ACHIEVING PCI COMPLIANCE

Best Practices working with your Cloud Provider

Matthew Heap, Head of Solution Architecture

WHAT IS PCI-DSS

It's a Data Security Standard that applies to all entities that store, process, and/or transmit cardholder data. It covers technical and operational system components included in or connected to cardholder data.

There are three ongoing steps

Assess - identifying all locations of cardholder data, taking an inventory of your IT assets and business processes for payment card processing and analyzing them for vulnerabilities that could expose cardholder data.

Repair - fixing identified vulnerabilities, securely removing any unnecessary cardholder data storage, and implementing secure business processes.

Report - documenting assessment and remediation details, and submitting compliance reports to the acquiring bank and card brands you do business with.

PCI DATA SECURITY STANDARD – High Level Overview

Build and Maintain a Secure Network and Systems	**1**	Install and maintain a firewall configuration to protect cardholder data
	2	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3**	Protect stored cardholder data
	4	Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5**	Protect all systems against malware and regularly update anti-virus software or programs
	6	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7**	Restrict access to cardholder data by business need to know
	8	Identify and authenticate access to system components
	9	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10**	Track and monitor all access to network resources and cardholder data
	11	Regularly test security systems and processes
Maintain an Information Security Policy	**12**	Maintain a policy that addresses information security for all personnel

SHORT HISTORY OF PCI-DSS

Pre-2001 – e-commerce relatively small - but breaches start to be detected ($1.5bill in 2001)

2001-04 – Each CC provide tries to go it alone

Introduced in Dec 2004 - 1.0 – Backed 5 Major CC providers

6 months later – 1st time to be compliant (many fail)

1.1 released in Sep' 2006 – Add WAF / Code review requirement

2007 – Concerns about QSA's, difficulty to comply, costs to comply

2008 – PA-DSS Application Standards to help ISVs

1.2 released – Big change to WIFI controls - millions of $$ to fix

2.0 No huge changes (add Virtualization guidance quickly after)

3.0 release in Oct'2013

All 3.2 Controls must be in place by Feb'2018

WHAT HAPPENS WHEN THINGS GO WRONG

1984 **TRW** – **90** mill peoples credit data

2006 **TJX** – **94** mill CC no. exposed

2008 **Heartland System 134** million CC lost (not discovered for 10 months)

2011 **Sony** – 12 mil CC lost – 1st large publicized global breach

2013 **Target** – **110** million CC lost

2013 **Adobe** - **150** mill CC lost

2014 **Home Depot** – 56 mill CC lost

Jul'2017 Equifax – 200k CC lost and growing (effected **~45%** of US citizen)

Date of disclosure very different that the original breach

KNOW YOUR DOCS (YOU & YOUR VENDORS)

PCI-DSS Requirements and Security Assessment Produces (169 pages)

The actual Standard to comply to

AOC - Attestations of Compliance

Summary of Scope / Locations / Dates / Refers to the ROC

ROC - Report on Compliance

Detailed report on how the organization meets the PCI-DSS

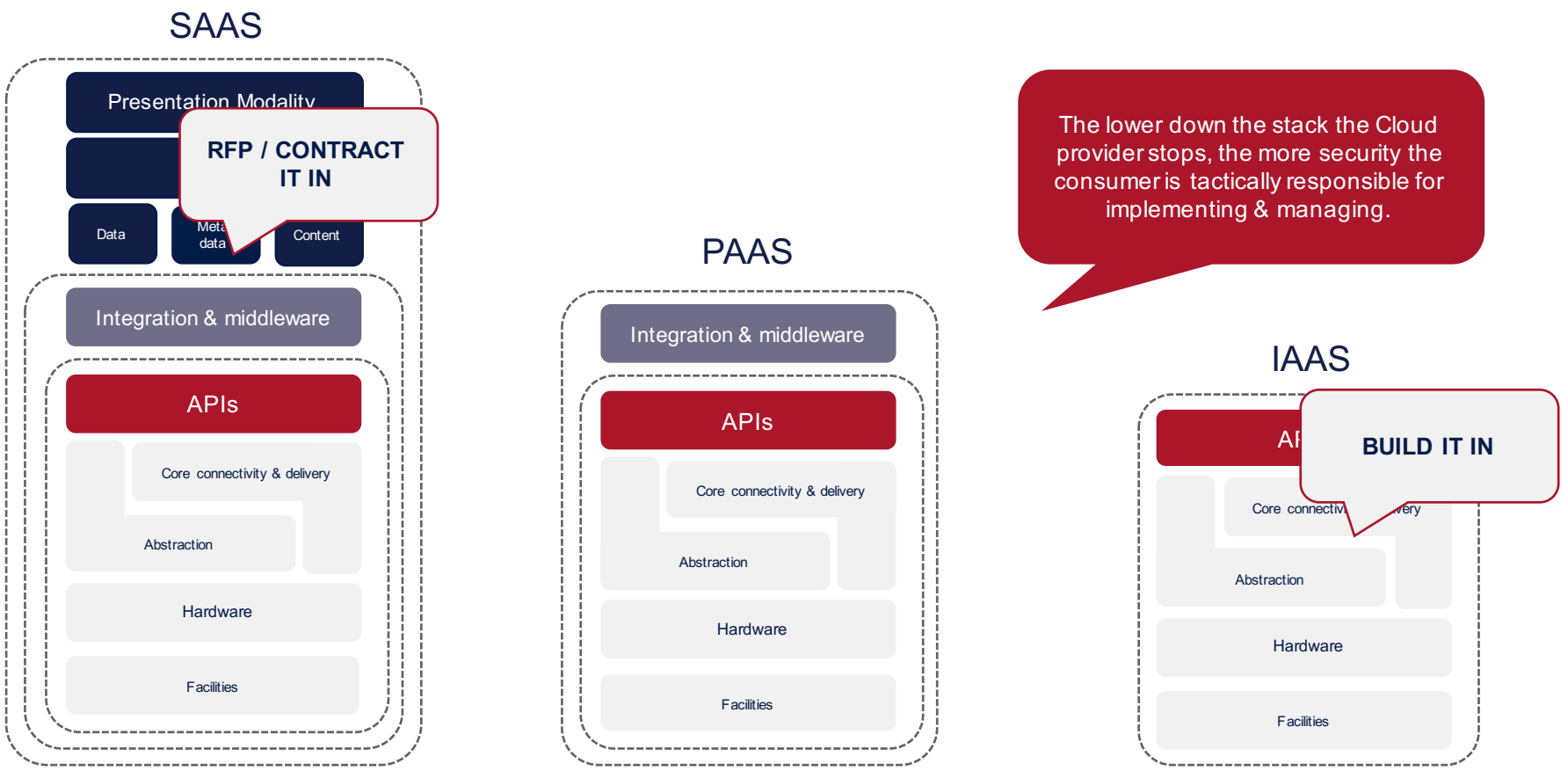
SAQ – Self Assessment Questionnaire – Aimed at small vendors

Platform Risks & Best Practices

CLOUD COMPLIANCE

In a perfect world there would be a SaaS for every business function you need, customized precisely how you need it, that you trusted and complied with all regulations. Life would be easy.

AS-A-SERVICE DIFFERENTIATION



WHAT IS THE SCOPE OF YOUR VENDOR

So as PCI-DSS reports occurs on an annual basis, certain things will be missing from the scope

- New services (Azures release 2 new features a day)
- New locations (AWS's 2018 Hong Kong Region)

This doesn't mean the service cannot be compliant, but there is no evidence for a QSA to assess from the vendor to show that it is.

Understand how they reply to important questions – Common response is

Cloud Vendor X is Service Provider that does not directly store, transmit or process any CHD.

Requirement 3.4 is the likely the trickiest by customers / vendors – talk to your QSA

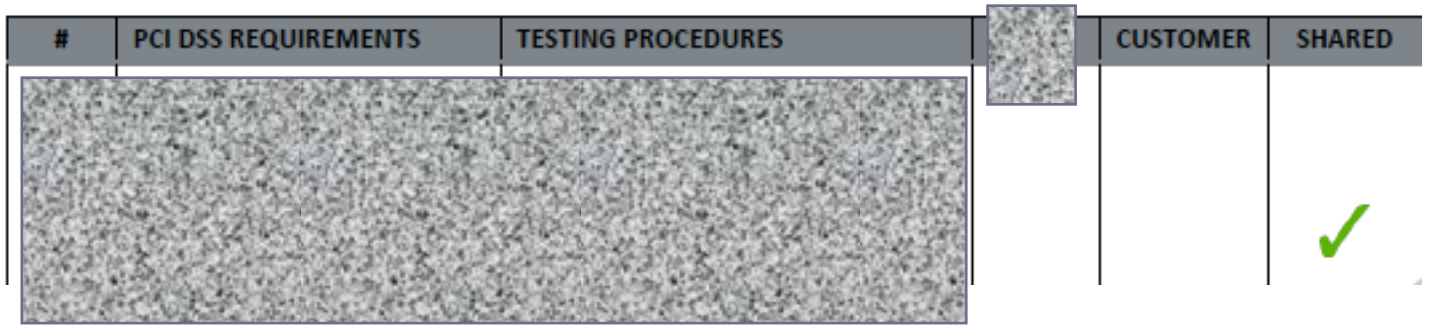
WHAT IS YOUR RESPONSILBITY

Certain controls will be 100% your will company responsible - Application Coding

Some controls will be 100% Cloud Provider – Physical Security of Cloud ‘DC’ (AZ or Region)

Some will be shared such as PaaS, Cloud Provider will be responsible for generating logs from the PaaS, Customer would be responsible to review and action them

Review documents closely – As your QSA will know these requirements very well.

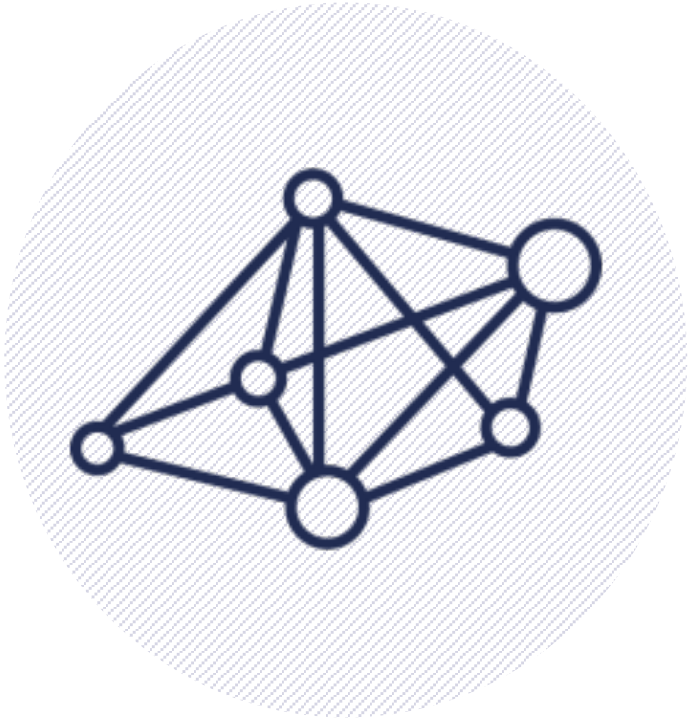


VENDOR MANAGEMENT

- Inherited compliance and certifications
  - Scope matters

Not only PCI concerns

- Indemnification and Liability Limits
  - Differ amongst hyper-scalers
- Privacy (NDA, privacy policies)
- Data storage & data sovereignty (DPA, Privacy Shield)



SHARED RESPONSIBILITY MODEL

CUSTOMERS

CUSTOMER CONTENT

Platform, Applications, Identity & Access Management

Operating System, Network & Firewall Configuration

Client-side Data Encryption | Server-side Data Encryption | Network Traffic Protection

Customers are responsible for their security and compliance **IN** the Cloud

FOUNDATION SERVICES

Compute | Storage | Database | Networking

GLOBAL INFRASTRUCTURE

Availability Zones

Regions

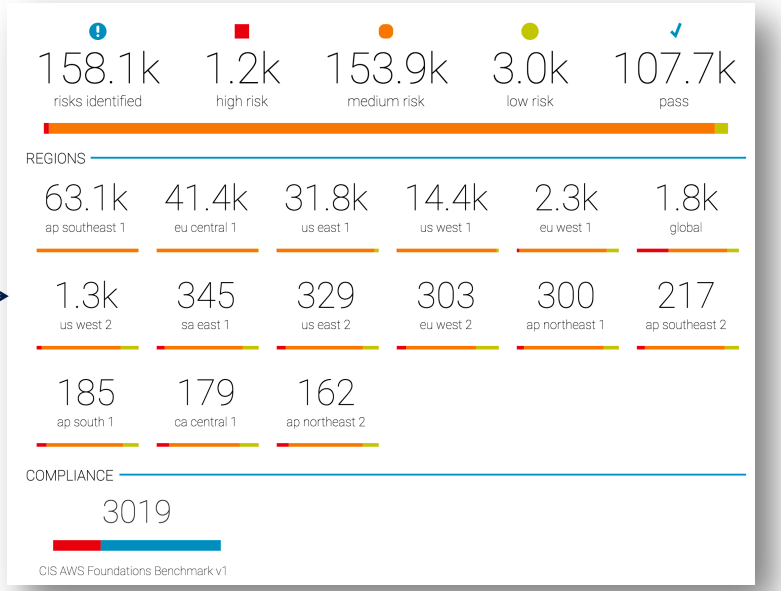
Edge Locations

AWS is responsible for the security **OF** the Cloud

DATAPIPE

PLATFORM SECURITY SETTINGS

Numerous user controllable options governing cloud security. Define a corporate policy around appropriate settings, and ideally leverage tools which automatically check and report on a continual basis.



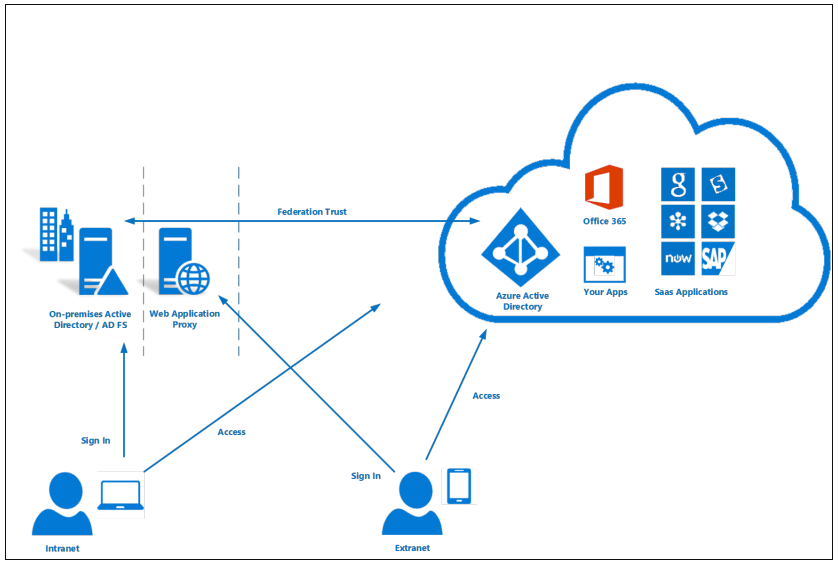
USER SECURITY SETTINGS

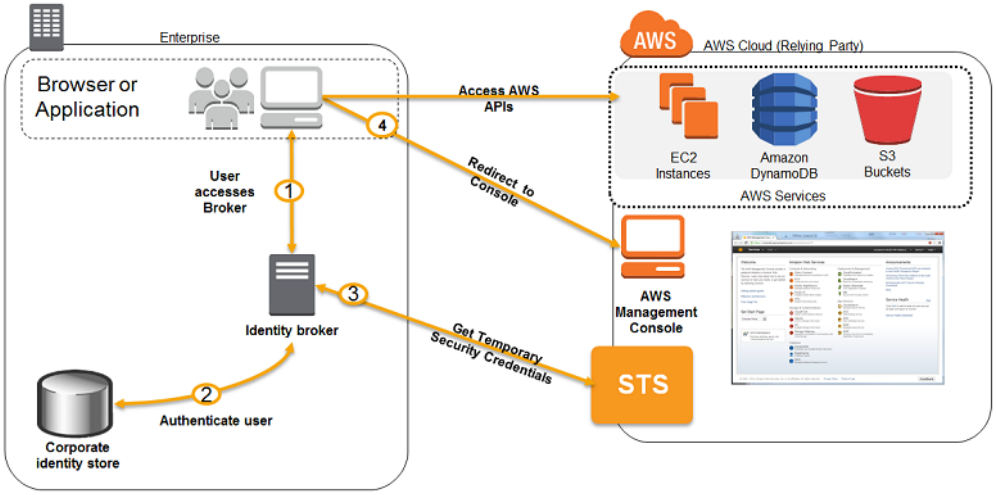
- Root account
- Root API
- Password Policy
- MFA
- VPC
- Encryption
- Insecure SGs / NACLs
- IAM Policies
- Object Storage Permissions

IDENTITY AND FEDERATION

External identity management provides:

- ✓ Unified identity for cloud and on premise users
- ✓ Integration into existing starters/leavers process
- ✓ Integration into corporate RBAC process (map to Roles)
- ✓ Sign-Sign On (MFA, UBA, etc..)





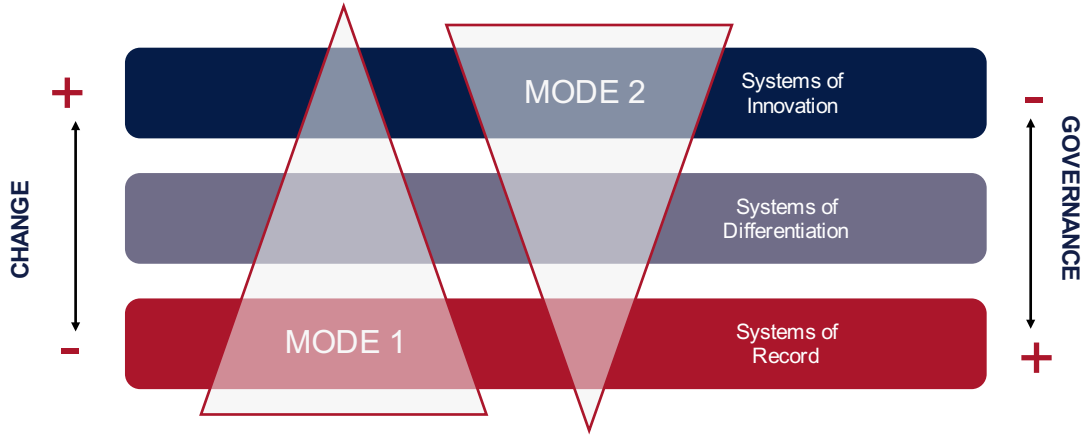
INFRASTRUCTURE MATURITY

STEADY STATE DATACENTER

- Generally labeled as ‘Mode 1’
- Slowly changing applications with larger sets of changes per deployment
- Less time-critical, business-focused need to change
- Often seen in back-office applications

HIGH-VELOCITY CLOUD DEPLOYMENTS

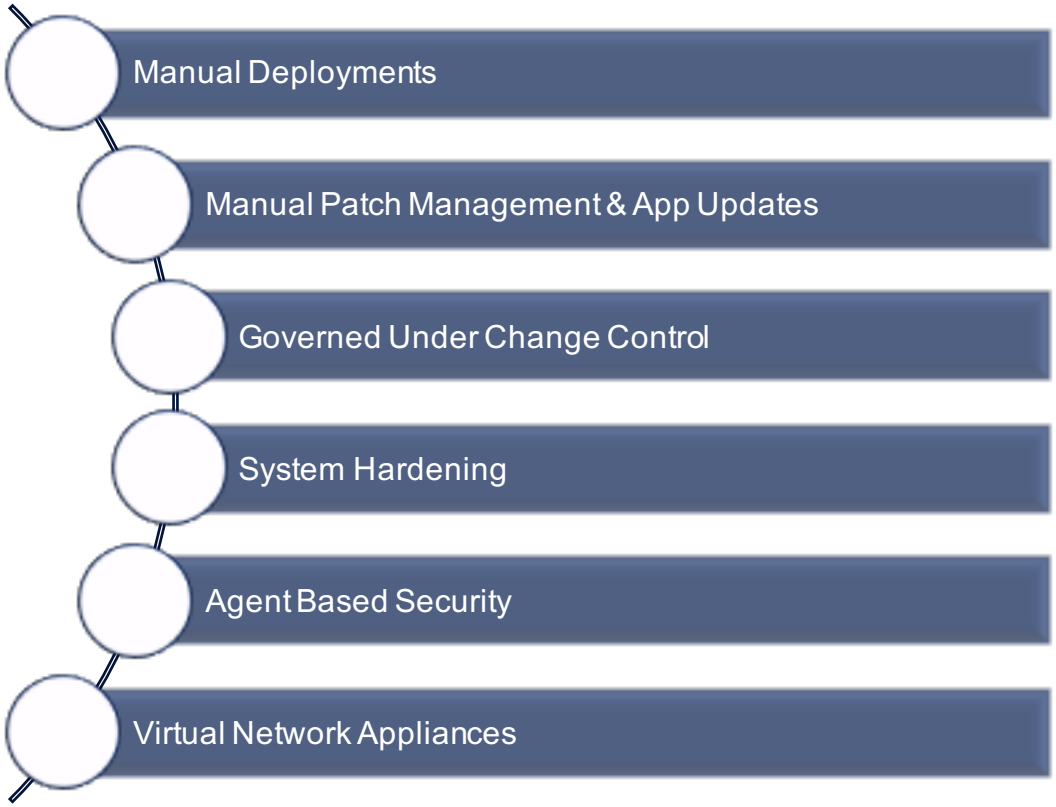
- Generally labeled as ‘Mode 2’
- Also labeled as ‘DevOps’ in popular press
- Key feature is smaller, more rapid deployments driven by need to provide direct business value
- Often necessary due to competitive landscape in a line of business



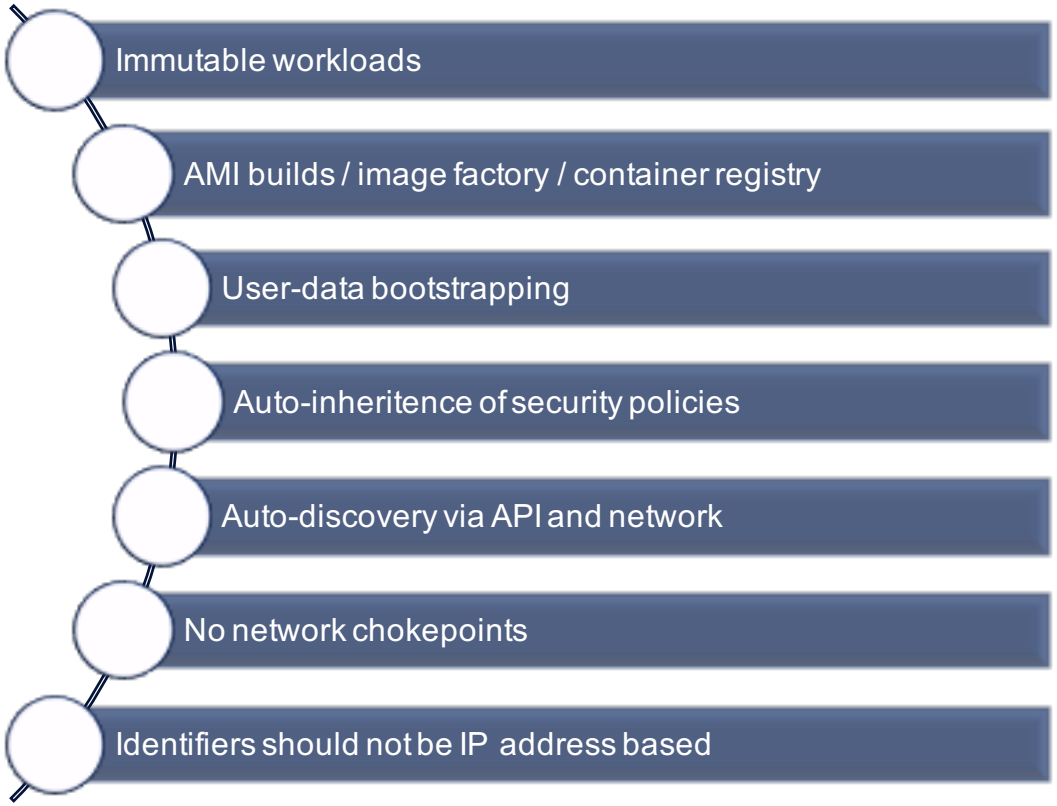
Gartner

DATAPIPE

MODE 1: SECURITY



MODE 2: SECURITY



NATIVE OR BRING YOUR OWN

Key / Encryption Management

- Platform / Customer Managed Keys
- IAM Integration vs. Separate Identities
- HSM

Network Management

- Scale or visibility?
- Centralized vs. distributed control

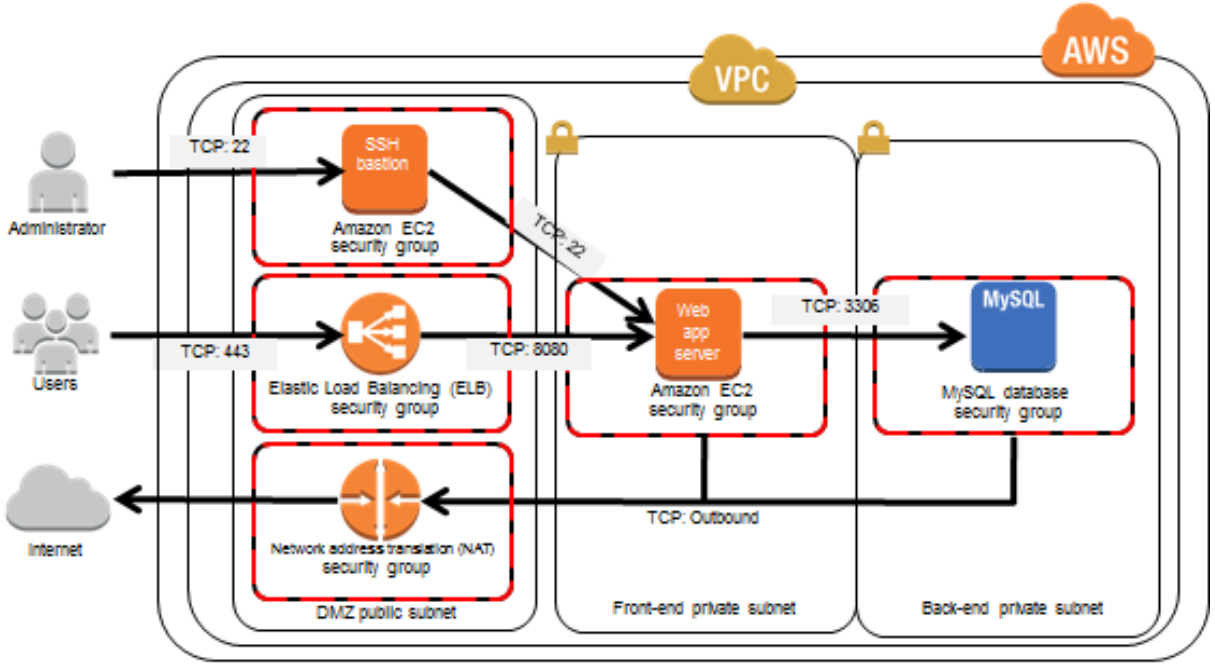
DATAPIPE

GOVERNANCE

- Tagging
- Account & VPC segregation
- Continuous Integration / Continuous Deployment
- Cloud Access Security Broker (CASB)
  - SaaS encryption, User Behavior Analytics / Compromised Credentials, Data Leak Protection

ARCHITECTURAL PATTERNS

- ✓ Management VPC
- ✓ Bastion Hosts
- ✓ NACLs & Security Groups
- ✓ VPN



WHY USE DATAPIPE FOR YOUR PCI NEEDS

- Compliant level 1 Service Provider since 2004
- SOC staffed globally inc 3 staff in Hong Kong (Cantonese & Mandarin)
- Audited annually by a Qualified Security Assessor (QSA)
- Achieved PCI DSS 3.0 validation in December 2014
- Participating Organization in the Security Standards Council
- PCI compliance package is supported on public and private clouds, dedicated server(s) and hybrid solutions.
- Internal Security Assessor (ISA) certified staff
- Turn-key suite of audited and validated security controls.
- PCI Schedule that clearly defines entity responsibilities (PCI Responsibility Matrix)
- PCI Community Cloud available exclusively to PCI clients

SECURITY SERVICES FOCUSED ON CONTINOUS COMPLIANCE

Global Security Operations Center (SOC)

- Continuous Audit — tripwire
- Data Encryption — Vormetric
- Patch Management — IBM Tivoli software
- Event Management — ALERT LOGIC
- Two-Factor Authentication — DATAPIPE
- Firewall & VPN — FORTYCLOUD MAKE YOUR PUBLIC CLOUD PRIVATE
- Web Application Firewall — Incapsula
- Intrusion Detection Services — ALERT LOGIC
- Vulnerability Management — RAPID7
- Firewall Review — Dome9 SECURITY
- DAC – Datapipe Access Control — DATAPIPE
- Continuous Compliance — evident.io
- Anti-Malware / Virus — eset, TREND MICRO

- Each Service contractually maps back to a required PCI-DSS requirement
- Ensuring ongoing responsibility from both parties for ongoing compliance
- Our goal is not just to meet the requirements dictated by PCI (or any other body HKMA, SFC), but to ensure a compliance record that reaffirms the security and integrity of your organization.

FURTHER READING

CLOUD SECURITY ALLIANCE

Security Guidance for Critical Areas of Focus in Cloud Computing
CSA Security, Trust & Assurance Registry (STAR)
Cloud Controls Matrix (CCM)
Consensus Assessments Initiative Questionnaire (CAIQ)

AWS

- Introduction to AWS Security
- Introduction to AWS Security Processes
- Security Best Practices
- AWS Security Checklist
- Well Architected Framework – Security Pillar
- Many more…

ALIBABA

Cloud Security Whitepaper

AZURE

- Network Security Best Practices
- Data security and encryption best practices
- Identity management and access control security best practices
- IaaS Security Best Practices
- Many more…

THANK YOU FOR LISTENING

ANY QUESTIONS?