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

*It’s also a really good marketing job...
Cloud is an adaptive operational model, not a particular technology and there are lots of different types of Clouds.
The Technician’s Definition

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

Essential Characteristics

Delivery Models

Deployment Models

Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)

Broad Network Access
Rapid Elasticity
Measured Service
On-Demand Self-Service

Resource Pooling

Public
Private
Hybrid
Community

amazon.com
salesforce.com
:: The Consumer’s Definition

Everything Is Cloud...
Key Ingredients In Cloud

- Abstraction of Infrastructure
- Resource Democratization
- Services Oriented
- Self-Service
- On-Demand Elasticity/Dynamism With a Utility Model Of Consumption & Allocation
:: We’ve Been Here Before...

Mobility

Mainframes

The Cloud

Web2.0

Web1.0

Client/Server

Centralized

Distributed

Mostly Distributed

Unreliable/Slow

Mostly Centralized

Mostly Reliable/Fast

Reliable/Fast

More Reliable/Faster

Display

Compute

Data

Bandwidth

Thursday, September 1, 11
Three delivery models that people talk about when they say “Cloud”:

- **Software as a Service (SaaS)**
- **Platform as a Service (PaaS)**
- **Infrastructure as a Service (IaaS)**

What Do These Look Like?
IaaS Security :: Guest/Host-Based

- Provider secures “their” infrastructure to maximize availability & multi-tenancy
- Remainder of the stack (and confidentiality, integrity) is your problem
- General focus is on VM’s & Guest-Based
Provider owns the compute, network, storage layers & programmatic interface security

The consumer creates the applications based upon supported development environment

Writing secure applications and ensuring your data is safe is your responsibility
The Provider Owns the Entire Stack

Security (C, I and A) Become A Contract Negotiation

Traditional Security & Compliance Functions Are More Administrative & Policy-Focused
:: What This Means To Security

IaaS

Build It In

PaaS

Contract It In

SaaS

Provider

Consumer

Build It In

Contract It In
:: The Punchline

- In the simplest of terms, using cloud means imagining applications & information across all tiers have the potential to be connected directly to the internet...

- We can’t trust the provider, so we must engineer security into design patterns across the entire stack.

- Any “dumb” component in the stack compromises the integrity of the entire stack...

- APIs, intelligence and automation everywhere
All About Gracefully Giving Up Direct Operational Control Over Infrastructure
It All Comes Down To **Trust**...
Toward A Secure Cloud Future...
Journey To the Cloud Made Simple

Virtual Private Cloud

Federation / Workload Portability / Interoperability
Simple, Right?
Let’s Ask The Magic Cloud 8-Ball
Is Cloud A Major Shift In IT?
Will Everything Move To The Cloud?
Is All We Know & Do Today In Security Worthless In Cloud?
Is The Cloud More Secure?
Without Context, Silly Question
More Secure Than What?
Can We Trust The Cloud?
So I Have Options Today?
So, What’s The Future Of Cloud?
So, What’s The Future Of Cloud?
So, What’s The Future Of Cloud?
So, What’s The Future Of Cloud?
::The Internet Of Things

Connected Devices

1 Trillion
(140 connected devices per person)

500 million
(1/10th of a connected device per person)

35 billion
(5 connected devices per person)

Source: Forrester Research, Cisco analysis — forecast of 2013 assuming consistent growth trends

Applications

1,500,000
total mobile applications worldwide

3000
total mobile applications worldwide

265,000
total mobile applications worldwide

Source: Windows Mobile, Morgan Stanley
Cisco analysis — forecast of 2013 assuming consistent growth trends

Security Threats

5,700,000
security threats

624,000
security threats

2,600,000
security threats

Source: Symantec
Cisco analysis — forecast of 2013 assuming consistent growth trends

Cisco 2010 Mid-Year Security Report
There Are ~4,100,000,000 Of These....
...and 6,797,100,000 Of These

So While Mega Data Centers Re-Centralize Our Apps & Data In Fewer & Fewer Locations Thanks to Cloud...
These Little devices -- Distributed Everywhere -- Have Amazingly Powerful Processors, Lots Of Memory, Near-Ubiquitous Connectivity and Native Apps & Data…
The Consumption Modality Will Ultimately Become More Important Than The Back-End Delivery Mechanism
How Will You Choose What To Protect & Where Will You Choose To Invest To Protect It?
The Eight Things That Matter (Again)

- Open Standards & APIs
- Programmability & Automation
- Evolution of Name Spaces & Registries
- Transparency & Visibility
- {Id}Entity and Authentication
- Mobility
- Privacy & Law
- Information Centricity & System Survivability
What Does That Mean?
**Abstraction As Distraction**

- Cloud is a fantastic forcing function, let’s embrace it!
- Stay grounded: think globally, act locally
- The Cloud is De-Perimeterization...amplified
- Plan for FAIL | Re-architecture Means: Information Centricity & Survivability
- Public, Private, Hybrid? : All comes down to trust models
- Cloud is an iteration of a platform and an operational model, approach it as such and manage risk appropriately

**Focus on the data. It’s what we’re all concerned with in the first place.**
So What Will Cloud Bring Tomorrow?
Does It Really Matter?
What Are You Doing To Secure What You Have Today?
So, Can We Trust The Cloud?
Can You Afford Not To?
Find Out:

www.cloudsecurityalliance.org

http://www.enisa.europa.eu