Data Protection at AWS

what you don’t know COULD hurt you

All about us...

Certifications:

AWS Certified Solutions Architect – Pro
AWS Certified DevOps Engineer - Pro
AWS Certified Security - Specialty
Certified Information Security Professional (CISSP)
GIAC Certified Enterprise Defender (GCED)

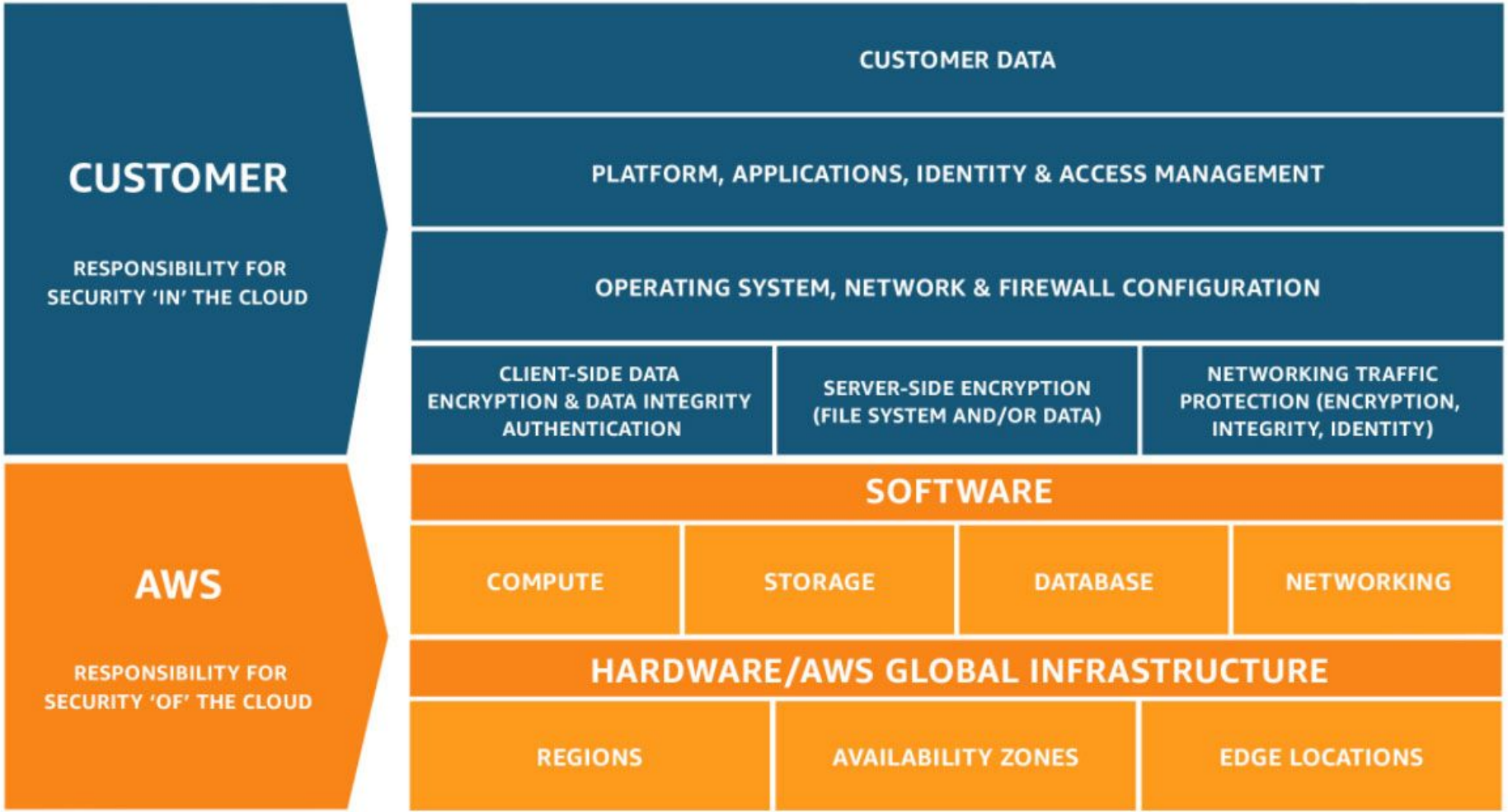
Steven D. Pressman (steve@alpinecyber.com)

10 years with Lockheed Martin
- Staff Computer Systems Analyst

2 years with The SI Organization
- Chief Solutions Architect

Alpine Cyber Solutions
- President and Chief Solutions Architect
- Chief Cloud and DevOps Champion

The Basics - Shared Responsibility


CUSTOMER
RESPONSIBILITY 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)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
AWS
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

The Basics - Data Storage Options

Data Storage/Access Services

"Traditional"

- S3
- EBS
- EFS
- Storage Gateway
- AWS Backup
- Snowball
- DataSync
- FSx

Database/Warehouse

- DynamoDB
- RDS
- ElastiCache
- Neptune
- QLDB
- DocumentDB
- Glue
- Lake Formation
- Redshift

Access/Reporting/Analysis

- Athena
- Quicksight
- Data Pipeline
- EMR

Protecting your Data

Network Protections

Architecture is Key

- VPC layout can make or break your security
- Protection comes in layers:
  - ➔ OS Firewall
  - ➔ Security Groups
  - ➔ Route Tables
  - ➔ NACLs
  - ➔ NAT Gateway
  - ➔ Firewall
  - ➔ CDN
  - ➔ WAF
- Most of AWS's built-in services can leverage VPC constructs

Encryption at Rest

Key Management Service (KMS)

- Centralized Key Management
- Built-In to Many Services
- Generate keys or bring your own
- For additional regulatory compliance, you can get a dedicated Cloud-based Hardware Security Module (HSM)
- Configurable with Infrastructure as Code
- Compatible with most/all AWS data structures
- You define who/what is allowed to use the key -- BE STINGY!

Encryption in Transit

Certificates

- IAM
  - Bring your own certs (legacy)
- ACM
  - Public certs - Free!
    - Caveat: You don’t get access to the private key
    - Good for load balancers, API gateway, etc.
  - Private CA
    - Issue private certs
    - You keep the key
    - Cost is $400/mo + nominal cert fee

Identity/Access Management

IAM

- Protect the API by restricting/allowing accesses
- Tips for Good IAM
  - Avoid the demon * (least privilege FTW)
  - Use roles instead of users (eliminates credentials)
  - Permission with groups if you need to have users
  - Leverage CloudTrail to help identify proper permissions
  - Do it in code
    - Use a linter/nag
    - Have code reviews
    - Include your security people

Identity/Access Management

Security Policy

- Require MFA
- Enforce password complexity
- Enforce password expiration
- Rotate Keys
- Only grant console/API access as needed
- Least privilege

Root Account Protections

- Enable MFA (physical token)
- Never use it

Making things Public is OK

Just be aware... and careful!!!

Secrets Management

Remember: If someone has the password or key, encryption doesn't matter!

- Vaults
  - AWS Secrets Manager
  - Thycotic Secret Server
  - (Ansible, Hashicorp, *) Vault
- Parameter Stores
  - AWS Systems Manager (SSM)
- S3
  - Nothing preventing secrets there, but protection is harder
- Source code repository
  - JUST KIDDING! Never store secrets there...

Storage Architecture

General Tips for Protecting your Data

- Beware the Blast Radius
  - Production is Sacred
  - Go multi-account for a firmer barrier
- Protect your DR/Replication
- Sanitize your replication to lower environments
  - Automate this with Data Pipeline
- Athena is great! But...
  - Remember that the roles you give it should be cognizant of production access

Logging

CloudTrail

- You have to enable it
- Pay especially close attention to changes in KMS access

CloudWatch Logs

- Insights and Anomaly Detection can be useful in the right hands

SIEM

- If your security team has one, get your logs there!
- Consider getting one (and staffing it - MSSP?)
  - SaaS options abound
  - AWS Elasticsearch Service

What Could Go Wrong?

Github Oopsie

- New DevOps employee wants to be proactive and do some practice at home, so they commit their working branch to a public repo...
- They don’t comprehend that committing your SECRET key is a bad idea
- The next day, the employer’s account is a cryptocurrency mine!
- Bright side:
  - They didn’t destroy anything
  - DevOps guy kept his job and learned a valuable lesson
  - Showed the security team where their processes were deficient
- Takeaway:
  - Train your people which things are SECRET!
  - Monitor your repos (https://github.com/awslabs/git-secrets)

Too Permissive KMS Policy

(AKA “I made it work!”)

- Production KMS policy has this statement in it:

```
"Effect": "Allow",
"Action": "kms:Decrypt",
"Resource": "*"
```

- What could go wrong?
  - Non-prod application can improperly access prod data
  - Devs or other “shouldn’t be in prod” users can decrypt and see prod data
  - DevOps staff intending to change a test environment value with curated, well-written scripts could possibly affect production by accident

S3 Bucket Policy Silliness

“AWS had a breach”

- Administrator blows through all of the (increasing number of) warning flags and makes something publicly visible that shouldn’t be
- Totally avoidable, unforced errors…
- List of offenders is long and growing…
- Most informed people agree that this is ALWAYS user error, but some still blame AWS. ¯_(ツ)_/¯

ALPINE CYBER

Managed Security, Cloud & IT Services

www.alpinecyber.com

meetup.com/gpawsug

abington.psu.edu/ce-business-it/cybersecurity-fundamentals
berks.psu.edu/fundamentals-cybersecurity