Challenges and Solutions in Cloud Security

Jonathan Villa | Practice Director, Cloud Security | GuidePoint Security
My story: Introduction

• I’ve been having fun for 18 years
  • App Arch., Middleware, SysAdmin
  • PCI, InfoSec, AppSec
  • ISACA Presentations to NYC & MKE

• Building solutions in AWS since 2007
  • Operations
  • Architecture
  • Compliance
  • For organizations large and small

• AWS Advanced Consulting Partner
  • Security Competency Launch Partner

• How “cloud” happened for me
My story: Career Timeline

System Administrator, Application Security, Middleware Administrator
How “the cloud” happened for me
and why it’s relevant to cloud security
Why is “cloud” security needed?

- Cloud security is still evolving and maturing as a discipline as cloud service providers release new services.

- Security leaders/teams **are not** spending 40 hours working with or learning cloud.
  - IT and application teams **are** spending **50+ hours a week building** in the cloud.
  - Steep learning curve for many security professionals due to significant reliance on code.

- There is a need for equal knowledge of cloud operations and information security.

- History is repeating itself.
  - New technologies.
  - New/modified processes.
  - Redefining industry standards in light of the Shared Responsibility Model.
Principles of Cloud Computing – the “why”

“Cloud computing is a model for enabling ubiquitous, 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.” (NIST 800-145)
Relationship Problems: Cloud and Security

• Cloud adoption began with developers
  • Driven by the technology, speed, and bypassed security

• “We’re agile, security will slow us down”

• Blurred the defined “separation of duties” boundaries

• Enterprise cloud adoption driven by leaders
  • “...our CIO has a cloud first strategy.”
  • “...we’ll be 100% cloud in 18 months.”

• Relationship needs improvement but we’re getting along
  • Technology solutions
  • Consultants
  • Cloud Service Providers
Understanding the risks and concerns

- Risk of breach with the cloud service provider
- Data residency violations
- Direct impact from attacks on cloud platforms
- Misunderstanding the what/where of the Shared Responsibility Model
- Misunderstanding financial impact of provisioning cloud resources
- Loss of visibility ("I used to be able to see everything")
- Identity management creates a new perimeter
- New technology and a new lexicon
New technology, new lexicon, and new icons?!?

CloudFormation
Instance Roles
IAM and Bucket Policies
What’s a “bucket”?  
VNet
S3
VPC
Cognito
SQS, SNS, SES
DocumentDB
DynamoDB
Beanstalk
CloudTrail
ExpressRoute

InfoSec
Understanding the cloud delivery models
Cloud Security Domains

- Cloud Security Alliance Cloud Controls Matrix

  - Application & Interface Security
  - Audit Assurance & Compliance
  - Business Continuity Mgmt & Op Resilience
  - Change Control & Configuration Management
  - Data Security & Information LifeCycle Mgmt
  - Datacenter Security
  - Encryption & Key Management
  - Governance & Risk Management
  - Human Resources Security
  - Identity & Access Management
  - Infrastructure & Virtualization
  - Interoperability & Portability
  - Mobile Security
  - Sec. Incident Mgmt, E-Disc & Cloud Forensics
  - Supply Chain Mgmt, Transparency, Accountability
  - Threat & Vulnerability Management
Common Challenges

- Supply chain, knowing who/what is a “cloud” based solution
- Access governance
- Infrastructure management
- Vulnerability management
- Incident response
- Compliance
Supply Chain Management – Cloud Providers

• Can I trust all cloud vendors?

• Not all solutions are “cloud” solutions. SaaS means “as-a-service”

• Not all cloud solutions are built the same

• Remember, you own the data

• Shared Responsibility means “shared responsibility”
Access Governance

- Least-privilege is challenging, but it can be done
- Own the perimeter
- Developers will need privileged access to build and design
- Work with developers to identity best-fit access governance models
- Yes, production environments can be locked-down
- Require cross-account roles for third-parties
- Identity Federation
- Require multi-factor for CLI and cloud console access
Infrastructure-as-Code

- Components of Secure SDLC have an important role

- Build a pipeline and automate enforcement
  - Event-driven-security
  - Reduce audit gaps/findings

- Static code analysis
  - Source code
  - Infrastructure code

- Automated builds and deployments
Vulnerability Management

• The best fit tools depend on deployment model

• DevOps challenges traditional tools, but it’s not impossible

• Traditional vendors are improving and re-architecting

• Immutable and Ephemeral
Incident Response

- Automate containment

- Forensics challenged due to only having guest access to hypervisor

- What is your provider's involvement and process?

- Prepare for digital forensics
Cloud Security Technologies

• Do they understand elasticity?

• Does the CSP support their method?
  • Technology
  • Cost

• Does the CSP provide a comparable solution?

• Do they have an API?
Conclusion

• In my experience, the cloud has to be done right
  • Computing
  • Security

• When done right, you can be more secure
  • Ubiquitous
  • On-demand
  • Configurable computing resources
  • Rapidly provisioned and released

• Learn fast, test often, & improve
  • ...because “the cloud” has just changed again.