Security Hardening for AWS Cloud Hosting

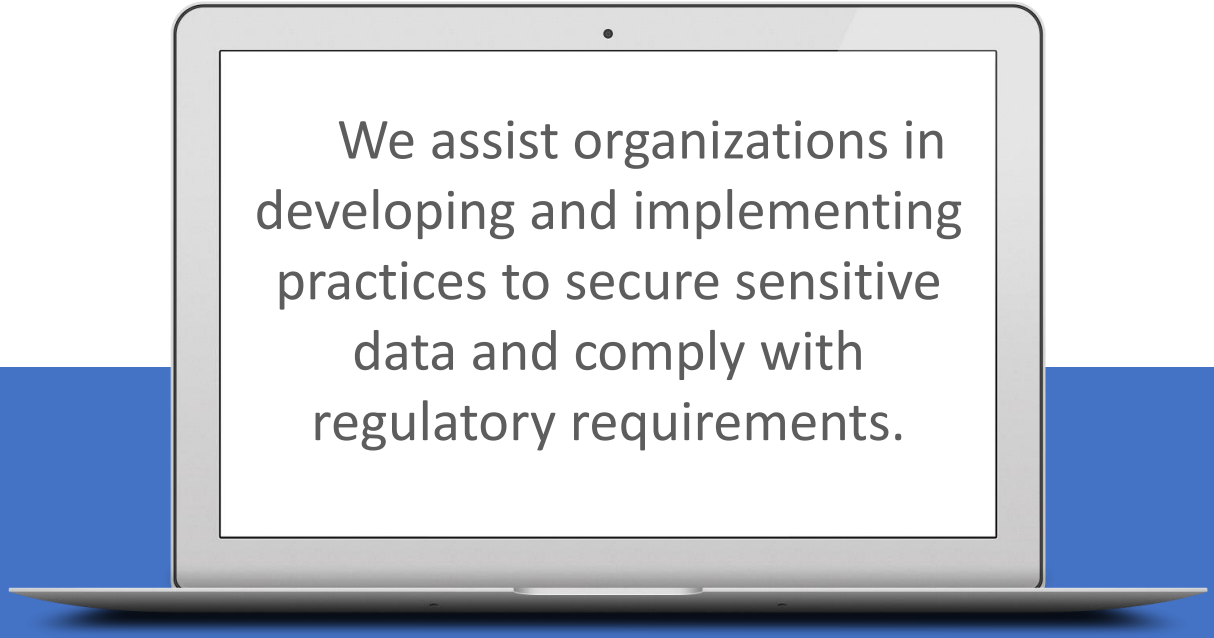
Nehal Trivedi
AWS Certified Solution Architect

databrackets
info@databrackets.com
866-276-8309

{databrackets
cybersecurity • audit • compliance}

WHO WE ARE …

databrackets
audit · compliance · certification



DIY TOOLKIT
DIY assessment, training, customized policies & procedures and much more …

CONSULTING
Professional services to help you with your Compliance needs

MANAGED SERVICES
Managed compliance and security services to focus on your key business outcome.

DISCLAIMER

Consult your attorney

databrackets
cybersecurity • audit • compliance

This webinar has been provided for educational and informational purposes only and is not intended and should not be construed to constitute legal advice.

Please consult your attorneys in connection with any fact-specific situation under federal law and the applicable state or local laws that may impose additional obligations on you and your company.

ALL WEBINARS ARE RECORDED AND AVAILABLE AS AN "ON DEMAND" SUBSCRIPTION

Nehal Trivedi

AWS Solution Architect

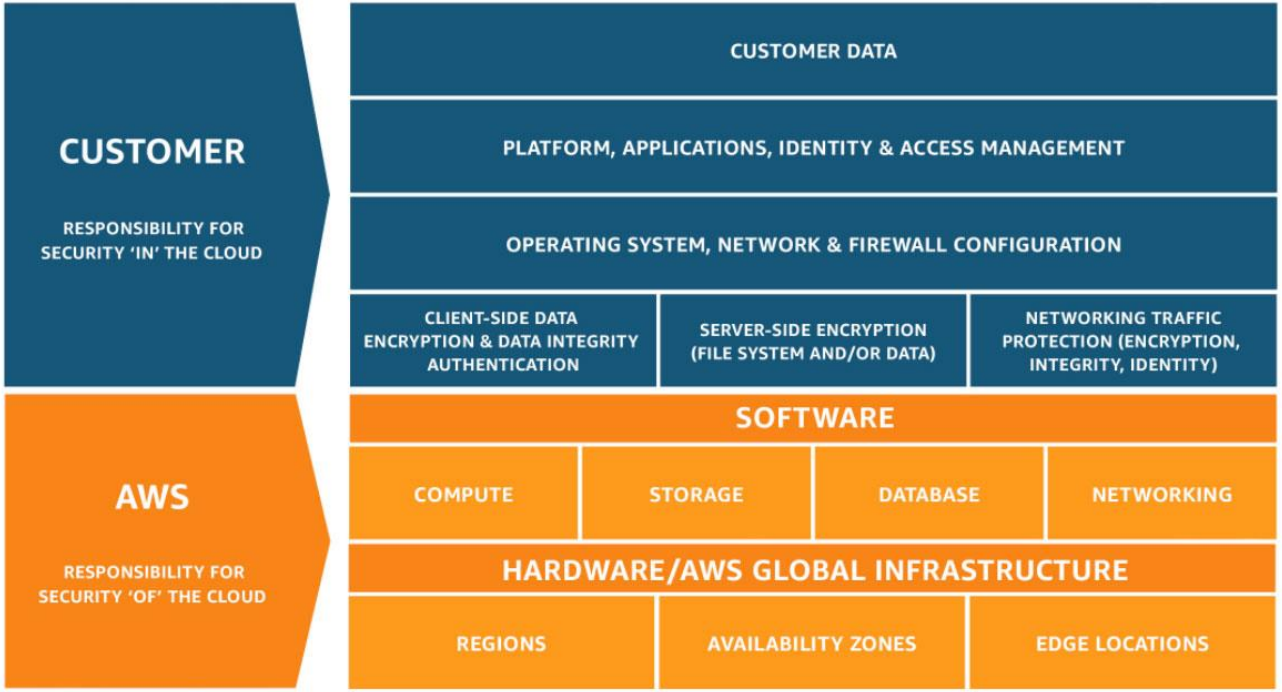
President, Innogile

Nehal's Background

Nehal has been solving complex business problems using software for nearly two decades and loves what he does. He has experience with Healthcare, Financials, Pharma, Manufacturing, Publishing and Non-Profit to name a few. Nehal helps us with cloud and software best practices, picking things apart and putting them together again.

AWS Shared Responsibility Model

infrastructure services



- Inherited Controls
  - Physical & Env.
- Shared Controls
  - Patch
  - Configuration
  - Training
- Customer Specific
  - Zone Security
  - Service protection

Customer responsibility will be determined by the AWS Cloud services that a customer selects.

AWS Shared Responsibility Model

application stack

databrackets
cybersecurity • audit • compliance

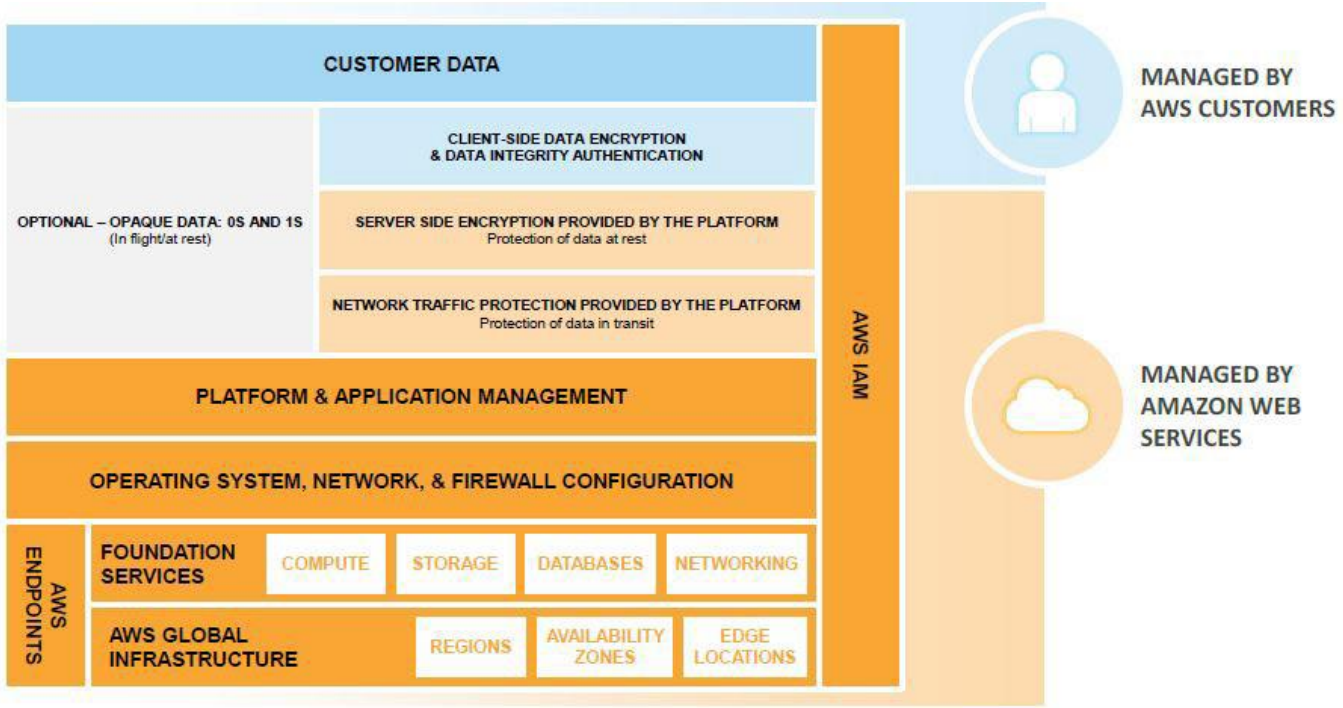
	Customer Data			
Customer	Identity & Access Management / Firewall Configuration (Security Groups)			
	Client-side Data Encryption & Data Integrity Authentication	Server-side Encryption (File System and/or Data)	Network Traffic Protection (Encryption, Integrity, Identity)	
	Platform & Application Management / Operating System & Network Configuration			
AWS	AWS Foundation Services			
	Compute	Storage	Database	Networking
	AWS Global Infrastructure			
	Regions	Availability Zones	Edge Locations	

Resource Access Policy

Customer responsibility will be determined by the AWS Cloud services that a customer selects.

AWS Shared Responsibility Model

abstracted services



Customer responsibility will be determined by the AWS Cloud services that a customer selects.

AWS Infrastructure Design

{databrackets
cybersecurity • audit • compliance

IAM Services
- Console Access
- Programmatic Access
  - Least privileges
  - Security Credentials
  - 2FA
    - Hard token
    - Soft token
  - Permissions or Policies

AWS Organizations

Regions/Availability Zones
- High Availability/DR
- *AWS Cloudfront*

Define and Categorize Assets

databrackets
cybersecurity • audit • compliance

Required for Compliance Management

- HIPAA, GDPR, CCPA and NIST Framework
- Inventory and Data Management

- ARN - Amazon Resource Names

arn:aws:clouddirectory:us-west2:accountId:schema/development/SchemaName

- Resource Tags - Name, Purpose, etc.

arn:aws:clouddirectory:us-west-2:12345678910:directory/ARIqk1HD-UjdtmcIrJHEvPI

Name, Owner, Project, BillingDept

- AWS Config

Secure Data

databrackets
cybersecurity • audit • compliance

Encryption

- Protecting data-at-rest on various AWS services
  - KMS for storing and retrieving data
    - Block storage, S3, Databases, Filesystems

- Protecting data-in-transit on various AWS services
  - TLS/SSL encryption SHA-256
    - Using ACM to manage TLS Certs, attach them to ELBs, Cloudfront

Encryption needs to be enabled for all sensitive data

Secure Operating System & Applications

databrackets
cybersecurity • audit • compliance

Network

- VPC, VPN, Security Groups

Operating System

- Harden AMIs
- Manage Patches
- Use Storage Encryption By default
  - EBS Encryption and S3 Encryption

Avoid mitigating Compromise & Abuse

Secure your Infrastructure

{databrackets
cybersecurity • audit • compliance

VPC
- VPN
- Inspector
- Security Zoning and Segmentation

Public-facing Application
- Protect using AWS Shield and WAF
- Certificate Manager

Enable Cloudwatch logs for resource access

Continuous Threat Detection - GuardDuty

Summary

databrackets
cybersecurity • audit • compliance

- Shared responsibility model drives cloud effectiveness
- Whenever possible use AWS managed services
- Pay attention to Service Level Agreement (SLA)
  - Ephemeral vs. persistence data
- Use least privilege access
- Logs are critical, so enable and monitor them

Resources

databrackets
cybersecurity • audit • compliance

- ❑ AWS Security Best Practices
- ❑ AWS Security Blog
- ❑ Multi-Factor Authentication
- ❑ Security, Identity and Compliance on AWS

13

Next Steps

Contact us for free no-obligation evaluation and quote

866-276 8309 or info@databrackets.com

14

UPCOMING EVENTS

databrackets
cybersecurity • audit • compliance

- Security Hardening of Azure Cloud Hosting – April 16, 2020

Register now >> https://databrackets.com/events/

15

FIND US

databrackets
cybersecurity • audit • compliance

CALL US
866-276 8309

SERVICE
info@databrackets.com

LOCATION
150, Cornerstone Dr.
Cary, NC

SOCIALIZE
Facebook
Twitter

Twitter: @databrackets

Facebook: databrackets

databrackets
cybersecurity • audit • compliance

Questions

Please don’t hesitate to ask

databrackets
cybersecurity • audit • compliance

Thank You

for your attention!

databrackets
cybersecurity • audit • compliance

To purchase reprints of this document, please email info@databrackets.com.

Thank you for joining us today

05 March 2020