ASMC
National Capital Region
Professional Development Institute

10 March 2016

Innovation Insight Sessions

Innovation Insight Sessions: 1040 - 1150

- **Mr. Michael Allen,** Beacon Global Strategies
- **Mr. Scott Forrest,** USN
- **Ms. Lauren Leo**, NASA
- **Mr. Mark Ryland**, Amazon Web Services
- **Mr Phil Searle**, Founder, Chazey Partners
- **Brig.Gen. Greg Touhill, USAF(Ret),** DHS
- **Mr. Leif Ulstrup**, PrimeHook Technology

Improving Security and Compliance with Amazon Web Services

Mark Ryland – Chief Solutions Architect, WWPS
markry@amazon.com

amazon web services

Improving Security with AWS…

"From a physical and logical security standpoint, I believe that, if done right, public cloud computing is as or more secure than self-hosting."

– Steve Randich, EVP and CIO, Financial Industry Regulatory Authority in the USA

- FINRA now deploying multiple Hadoop-based and Redshift-based analytics apps core to their regulatory mission
  - Multi-petabyte clusters growing by terabytes per day
  - In full production since January 2015
  - Two year plan to go "all in" to the AWS cloud

FINRA
Financial Industry Regulatory Authority

amazon web services

Rob Alexander / CIO of Capital One Bank

"And of course, security is critical for us. The financial services industry attracts some of the worst cyber criminals. So we worked closely with the AWS team to develop a security model which, we believe, allows us to operate *more securely* in the public cloud than we can even in our own datacenters."

re:Invent Keynote 2015 https://youtu.be/0E90-ExySb8

amazon web services

Improving Security with AWS

“Based on our experience, I believe that we can be even more secure in the AWS cloud than in our own datacenters.”

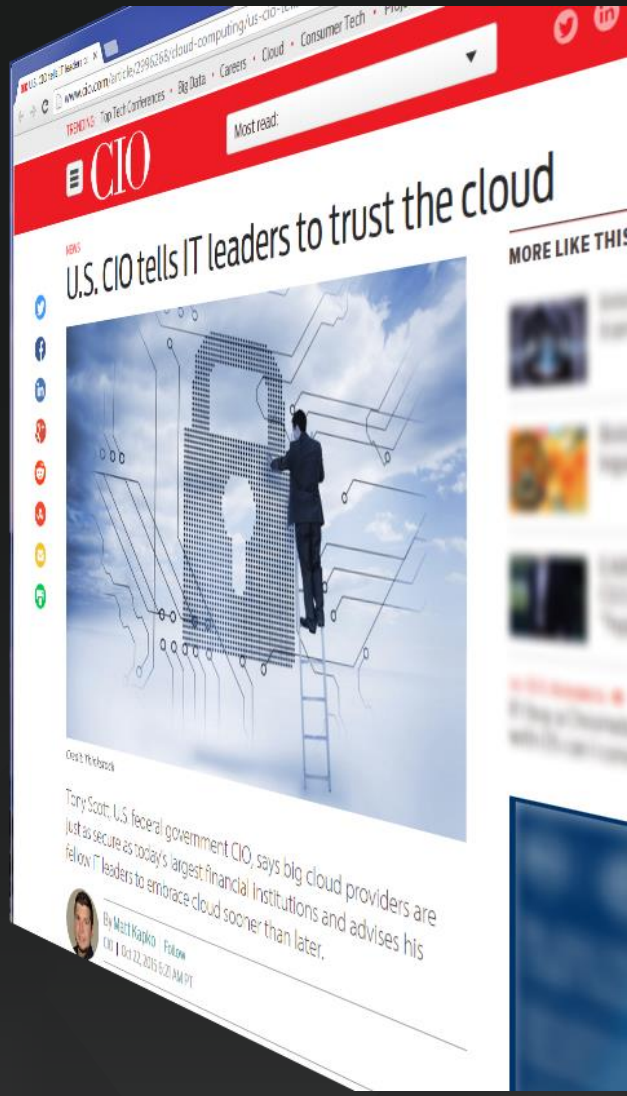
-Tom Soderstrom, CTO, NASA JPL

For more details, see Re:Invent 2013 presentations by NASA JPL cyber security engineer Matt Derenski (http://awsps.com/videos/SEC205E-640px.mp4)

USA CIO Tony Scott

“I see the big cloud providers in the same way I see a bank,” he says. “They have the incentive, they have skills and abilities, and they have the motivation to do a much better job of security than any one company or any one organization can probably do. […] I think today the better bet is get to the cloud as quick as you can because you're guaranteed almost to have better security there than you will in any private thing you can do.”

CIO Magazine: http://bit.ly/1LpX8Uy



amazon web services

Improving Security with AWS…

"… We'll also see organizations adopt cloud services for the improved security protections and compliance controls that they otherwise could not provide as efficiently or effectively themselves."

Security's Cloud Revolution is Upon Us

Forrester Research, Inc., August 2, 2013

amazon web services

Analyst's Latest Perspective

CIOs and CISOs need to stop obsessing over unsubstantiated cloud security worries, and instead apply their imagination and energy to developing new approaches to cloud control, allowing them to securely, compliantly and reliably leverage the benefits of this increasingly ubiquitous computing model.

-- Jay Heiser

Clouds Are Secure: Are You Using Them Securely?
Published: 22 September 2015

Gartner

amazon web services

Cloud Security Alliance Keynote (Dec 2013)

"Seven Systemic Advantages of Cloud Security"

Six reasons, plus one to grow on:

1. Integration of compliance and security
2. Economies of scale apply
3. Customer refocus on systems and applications
4. Visibility, homogeneity, and automation
5. Cloud platforms as "systems containers"
6. Cloud, big data, security: cloud secures cloud
7. With cloud speed of innovation and increasing scale, the story will only get better – quickly!

Former CIO of VA & Commerce Roger Baker in NextGov.com (Jan 2015):
"Why Commercial Cloud Are More Secure Than Federal Data Centers"

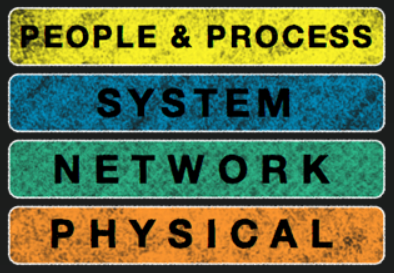
Six reasons:

http://bit.ly/1tMrUSp

- New and sometimes purpose-built equipment and software, constantly updated;
- System configurations are standardized and automatically created to eliminate variances, and for maximum efficiency;
- Security patches are automatically applied to all systems on a timely basis;
- Cloud environments are certified to multiple different national and international security standards;
- The private sector can hire high-level system engineering and security talent more readily; and
- The company's brand is at risk should security be compromised, ensuring full alignment and motivation.

amazon web services

Security is Job Zero



Familiar security model

Validated by security experts

Collaboration on Enhancements

Every Customer Benefits

Physical Security	Network Security	Platform Security	People & Procedures

Security & compliance is a shared responsibility

Customers

Customer applications & content

Platform, Applications, Identity & Access Management

Operating System, Network, & Firewall Configuration

Client-side Data Encryption | Server-side Data Encryption | Network Traffic Protection

AWS Foundation Services

Compute | Storage | Database | Networking

AWS Global Infrastructure

Availability Zones | Regions | Edge Locations

amazon web services

Customers have their choice of security configurations **IN** the Cloud

AWS is responsible for the security **OF** the Cloud

amazon web services

Build everything on a constantly monitored and audited, constantly improving security baseline

GxP
ISO 13485
AS9100
ISO/TS 16949

AWS is responsible for the security **OF** the Cloud

amazon web services

Simple Security Controls

Easy to Get Right

Easy to Audit

Easy to Enforce

This

To This

Our Culture

Make your security engineers part of your product/service engineering teams

Make your compliance team part of your security operations

Our Culture…

Proactive, predictive monitoring rules the day

- What's "normal" in your environment?
- Depending on signatures == waiting to find out WHEN you've been had

Our Culture…

Collect, digest, disseminate
& use intelligence

Our Culture…

Base decisions on facts, metrics, & detailed understanding of your environment and adversaries

Our Culture…

Test, CONSTANTLY

- Inside/outside
- Privileged/unprivileged
- Black-box/white-box
- Vendor/self

AWS is Cloud Leader and Visionary

Gartner Magic Quadrant for Cloud Infrastructure as a Service, Worldwide

Source: Gartner (May 2015)

Gartner "Magic Quadrant for Cloud Infrastructure as a Service, Worldwide," Lydia Leong, Douglas Toombs, Bob Gill, May 18, 2015. This Magic Quadrant graphic was published by Gartner, Inc. as part of a larger research note and should be evaluated in the context of the entire report. The Gartner report is available at http://aws.amazon.com/resources/analyst-reports/. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

amazon web services

Forrester Cloud Security Wave (Nov 2014)

Cloud provides better answers to key governance questions

- What do I have?
- How it is performing?
- Who is controlling it?
- What is it costing me?
- Is it secure and compliant?
  - Are changes occurring with the right processes and protections?

What do I have?

- Describe* calls provide comprehensive lists of all resources (for example, `aws ec2 describe-instances`)
- AWS Config provides graph-based integration, time-based insights
  - (Building a comprehensive, accurate configuration DB on-premises is practically impossible)
  - AWS Config Rules to evaluate changes and respond
- Partner ecosystem adds more value, richer capabilities
  - Theme: AWS provides data feeds, anyone can build tooling

How is it performing?

- Services emit metrics into CloudWatch, accessible through console, CLI, API
  - Alerting and alarming on all metrical data
- CloudWatch Logs integrates OS and app log data
  - AWS Elastic Search automates the pooling, querying, and visualization of CW Logs
  - Rich integration of both CW and CWL w/ Simple Notification Service
- Trusted Advisor for dashboard and alerts for under-utilization, security, availability issues
- Rich integration into third-party monitoring platforms from AWS partners

Who is controlling it?

- Powerful, fine-grained IAM capabilities
  - Authentication and *authorization*
  - Reporting and analysis
- Rich integration to enterprise identity systems through SAML or directly into Active Directory
- Tagging for authorization, administration, billing

Cost transparency and control

- Everything billed by hour, gigabyte, etc.
- Billing data updated ~4x *per day*
- Programmatic access to all billing data linked to user-created resource tags
- Cost Explorer and other tooling
- CloudWatch tools/alarms for billing data
- AWS MarketPlace helps with software license management challenges

amazon web services

Secure and compliant?...

- … Are changes occurring with the right processes and protections?
- AWS infrastructure: **yes**
  - See frequently updated 3rd party audits
- Customer usage of AWS: get to **yes** like never before
  - Great tools and building blocks to build the right models, processes, and automation

Agile security with programmable infrastructure

- Trusted Advisor displays obvious (possible) issues
- CloudWatch (Logs), VPC Flow Logs, S3 logs, ELB logs
  - AWS ElasticSearch for managed search, analysis, visualization
- CloudTrail, Config and Config Rules, Inspector
- VPC peering (including cross-account)
- Identity federation and cross-account role-based access
- Service Catalog/CloudFormation for repeatable processes
- Compliance Enterprise Accelerator: pre-audited CF templates for *automated* compliant environments

Customer's horizontal shared responsibility

- Mission teams control their own infrastructure (VPCs, instances, AMIs, DBs, S3 buckets, etc.)
- Central GRC/security team has audit and control rights over core infrastructure along with "shared security & compliance services"
- Best of both worlds: agility benefits of mission-driven "shadow IT," governance/security benefits of central IT control

Concretely: Managed Services Organization (MSO)

- Central team providing shared services:
  - Account creation and IAM provisioning/setup
  - Identity management, federation endpoint(s)
  - Core networking security and IAM policies
  - Golden OS images (AMIs), associated IAM limits
  - Central auditing services
    - CloudTrail, Config, security log management
  - Incident response/forensics services
  - Cost alarm/review/auditing services

Demo: scenario

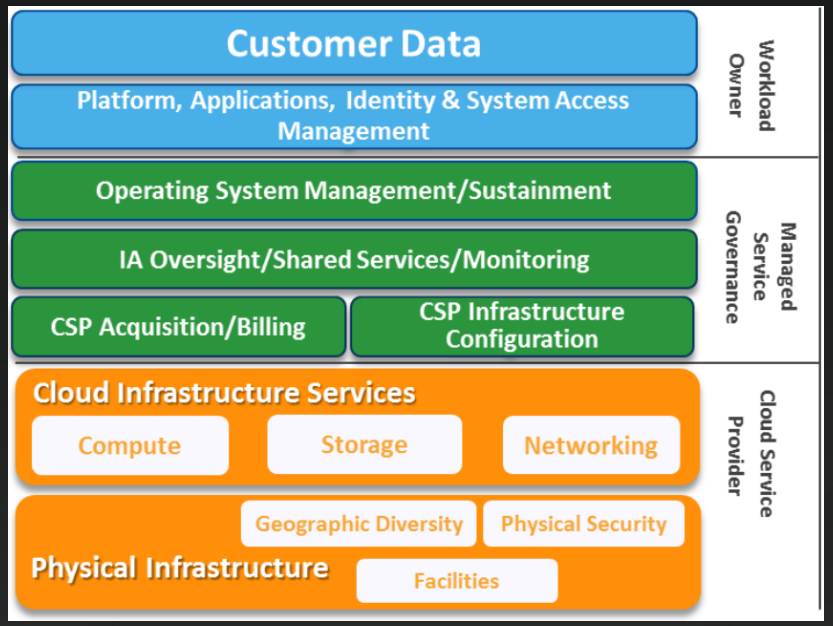
- Development Team requires:
  - Direct access to AWS console
  - On-demand provisioning of Dev environments
  - Login credentials for running instances
  - Support for continuous integration and deployment
- Company requires:
  - Adherence to approved reference architectures
  - Auditability of activities within the account and instances
  - Visibility to resources used and network traffic flow
  - Control of the account, VPCs, and instances

Full presentation with demo: https://youtu.be/YYiV_z9D2CE

Demo: automating governance

- Company creates a Managed Services Organization (MSO)

- Delivers the implementation piece of the governance puzzle
- Provides automated, self-service delivery of approved architectures
- Maintains centralized control of accounts, security oversight
- Leverages AWS Compliance Accelerator



Security and the AWS ecosystem

AWS Marketplace: One-stop shop for familiar tools

Advanced Threat Analytics	Application Security	Identity and Access Mgmt	Server & Endpoint Protection	Network Security	Encryption & Key Mgmt	Vulnerability & Pen Testing
ALERTLOGIC	IMPERVA	CIPHERGRAPH networks	TREND MICRO	SOPHOS	SafeNet	tenable network security
ALIEN VAULT	FORTINET	SECUREAUTH	intel Security	FORTINET	Vormetric	QUALYSGUARD
	Barracuda	M-Pin SSO Authentication for Enterprises		Check Point We Secure the Internet	HYTRUST	
				paloalto networks		

amazon web services

It’s happening!

- Not a pipe dream, but reality at enterprises and gov’t agencies around the globe
- Even agencies with highly sensitive workloads like Citizenship and Immigration Services, DHS, USA; for example, Mark Schwartz, CIO:
  - https://youtu.be/QwHVlJtqhaI (on dev/ops in gov’t)
  - https://youtu.be/Whbed3dAxiU (on innovation in gov’t)
  - DevOps and CI/CD on the AWS cloud providing dev/ops CI/CD agility with baked-in governance and security benefits

Schwartz's List of DevSecOps/CI/CD Benefits

- Ease of changing contractors
- Metrics / objective data for decision-making
- Compliance, security, static code analysis, etc.; continuous monitoring of production systems (DevSecOps)
- Better risk management (risks are tiny, each day is full of lots of small experiments)
- Increased efficiency and reduced waste

THANK YOU!

Mark Ryland – markry@amazon.com

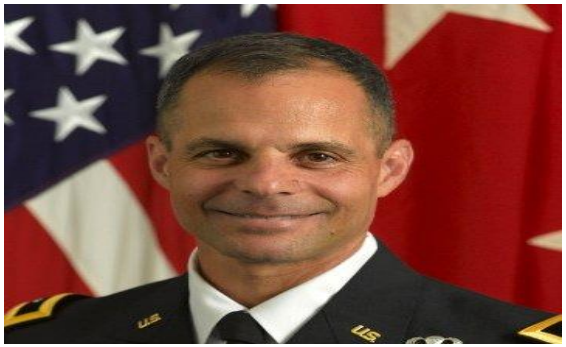
amazon web services

Improving Security with Cloud Computing

Mr. Mark Ryland, Director of Solutions Architecture and Chief Architect
Amazon Web Services

Luncheon: Atrium Hall

Luncheon Keynote:



Lieutenant General Anthony R. Ierardi, USA

Director, Force Structure, Resources & Assessment, J8
The Joint Staff

Note: Please be seated by 12:00

Luncheon: Atrium Hall

ASMC National Update:

Mr. Al Runnels, USA, CDFM, CGFM

ASMC Executive Director

Post NCR PDI Events

Speed Mentoring

- Government only, Pre-registration required
- Meridian DE at 1700
- 1.5 CPE Credits

ASMC 2015 Annual Survey

- Invitation Only
- Horizon at 1700 [Concourse Level]
- **Host: Mr. Al Runnels, USA, CDFM, CGFM**
  ASMC Executive Director
- Mr. Mark Easton, Deputy Chief Financial Officer, Department of Defense
- Mr. Doug Bennett, Principal Deputy, Assistant Secretary of the Air Force, Department of the Air Force
- Mr. Joe Marshall, Principal Deputy, Assistant Secretary of the Navy, Department of the Navy
- Mr. Craig Bennett, Deputy Chief Financial Officer, United States Coast Guard
- VADM Louis Crenshaw, Ret, USN, Moderator

With Gratitude to our 2016 Corporate Sponsors


Grant Thornton
pwc
CALIBRE
EY Building a better working world
KEARNEY& COMPANY
ORACLE
SAP
SEHLKE consulting
AOCSolutions
CACI EVER VIGILANT
Deloitte.
KPMG
savantage solutions
CMMI-DEV Level 3 | ISO 9001:2008
TRANSFORMING CLIENTS' VISION INTO RESULTS
DEFINITIVE LOGIC
VANGUARD ADVISORS
CONSULTING LEADERS IN BUSINESS AND GOVERNMENT
ST. MICHAEL'S
TG THOMPSON GRAY INC.
ACUITY
citi
Cotton& Company
Answers Questioned
IFAS
Mission Focused. Results Driven.
KGS
Lynch consultants
MANAGEMENT CONCEPTS
MIL corp.
MORGANFRANKLIN CONSULTING
WILLIAMS ADLEY
BECKER PROFESSIONAL EDUCATION
Castro& Company
CGI
IMMERSION CONSULTING
LMI
COMPLEX PROBLEMS. PRACTICAL SOLUTIONS.
NEUBRAIN
TERATHINK