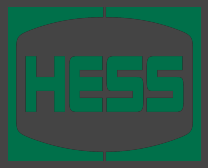
The Art and Science of Information Security

Stephen Schmidt

Vice President & CISO

Amazon Web Services

How are enterprises thinking about and using the cloud in 2014?



Strategies Enterprises Are Using on AWS…

1. Development & Testing
2. New Workloads
3. Supplement Existing Workloads with the Cloud
4. Supplement Workloads with Existing On-Premises Infrastructure
5. Migrating Existing Applications
6. Data Center Migration
7. All-in – IT Entirely in the Cloud

The common theme?

Increased Agility
Has Become the No. 1 Reason
Businesses Use AWS

Hotels

Music

Magazines

Storage

This is something “born in the cloud” companies have already discovered.

150K hosted per night	15M guests	1,300 EC2 instances

150K hosted per night	15M guests	1,300 EC2 instances

"We have a 5 person operations team."

"AWS allows us to devote our resources and mindshare to the core business."

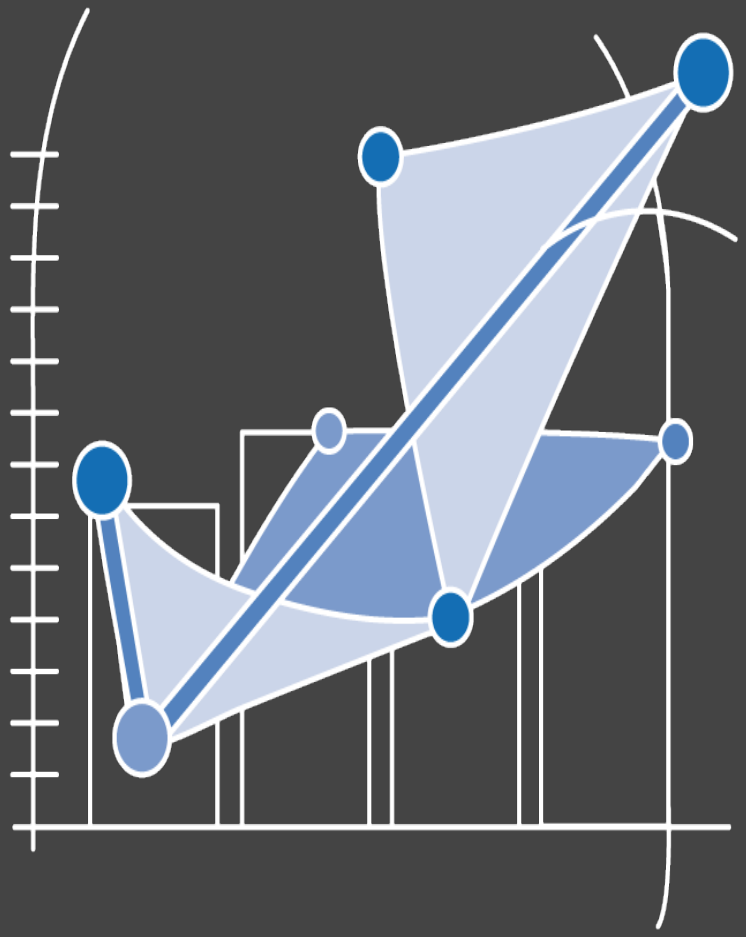
What does that mean for security?

AWS has to take on much of the undifferentiated heavy lifting

What does that mean for airbnb's staff?

They focus on what matters to *their* business

Forces Driving New Resource Models



Increasing Uncertainty

Limited Access to Capital

Growing Abundance

Intensifying Competition

Growing Power of Customers

Decreasing Brand Loyalty

Key Benefits of New Resource Models

Acquire Resources On Demand

Release Resources When No Longer Needed

Pay For What You Use

Turn Fixed Costs Into Variable

Leverage Other's Core Competencies

Enterprises Are Accelerating Time to Market with AWS

bankinter.

Credit-risk simulation application

Decreased the average processing time from 23 hours to 20 minutes

Development & test environments

Development and test seats access time reduces from week to 1 day

Migrated 500 web properties to AWS in 5 months

New product websites from 2 weeks to 2 days

Clinical trial simulations

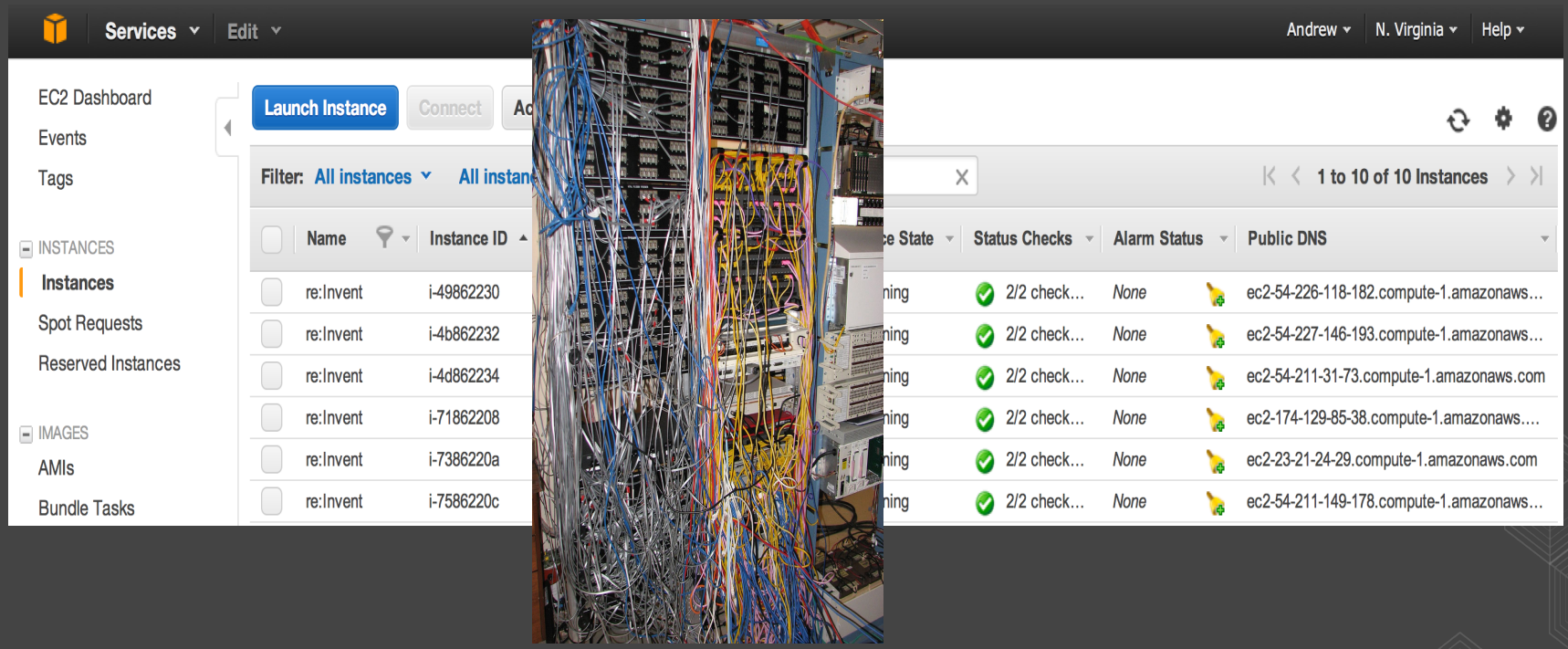
Simulations time reduced from 60 hours to 1.2 hours

AWS Security fundamentals

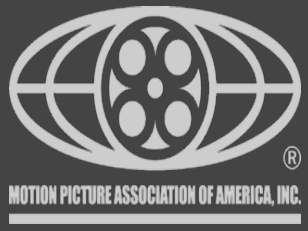
Visibility
Auditability
Control

Visibility

- In the AWS cloud, see your entire infrastructure at the click of a mouse
- Can you map your current network?

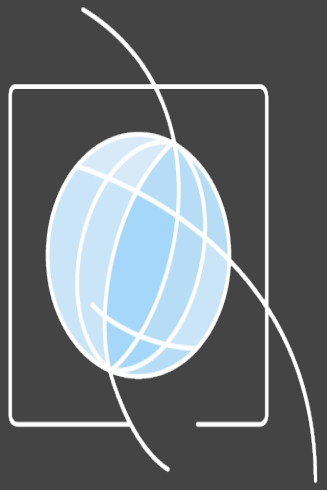


More auditable:
Certifications and Accreditations for Workloads That Matter



More Control: AWS Governance

Fine-grained access control over data and resources



Geographic data locality

Control over regional replication

Fine-grained access control

Policies, resource level permissions, temporary credentials

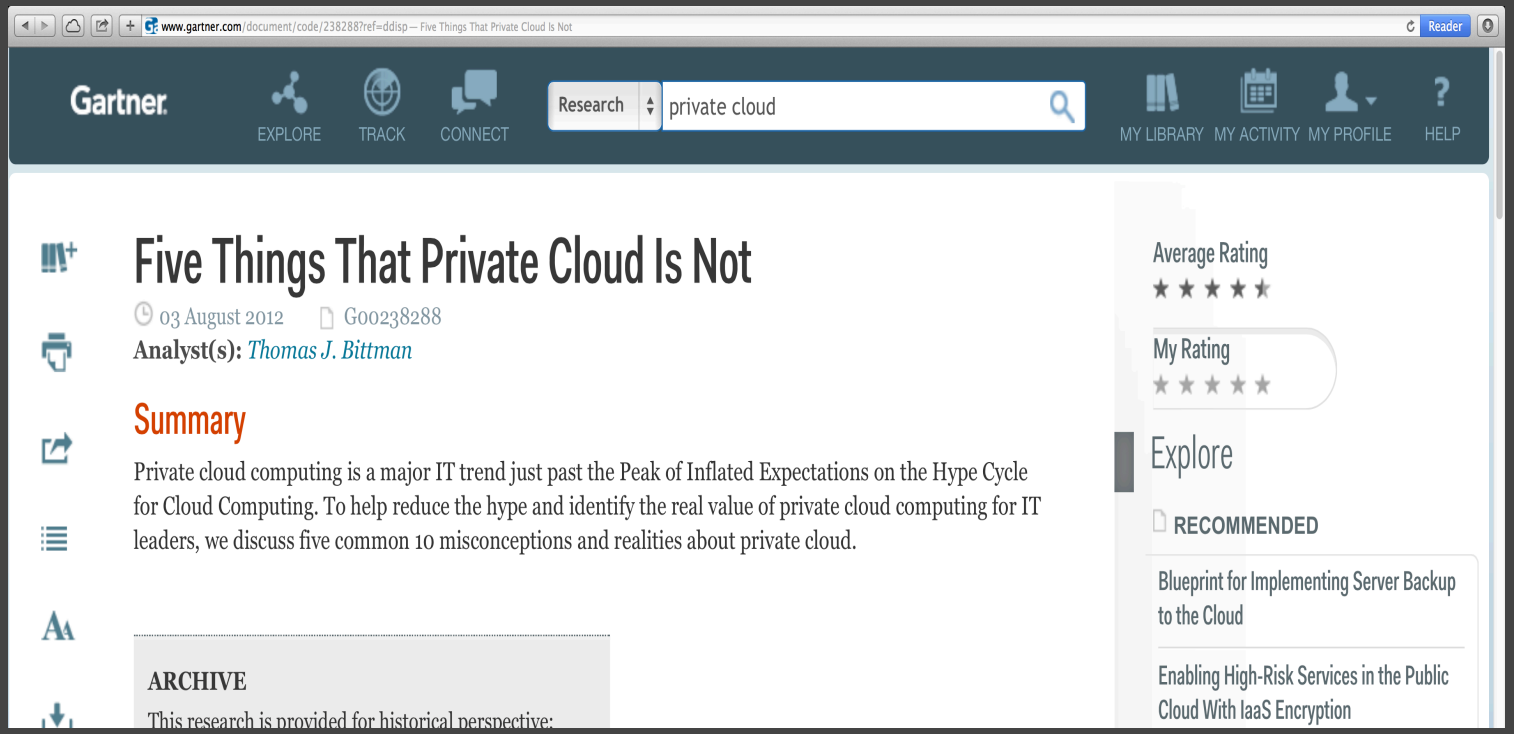
AWS CloudTrail

In-depth audits

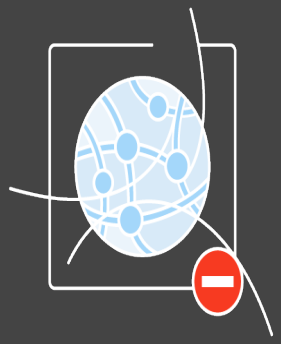
What if I need a private cloud?

Gartner®

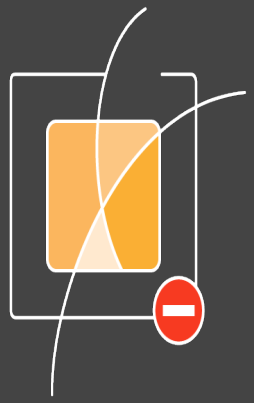
"Private cloud is not necessarily on-premises…"



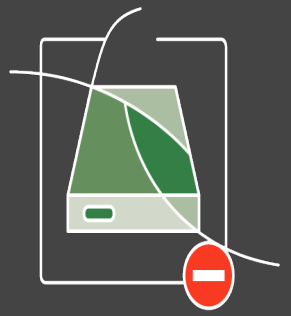
What Are Customers Really Looking For?



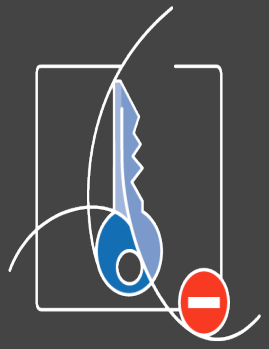
Private Network



Private Compute



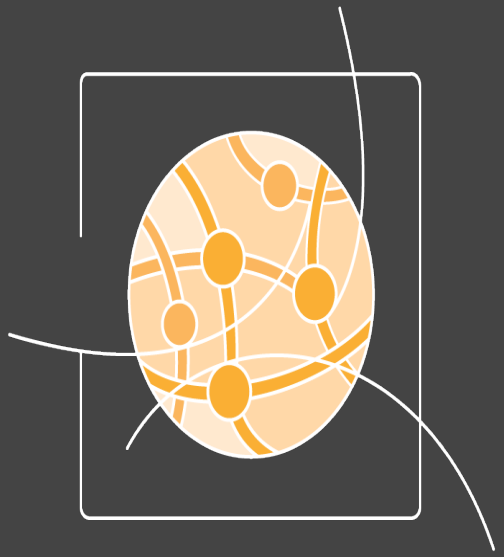
Private Storage



Private Key
Management

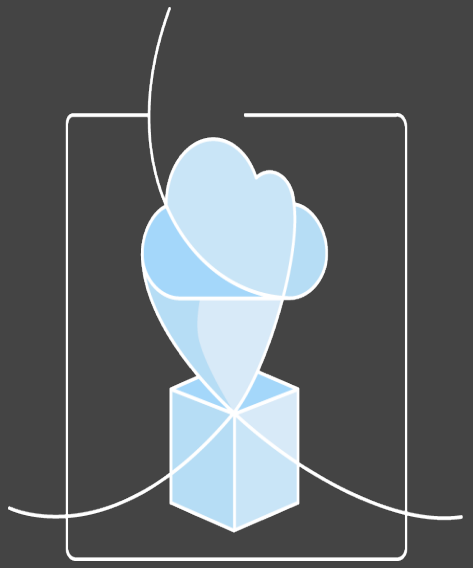
Good
Governance

AWS Private Network Capabilities



Amazon Virtual Private Cloud
(VPC)

Software-defined private network



AWS Direct Connect

Dedicated private network connection
to AWS

AWS Private Compute Capabilities

Choose the right level of compute isolation for every workload

Identity & Access Management (IAM)

Fine grained access roles and groups

EC2 in a VPC

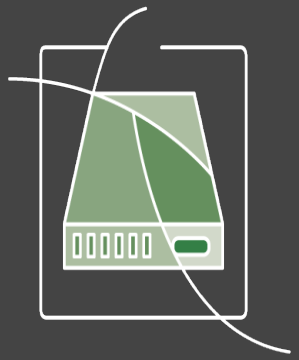
Software-defined network isolation

Dedicated Instances

Physical isolation

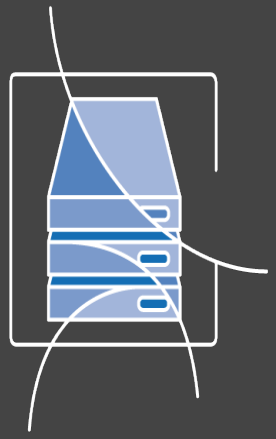
AWS Private Storage Capabilities

Choose the right level of storage isolation for every workload



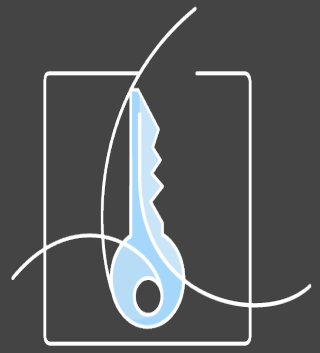
Amazon S3

Encrypted object storage



Amazon EBS

Encrypted block storage



Amazon CloudHSM

Private encryption key management

AWS Direct Connect

Single-tenet block storage

How does AWS do things differently when it comes to security?

The practice of security at AWS is different, but the outcome is familiar:

Focus on your business, not the undifferentiated heavy lifting

This applies within AWS, just as it does for our customers

The practice of security at AWS is different, but the outcome is familiar:

Apply more effort to the “why” rather than the “how”

Why is what really matters

When something goes wrong, ask the “five why’s”

The practice of security at AWS is different, but the outcome is familiar:

Decentralize - don't be a bottleneck

It's human nature to go around a bottleneck

Instead, hold senior executives accountable for security – have them drive the right culture

The practice of security at AWS is different, but the outcome is familiar:

Everyone’s an owner

When the problem is “mine” rather than “hers” there’s a much higher likelihood I’ll do the right thing

For a security professional, saying “NO” is a failure

AWS Cloud Security

"Based on our experience, I believe that we can be even more secure in the AWS cloud than in our own data centers."

-Tom Soderstrom, CTO, NASA JPL

Thank You