CLOUD COMPUTING DEMYSTIFIED

Definitions you've been pretending to understand

JACK DANIEL, CCSK, CISSP, MVP ENTERPRISE SECURITY

Definitions

- **Words have meaning, professionals need to understand them.**
- **We need to understand that the public, end-users, and the media will get things wrong, and not worry about that.**
  - Not much, anyway.
- **There isn't just one cloud, so saying "the cloud" is wrong. (Yes, I know we've already lost this battle).**

What do we mean by "Cloud Security"?

- **Securing data in a cloud environment?**
  - We will talk about this.
- **Securing a cloud environment?**
  - That's out of scope for this webinar. And for most people.
- **Using a cloud service for security?**
  - You are already doing this for anti-virus, web and email security.
- **We're still struggling with similar confusion over "virtual security".**


HYBRID
POOL
COMMUNITY
DEMAND
RIVAL
PUBLIC
ELASTIC
PAAS
MEASURED
CLOUD

Who Defines "Cloud Computing"?

A lot of folks claim to, but I'll stick with:

NIST, National Institute of Standards and Technology

- Their "Definition of cloud computing and related terminology" is good and concise. It is cited frequently in this deck

CSA, Cloud Security Alliance

NIST Definition Of Cloud Computing

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential *characteristics*, three *service models*, and four *deployment models*.

NIST Definition Of Cloud Computing

…convenient, on-demand network access to a shared pool of configurable computing resources…

NIST Definition Of Cloud Computing

…and is composed of:

five essential *characteristics*

three *service models*

and four *deployment models*.

Alternate Definition Of Cloud Computing

Anything on the Internet.


011010
10011011
1011100
101011
101100101
10110
CLOUD
COMPUTING
100110
010101011
010
10100111
011010101
010 10
10110110
1001

Service Models

Software as a Service (SaaS)

Platform as a Service (PaaS)

Infrastructure as a Service (IaaS)

Software as a Service (SaaS)

…use the provider's applications running on a cloud infrastructure…

Isn’t This Just ASP?

It is an evolution of Application Service Provider offerings, but SaaS is different.
How many ASPs offered:

Near instant provisioning?

Global scalability?

Data portability?

REAL cost savings?

SaaS/PaaS/IaaS Matrix

LAYER	SaaS Control	PaaS Control	IaaS Control	
User				
Data and content				
Client Software				
Software Layer				
Platform Layer				
Infrastructure layer				
Load balancers (maybe)				
Virtualization (maybe)				
Physical Servers				

SaaS/PaaS/IaaS Matrix

LAYER	SaaS Control	PaaS Control	IaaS Control
User	Consumer		
Data and content	Consumer		
Client Software	Consumer		
Software Layer	Provider		
Platform Layer	Provider		
Infrastructure layer	Provider		
Load balancers (maybe)	Provider		
Virtualization (maybe)	Provider		
Physical Servers	Provider		

Platform As A Service (PaaS)

…deploy onto the cloud infrastructure consumer-created or acquired applications*

***created using programming languages and tools supported by the provider…**

SaaS/PaaS/IaaS Matrix

LAYER	SaaS Control	PaaS Control	IaaS Control
User	Consumer	Consumer	
Data and content	Consumer	Consumer	
Client Software	Consumer	Consumer	
Software Layer	**Provider**	**Consumer**	
Platform Layer	Provider	Provider	
Infrastructure layer	Provider	Provider	
Load balancers (maybe)	Provider	Provider	
Virtualization (maybe)	Provider	Provider	
Physical Servers	Provider	Provider	

Infrastructure as a Service (Iaas)

…provision processing, storage, networks, and other fundamental computing resources…

Infrastructure as a Service (Iaas)

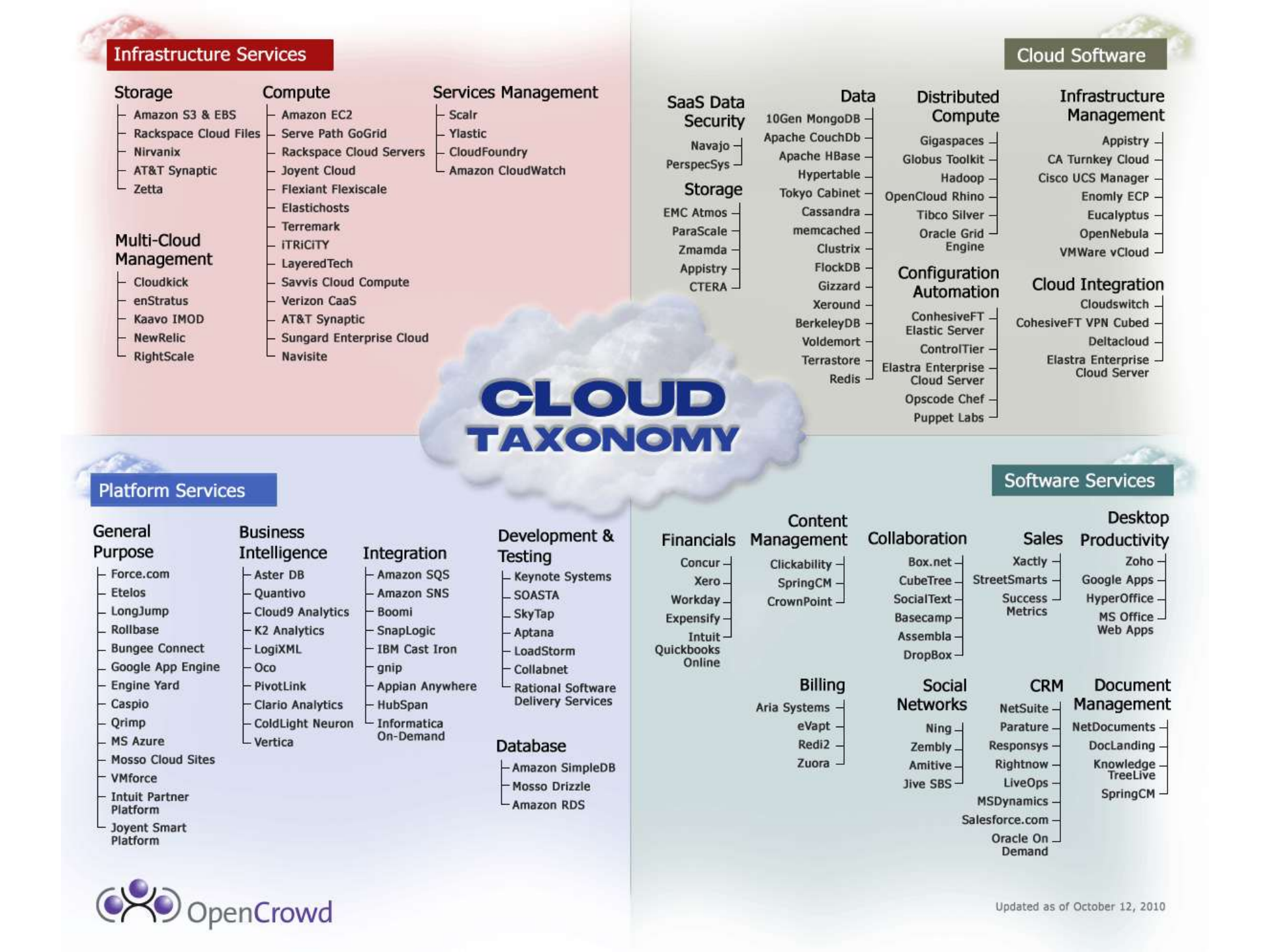
…control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

SaaS/PaaS/IaaS Matrix

LAYER	SaaS Control	PaaS Control	IaaS Control	
User	Consumer	Consumer	Consumer	
Data and content	Consumer	Consumer	Consumer	
Client Software	Consumer	Consumer	Consumer	
Software Layer	**Provider**	**Consumer**	**Consumer**	
Platform Layer	**Provider**	**Provider**	**Consumer**	
Infrastructure layer	Provider	Provider	Provider	
Load balancers (maybe)	Provider	Provider	Provider	
Virtualization (maybe)	Provider	Provider	Provider	
Physical Servers	Provider	Provider	Provider	

SaaS/PaaS/IaaS Matrix

LAYER	SaaS Control	PaaS Control	IaaS Control	Who has ultimate responsibility?
User	Consumer	Consumer	Consumer	
Data and content	Consumer	Consumer	Consumer	
Client Software	Consumer	Consumer	Consumer	
Software Layer	Provider	Consumer	Consumer	
Platform Layer	Provider	Provider	Consumer	
Infrastructure layer	Provider	Provider	Provider	
Load balancers (maybe)	Provider	Provider	Provider	
Virtualization (maybe)	Provider	Provider	Provider	
Physical Servers	Provider	Provider	Provider	


CLOUD TAXONOMY
Infrastructure Services
Storage
Amazon S3 & EBS
Rackspace Cloud Files
Nirvanix
AT&T Synaptic
Zetta
Compute
Amazon EC2
Serve Path GoGrid
Rackspace Cloud Servers
Joyent Cloud
Flexiant Flexiscale
Elastichosts
Terremark
iTRiCiTY
LayeredTech
Savvis Cloud Compute
Verizon CaaS
AT&T Synaptic
Sungard Enterprise Cloud
Navisite
Services Management
Scalr
Ylastic
CloudFoundry
Amazon CloudWatch
Multi-Cloud Management
Cloudkick
enStratus
Kaavo IMOD
NewRelic
RightScale
Cloud Software
SaaS Data Security
Navajo
PerspecSys
Storage
EMC Atmos
ParaScale
Zmamda
Appistry
CTERA
Data
10Gen MongoDB
Apache CouchDb
Apache HBase
Hypertable
Tokyo Cabinet
Cassandra
memcached
Clustrix
FlockDB
Gizzard
Xeround
BerkeleyDB
Voldemort
Terrastore
Redis
Distributed Compute
Gigaspaces
Globus Toolkit
Hadoop
OpenCloud Rhino
Tibco Silver
Oracle Grid Engine
Configuration Automation
ConhesiveFT Elastic Server
ControlTier
Elastra Enterprise Cloud Server
Opscode Chef
Puppet Labs
Infrastructure Management
Appistry
CA Turnkey Cloud
Cisco UCS Manager
Enomly ECP
Eucalyptus
OpenNebula
VMWare vCloud
Cloud Integration
Cloudswitch
CohesiveFT VPN Cubed
Deltacloud
Elastra Enterprise Cloud Server
Platform Services
General Purpose
Force.com
Etelos
LongJump
Rollbase
Bungee Connect
Google App Engine
Engine Yard
Caspio
Qrimp
MS Azure
Mosso Cloud Sites
VMforce
Intuit Partner Platform
Joyent Smart Platform
Business Intelligence
Aster DB
Quantivo
Cloud9 Analytics
K2 Analytics
LogiXML
Oco
PivotLink
Clario Analytics
ColdLight Neuron
Vertica
Integration
Amazon SQS
Amazon SNS
Boomi
SnapLogic
IBM Cast Iron
gnip
Appian Anywhere
HubSpan
Informatica On-Demand
Development & Testing
Keynote Systems
SOASTA
SkyTap
Aptana
LoadStorm
Collabnet
Rational Software Delivery Services
Database
Amazon SimpleDB
Mosso Drizzle
Amazon RDS
Software Services
Financials
Concur
Xero
Workday
Expensify
Intuit Quickbooks Online
Content Management
Clickability
SpringCM
CrownPoint
Collaboration
Box.net
CubeTree
SocialText
Basecamp
Assembla
DropBox
Sales
Xactly
StreetSmarts
Success Metrics
Desktop Productivity
Zoho
Google Apps
HyperOffice
MS Office Web Apps
Billing
Aria Systems
eVapt
Redi2
Zuora
Social Networks
Ning
Zembly
Amitive
Jive SBS
CRM
NetSuite
Parature
Responsys
Rightnow
LiveOps
MSDynamics
Salesforce.com
Oracle On Demand
Document Management
NetDocuments
DocLanding
Knowledge TreeLive
SpringCM
OpenCrowd
Updated as of October 12, 2010

Anything as a Service?

Many more *aaS acronyms exist- but we are starting to move beyond this.

C: Compute

N: Networking

S: Storage (but we already have another SaaS…)

Anything you can imagine

- And some things you can’t

Deployment Models

- Public cloud
- Private cloud
- Community cloud
- Hybrid cloud
- Virtual Private Cloud (VPC)

Public Cloud

…available to the general public or a large industry group and is owned by an organization selling cloud services.

Private Cloud

…operated solely for an organization.

…managed by the organization or a third party.

…on premise or off.

Community Cloud

Is shared by several organizations and supports a specific community that has shared concerns.

- Mission, security requirements, policy, and compliance considerations, etc.

…managed by the organizations or a third party.

…on premise or off.

Hybrid Cloud

…composition of two or more clouds… that remain unique entities but are bound together by… technology that enables data and application portability

Virtual Private Cloud*

Created by isolating and securing Public Cloud facilities into a Private Cloud configuration.

***Not part of the NIST definition, but should be.**

Characteristics

On-demand self-service

Broad network access

Resource pooling

Rapid elasticity

Measured Service

On-demand Self-service

A consumer can *unilaterally* provision computing capabilities…

***…automatically* without requiring human interaction…**

Broad Network Access

…available over the network and accessed through standard mechanisms…

Resource Pooling

…resources are pooled to serve multiple consumers using a multi-tenant model…

Who Else Is In The Pool?

Sharing the “locker room”, too

Resource Pooling

…customer generally has no control *or knowledge* over the exact location of the provided resources…

Resource Pooling*

***This is starting to fade as some providers begin offering dedicated hardware for certain tasks, but resource pooling remains a key cloud concept.**

Rapid Elasticity

Capabilities can be rapidly and elastically provisioned, in some cases automatically...

Rapid Elasticity

…the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Rapid Elasticity

Measured Service

Cloud systems automatically control and optimize resource use by leveraging a metering capability…

Availability

What if you are off the Internet, even briefly?

- Local copies mean synchronization and reconciliation.

No SLA will cover your losses.

And What About…

Portability and interoperability?

Compliance?

- This is a rabbit hole-
  - What happens as things change? How fast can you “re-comply”?

Unique Commodities?

Sounds like an oxymoron, but it isn't.

The unique offerings of cloud service providers are both assets and liabilities to the consumer due to limits imposed on portability.

Want to have some fun? Ask cloud providers about their network design and how that enables or restricts your cloud deployment.

Compliance And Audit

How does a small department or organization demand SLAs and accountability?

- That's right, we can't.

What about compliance? Audit?

- Cloud Audit/A6 (now part of CSA)

Network Visibility

Network visibility is tricky with virtualization; is it even possible in a cloud?

- Where do you put the network tap?

Agent Software

Since we do not have access to the network or server hardware, we may need to deploy software agents to inspect systems and traffic for us.

And we'll have to trust them.

Do not forget the basics

Many “basics” are more critical than ever:

Backups

Encryption

Logging

Authentication

Access control

Monitoring

Disaster Recovery

Cloud computing can ease the pain of DR, but can also exacerbate it- especially if you have to redeploy to local resources.

But wait…

Cloud computing offers many benefits, don’t let the dangers scare you away.

Assess the risks and rewards, determine what (if anything) is appropriate for moving to a cloud computing platform.

Compare providers and choose the best for your needs.

Make informed decisions.

Don’t be this guy

Feeling left out?

Want to play in the clouds, but don't have a budget? Or much time?

There are nearly free Amazon micro instances.

Cloudshare has a 14-day free trial.

CloudSigma has a 7-day free trial.

Look around, you will find ways to seed the clouds.

References

Primary reference documents for this presentation:

NIST

- Definition of cloud computing and related terminology
- Cloud Computing Reference Architecture

CSA Security Guidance for Critical Areas of Focus in Cloud Computing v 3.0 (new)

References

Additional references used in this presentation:

Cloud Computing Wiki

OpenCrowd Cloud Taxonomy

- ENISA Cloud Computing: Benefits, Risks and Recommendations for Information Security

References

The single best document, from the Australian Defence Signals Directorate:

http://www.dsd.gov.au/publications/Cloud_Computing_Security_Considerations.pdf

If you read only one thing as a follow up to this webinar, read this document.

Career Study Project

A group of us in the security community are researching what makes security professionals tick, and what makes us twitch. Please consider helping with the research by taking about ten minutes to request access and take our current survey. Details are at:

http://www.careerstudy.org

THANK YOU!

Shameless Self-Promotion:

- pauldotcom.com
- www.tenable.com
- jdaniel@tenable.com
- twitter.com/jack_daniel
- blog.uncommonsensesecurity.com