Launching a Highly-regulated Startup in the Cloud

Poornaprajna Udupi (@poornaudupi)
Starting in the Cloud

86% by 2020

Cisco Global Cloud Index: Forecast and Methodology, 2015–2020
Building blocks, Cost, Scalability

Compute  Networking  Storage  Database  Monitoring  Alarm  Notifications  Deployments  Access Control  Key Management

Data Pipeline  Search  User Management  Device Farm  Gaming  IoT  Machine Learning

SANS Cloud Security Summit 2017
Lean, Agile, Scrappy Disruptor

Experiment

Iterate

MVP

Growth
Security Questionnaire
We use HTTPS
We use AWS
Military-grade encryption

Compliance Report: Here is AWS SOC2 report
Incident Management: Never happened so far, Yet to experience a security incident
Disaster Recovery: 99.95% uptime - from EC2 SLA, Enterprise-grade SLA
Vulnerability Management: We use Sophos Anti Virus
Risk Assessment: Free Qualys Scan Report
Coming of Age

Security whitepaper
Self Assessment

Client Assessment
Security

Guidelines

Compliance

Standardized Assessments
Guidelines

Security

Compliance

http://smartfaststartup.com/2011/09/20/how-to-become-a-must-have/
About Me: Poornaprajna Udupi (@poornaudupi)

- MS (CS), UCSD(2003)
- SW Engg., Sun(2010), Netflix(2012)
- Founder, Bitplanet(2015)
- CISO, LyraHealth(Present)
- Advisor, EmpInfo(Present)
Data Protection

Data Classification
- Scope
- Sensitivity
- AWS Tags

Encryption
- Storage
  - Application (multi tenant)
  - Amazon KMS, Azure Key Vault
  - Confidant (by Lyft)

Backup & Recovery
- Periodic snapshots
- Periodic backups
- Server snapshots
- AWS RDS, AWS AMI snapshots, Azure SQL Database

Data Loss Prevention
- Alerts
- Monitoring
  - AWS CloudWatch, Google Compute StackDriver
  - Monitoring

Network Access

Segregation
Based on data classification
AWS Virtual Private Cloud, Azure Virtual Network

Microservice Access
Subnets
NAT Gateway
Security Groups
Role based access

Application Access
Allow port 443 only

Employee Access
Virtual Private Network (VPN) Tunnel only
SSH required
WiFi, Network requirements
Endpoints

Mobile Device Management

- Installed applications
- Accessible data
- Disk encryption,
- Firewall
- Best practices (screen lock, password)
- JAMF Cloud for Apple Macs, iPhones, iPads,
  - Microsoft Intune for PCs, Windows mobile,
  - Google MDM for Androids

Anti Virus, Anti Malware

Removable Media

- Forbid.
- By Exception.
- Allow auditable transmission of data only.
Access Control

Minimum Necessary, Least Privilege

Administrators

Cross-account access

Role-based access

Groups

AWS Security Policies, AWS Identity and Access Manager, Azure Active Directory, Google Cloud IAM

Bless (by Netflix)
Audit, Logging & Monitoring

System Activities (create, read, update, delete) and Admin activities

- Application
- Servers
- Database
- Network

Report, Monitor and Audit periodically

- AWS CloudTrail, AWS CloudWatch, AWS VPC Flow Logs, Azure Application Insights, Azure Operational Insights, Google StackDriver Monitoring

- Security Monkey (by Netflix), ElastAlert (by Yelp), ElasticSearch (by Elastic)
Configure for best practices

Password Management

Single Sign On
Multi-factor
Strength
Reuse
AWS IAM, Google Cloud IAM, Azure Active Directory

Managed updates

Vulnerability management
Patching level
Time
Red/black
AWS ElasticBeanstalk, Azure CloudServices, Azure Websites and Apps, Google App Engine

Real time guidance on security, performance, cost, fault tolerance

AWS Trusted Advisor, AWS Config
Security Monkey (by Netflix), DbDat (by foospidy)
Organizational Maturity

Physical and Environmental Security

- Lean on the clouds
- No local data storage & processing
- Visitor logs and system Changes
- Network access requirements

Vulnerability Management

- Up to date inventory of assets: servers, workstations, portable devices, software
- Up to date with vendor software
- Handling zero-day vulnerabilities
- AWS Config, JAMF, Google MDM, Microsoft Intune

Third-Party Risk Assessment

- Contractual guarantees
- Xfer compliance requirements
- Minimum required data sets, access
- Monitor SLAs

Incident Response

- Up to date procedures for handling incidents
- Organizational Structure for handlers and communicators
Organizational Maturity

Disaster Recovery & Business Continuity
- Up to date procedure to start from scratch
- Organizational Structure for handlers
- Recovery Time Objective
- Recovery Point Objective

Risk Management
- Know the risks and manage them
- Likelihood and Impact analysis
- Outsourcing (e.g. Business Associate Agreement)

Secure SDLC
- Secure coding practices
- Code reviews, OWASP Top 10
- Issue tracking, Change Management
- findbugs, find-sec-bugs

Education, Training and Awareness
- US-CERT
- SANS Newsletters
- Training
- Cybrary, Coursera, Udemy
Launching a Highly-regulated Startup in the Cloud

Poornaprajna Udupi (@poornaudupi)