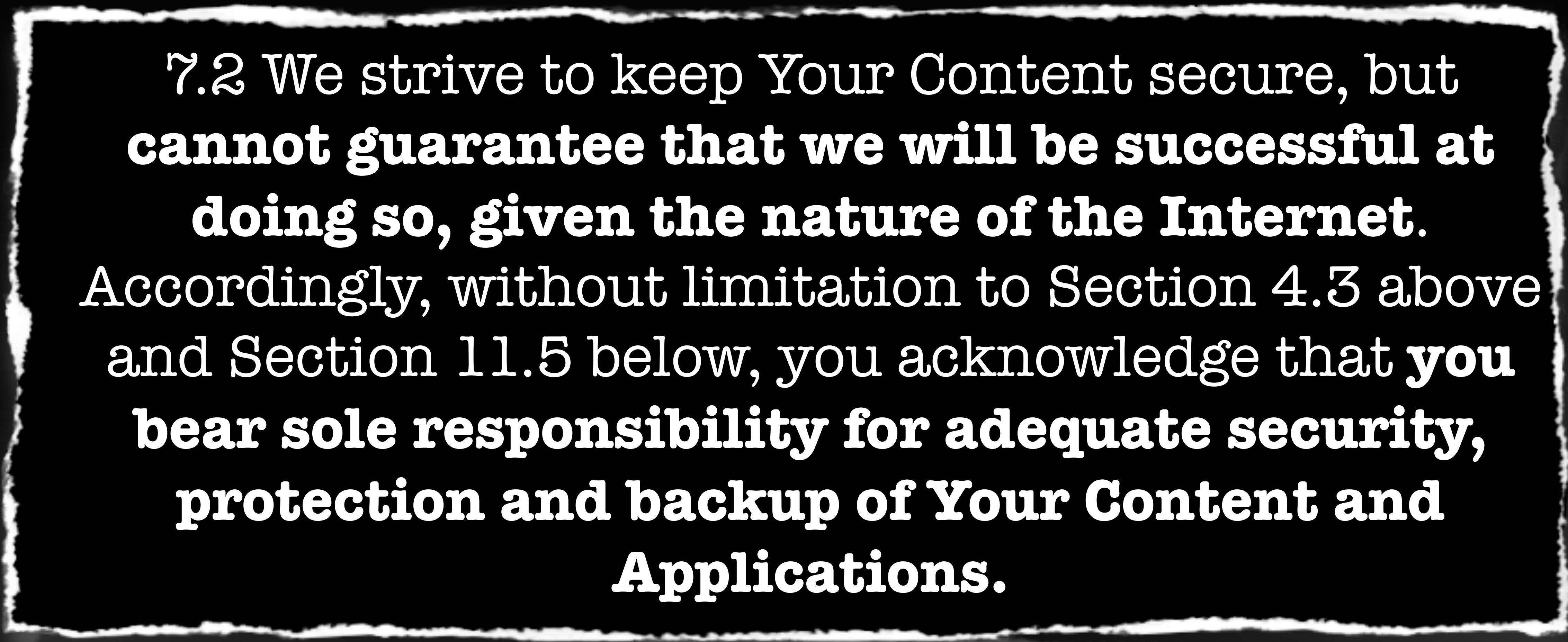
Blah Blah Blah

Service Credits FTW!

Blah Blah Blah

Blood Stained SLA

AWS Security Pledge



7.2 We strive to keep Your Content secure, but **cannot guarantee that we will be successful at doing so, given the nature of the Internet**. Accordingly, without limitation to Section 4.3 above and Section 11.5 below, you acknowledge that **you bear sole responsibility for adequate security, protection and backup of Your Content and Applications.**

AWS Security Advice

7.2. ...We **strongly encourage** you, where available and appropriate, to (a) **use encryption technology to protect Your Content from unauthorized access**, (b) **routinely archive** Your Content, and (c) keep your Applications or any software that you use or run with our Services current with the latest security patches or updates.

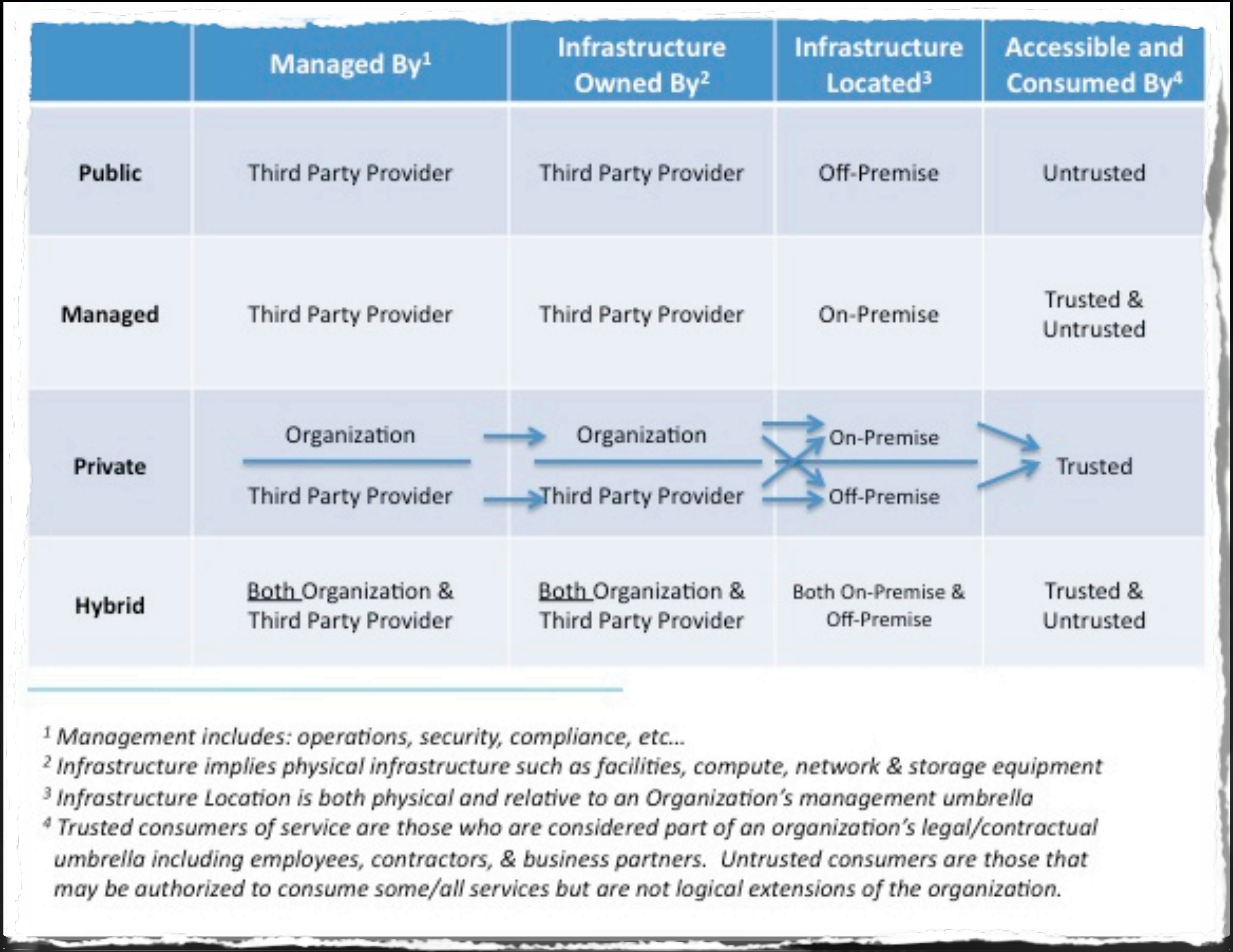
Not even Service Credits? ;-)

7.2. ...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.

Cloud Nirvana: The Rise of the Enterprise Private Cloud

- Maximum Control
- Interoperability
- Cloudbursting
- Extend Off-site
- VMware / CISCO
- Eucalyptus (OSS)

Private Clouds



	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
Managed	Third Party Provider	Third Party Provider	On-Premise	Trusted & 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*

[4] *Trusted consumers of service are those who are considered part of an organization's legal/contractual 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.*

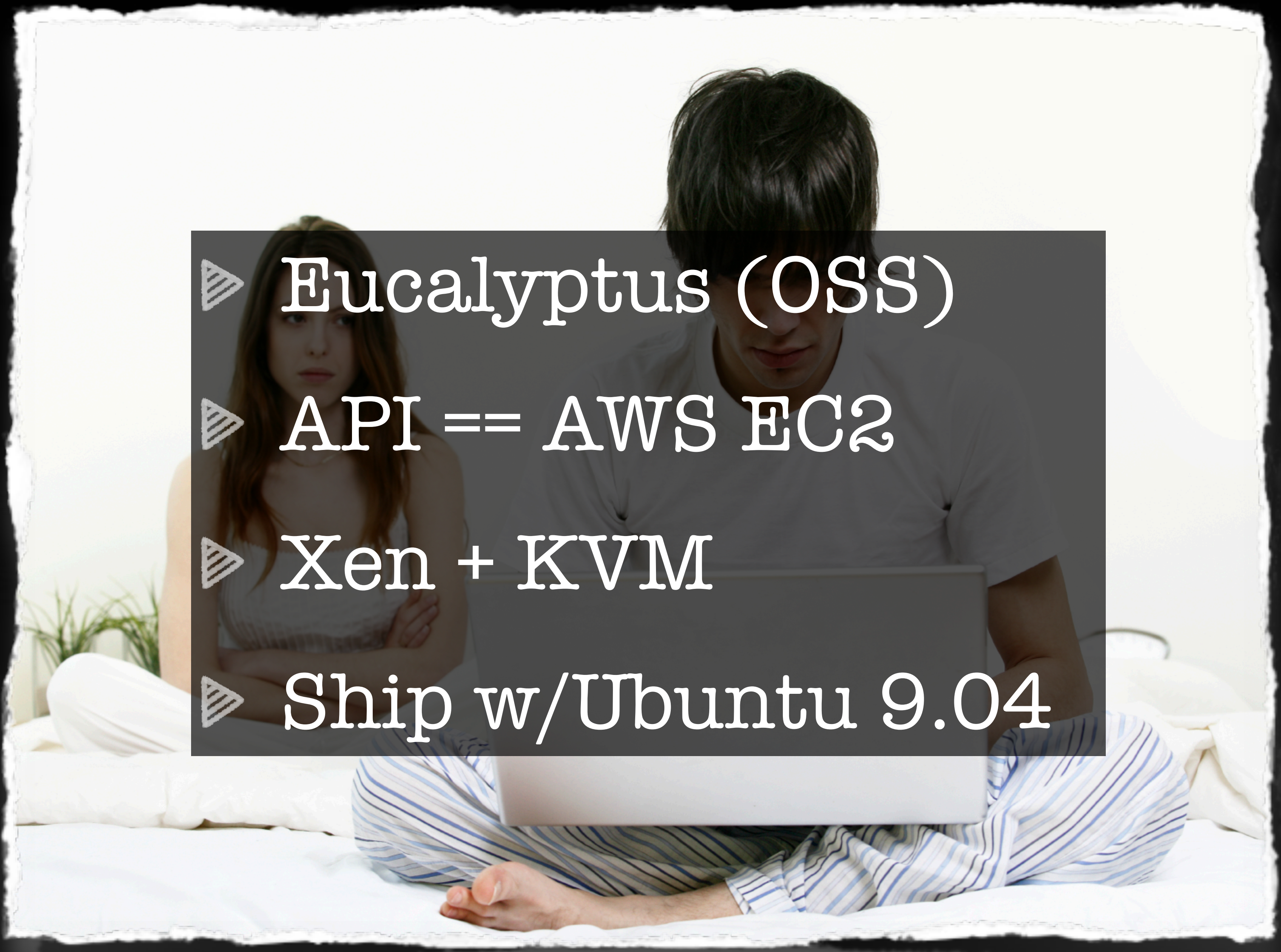
Source: Chris Hoff

- Infrastructure 1.0
- Firewall Mentality
- Controls vs Data
- Investments vs Risk
- DL Time Bombs
- Visibility & IR

Enterprise Skeletons

- 346 Legacy Apps
- Audit Reports
- 3rd Party Monsters
- Aging Policies
- Controls <> Assets
- Inner Control Freak
- Good Old Days

Call from the Grave



- Eucalyptus (OSS)
- API == AWS EC2
- Xen + KVM
- Ship w/Ubuntu 9.04

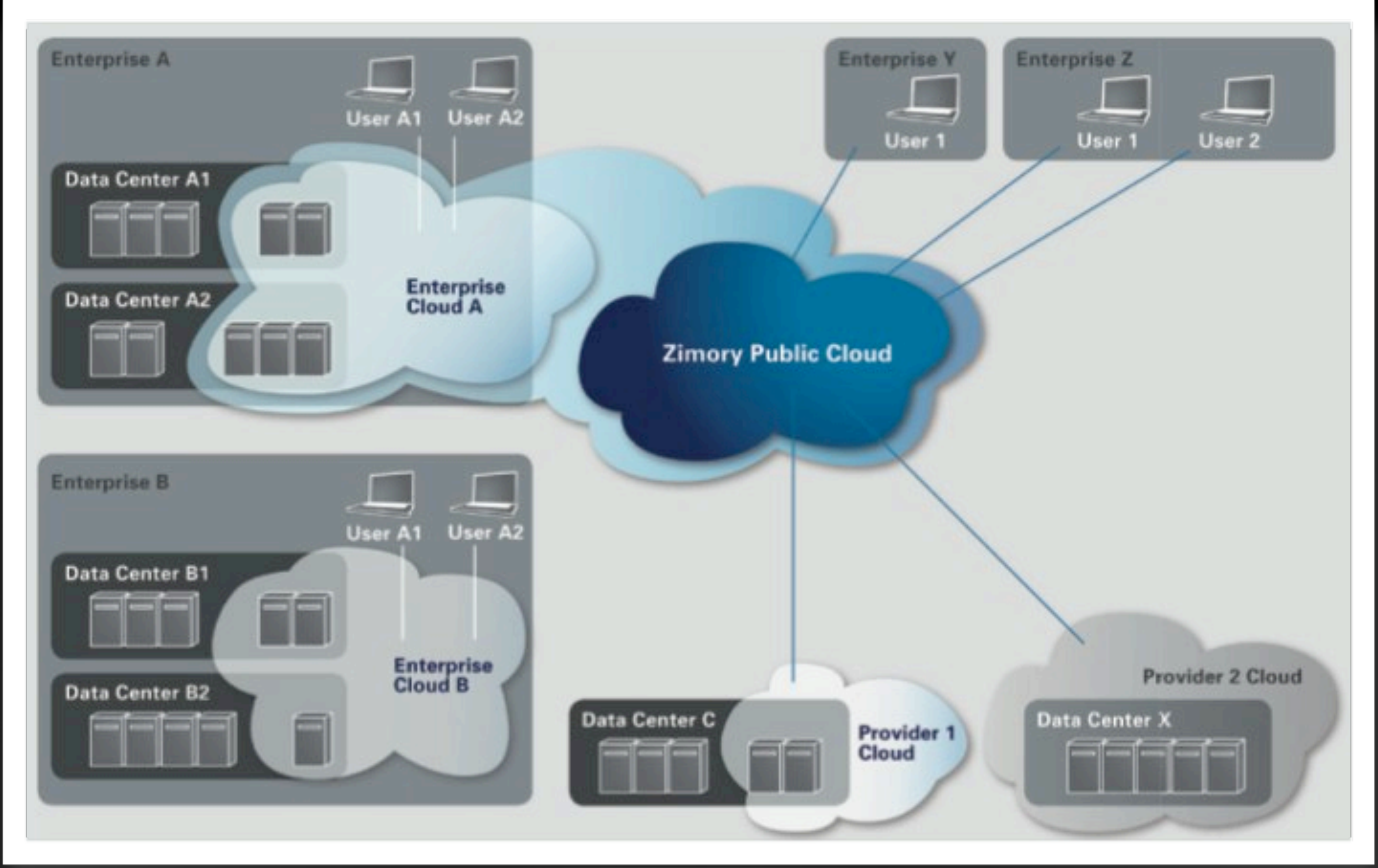
Open Source Private Cloud

- Centralised Controls
- Password Cracking
- Forensic Readiness
- Never Ending Logs
- Security Builds
- Security Testing

Embrace the Cloud

- Cloud Aggregator
- “Internet Trading Platform"
- Public/Private
- Handle Billing

Cloud Brokers



Example: Zimory

Pick Your Poison

- Gold: A gold SLA cloud delivers the strongest quality standards. This includes availability and security standards. The providers offering these resources are **compliant with all relevant security certifications**.

- Silver: A silver SLA offers **high availability and security standards**. The providers are known brands.

- Bronze: A bronze SLA delivers the **usual quality** and availability standards of hosting providers. It does not contain certifications and additional security offerings.

Cloud Spirits

General

John Willis: IT ESM and Cloud (Droplets)
Kevin L. Jackson: Cloud Musing (Federal)
James Urquhart (CISCO): Wisdom of Clouds
Werner Vogels (AWS CTO): All Things Distributed

Google Groups

Cloud Computing

Security

Christofer Hoff: rationalsurvivability.com
Craig Balding (aka Me): **cloudsecurity.org**

- Cloud Security Alliance
- ENISA Cloud Security Working Group

Cloud Security Initiatives

Cloud Security Alliance

- Non-profit organization
- Promote practices to provide security assurance
- Comprised of many subject matter experts from a wide variety disciplines
- Official launch next week @ RSA
- Join? Linkedin Group “Cloud Security Alliance” open to all

ENISA Cloud Computing Risk Assessment

- European Policymakers responsible for funding Cloud risk mitigation research, policy, economic incentives, legislative measures, awareness-raising initiatives
- Business leaders to evaluate Cloud risks of and possible mitigation strategies.
- Individuals/citizens to evaluate cost/benefit of consumer Cloud services.

Futures

- Hosting => Cloud
- Cloud Platform Wars
- Cloud Pwnage
- Trust Indicators
- Vertical Clouds
- Data Centric Security?
- Social Engineering++

Ghost Alley / Amsterdam

Thanks

Q&A

Craig Balding cloudsecurity.org

CSA: Domains

- Information lifecycle management
- Governance and Enterprise Risk Management
- Compliance & Audit
- General Legal
- eDiscovery
- Encryption and Key Mgt
- Identity and Access Mgt
- Storage
- Virtualization
- Application Security
- Portability & InteroperabilityData Center Operations Management
- Incident Response, Notification, Remediation
- "Traditional" Security impact (business continuity, disaster recovery, physical security)
- Architectural Framework