Locking Down Your Cloud

Teri Radichel | @teriradichel
CEO, 2nd Sight Lab
Can You Be More Secure in the Cloud?

• AWS security processes
• Segregation of duties
• Built-in inventory
• Platform to automate – almost everything
• Scalable log storage and backups

• More secure? Maybe...
But.

Read The Instructions.
Shared Responsibility

CUSTOMER

RESPONSIBLE FOR SECURITY "IN" THE CLOUD

- CUSTOMER DATA
- PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
- OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
- CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
- SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
- NETWORK TRAFFIC PROTECTION (ENCRYPTION/INTEGRITY/IDENTITY)

AWS

RESPONSIBLE FOR SECURITY "OF" THE CLOUD

- COMPUTE
- STORAGE
- DATABASE
- NETWORKING
- AWS GLOBAL INFRASTRUCTURE
- REGIONS
- AVAILABILITY ZONES
- EDGE LOCATIONS
Recent S3 Bucket Breaches...

- Sensitive medical records on AWS bucket found to be publicly accessible.
  SC Magazine UK - Jan 22, 2018
  A large cache of sensitive medical records handled by a US-based digital records management company was found stored in an Amazon S3 storage bucket. Researchers at security firm Kromtech Security Centre were made aware of the breach in early December by an independent researcher, following...

- Details of 12k social media influencers are leaked due to Octoly.
  2-spyware.com (blog) - 6 hours ago
  According to the breach analysis blog, UpGuard, more than 12 thousand social media stars were exposed during the data leak at a marketing firm Octoly. In addition to these personal details, the bucket also contains a large amount of brand and analytical information, the disclosure of which could be...

- Over 19 million California voter records leaked by Sacramento Bee.
  International Business Times UK - 19 hours ago
  The Secretary of State’s said it is taking the breach “very seriously” and is currently working with The Sacramento Bee and its parent firm The McClatchy. Misconfigured MongoDBs and AWS S3 buckets are among the most reported cases of data leaks for the last year and 2018 seems to be another...
S3 Bucket Security Controls (Customer!)

- S3 ACL – blocks Internet by default
- S3 Bucket Policy – many options
- IAM Roles to access bucket
- S3 endpoint to restrict network access
- Cross-account roles
- CloudFront restrictions
- Front with API Gateway
- CloudTrail and S3 access logs
S3 Misconfiguration – When and Why?

• **Before Deployment:** Did not understand or implement correctly.

• **After Deployment:** Malicious, inadvertent, or rushed change.

• *How can an organization prevent misconfigurations?*
Possible Solution

• Understand the controls and create policies

• Have a security professional review every change

• Reject any change that does not match security policies

• Some companies try to do this manually...does. not. work.
The Tug of War ~ Security and Innovation

• Security people want to prevent insecure deployments.
• Businesses acknowledge they need security…but...
• Will they delay deliverables for it?

• Experienced this tug of war – wrote a paper:
  
  *Balancing Security and Innovation With Event Driven Automation.*
A Tale of Two Clouds

Cloud One: Automated Response After Deployment
• Allow deployments to occur
• Monitor and reverse unwanted actions

Cloud Two: Automated Response During Deployment
• Force deployment through automated build system
• Built-in security checks
• Block or alert on non-compliant deployments
• Immutable Infrastructure
Immutable Infrastructure

• From concept of an immutable class in software engineering
• Infrastructure and containers, once created, cannot be changed
• To change the infrastructure requires re-deployment
• Prevent configuration changes outside build system
• Eliminate cost of agents (Chef, e.g.)
• Eliminate extra holes in network
Cloud One: Pros and Cons

Pros
- Non-blocking
- Faster to get up and running, fix problems
- Catches changes outside of deployment process

Cons
- Vulnerable time between detection and rollback
- Rollback failure leaves problem in production
- Doesn’t track who made changes
- Repeat problems drive up maintenance cost
Cloud Two: Pros and Cons

Pro

• Track every change with user name
• Limits attack surface
• Lowers long term costs by reducing human error
• Failure happens before deployment if implemented correctly

Cons

• Requires investment up front
• Longer process to fix bugs and problems
• An incorrectly designed build system impedes work
Ideally: Best of Both Clouds

- Create an automated deployment system
- Iteratively add security checks
- Architect for segregation of duties
- Monitor after deployment for unwanted changes
- Implement automated incident response
Automated Intrusion Detection and Response

https://www.sans.org/reading-room/whitepapers/incident/balancing-security-innovation-event-driven-automation-36837
Deployment System Considerations

- Immutable Infrastructure
  - VPC
  - docker
  - Credentials: Development

- Injected Configuration
  - VPC
  - Credentials: QA

- Per Environment Credentials
  - VPC
  - Credentials: Staging

- Segregation of Duties

- Failed Validation
  - Terminate

- Docker Containers
  - Software Libraries
  - PIP Packages
  - DLLS

- JFrog Artifactory
  - Source Code
  - Configuration Files
  - Nothing sensitive
  - No keys, no creds

- GitHub
  - Deployment jobs
  - Parameterized
  - Different users
  - Different environments
  - Logging
  - Security checks

- Jenkins

Deployment Systems
Packet Capture on AWS

- No access to span ports
- Instead leverage routing
- Set up capture and forward
- POC only...
- Architect for scalability
- Long running processes

https://www.sans.org/reading-room/whitepapers/detection/packet-capture-aws-37905
Transit VPC

- Security team account or VPC
- Capture traffic crossing boundaries
- No other escape routes
- Could replicate logs to this account
- Install a SIEM or other security analysis tools

Cost Control

• AWS Pricing = a Formula
• Need to know your inputs, to get accurate outputs (cost)
• Optimize system cost the way you optimize for performance
• More in the appendix of paper: *Packet Capture on AWS*
In Summary...

• Understand cloud security controls
• Secure, flexible, centralized deployment and monitoring
• Event driven automated response
• Segregation of Duties
• Cost management

“Dance like no one is watching. Encrypt like everyone is.” – Werner Vogels
Thank you!

Teri Radichel | @teriradichel
2nd Sight Lab | https://2ndsightlab.com