Security and Compliance in the Cloud

BARR
ADVISORY

Today's Agenda

- → Cloud Updates and Trends
- → Industry Regulations and Framework Application
- → Key Risks and Controls
- → Protecting AWS Workloads
- → Q & A throughout

BARR ADVISORY

BARR’s MISSION

To simplify the path
to security and compliance
for a more secure world.

BARR's CLIENTS

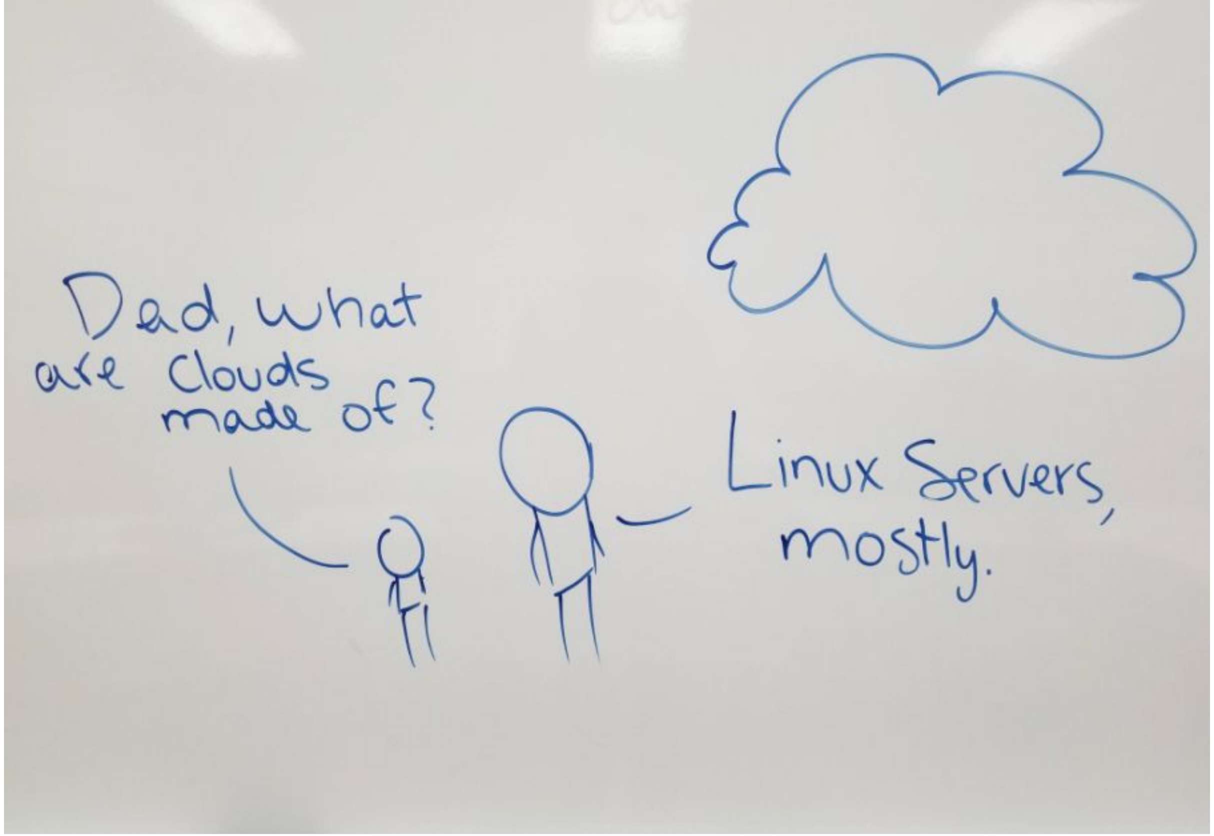
We serve innovative technology companies and cloud service providers.

BARR Advisory Services

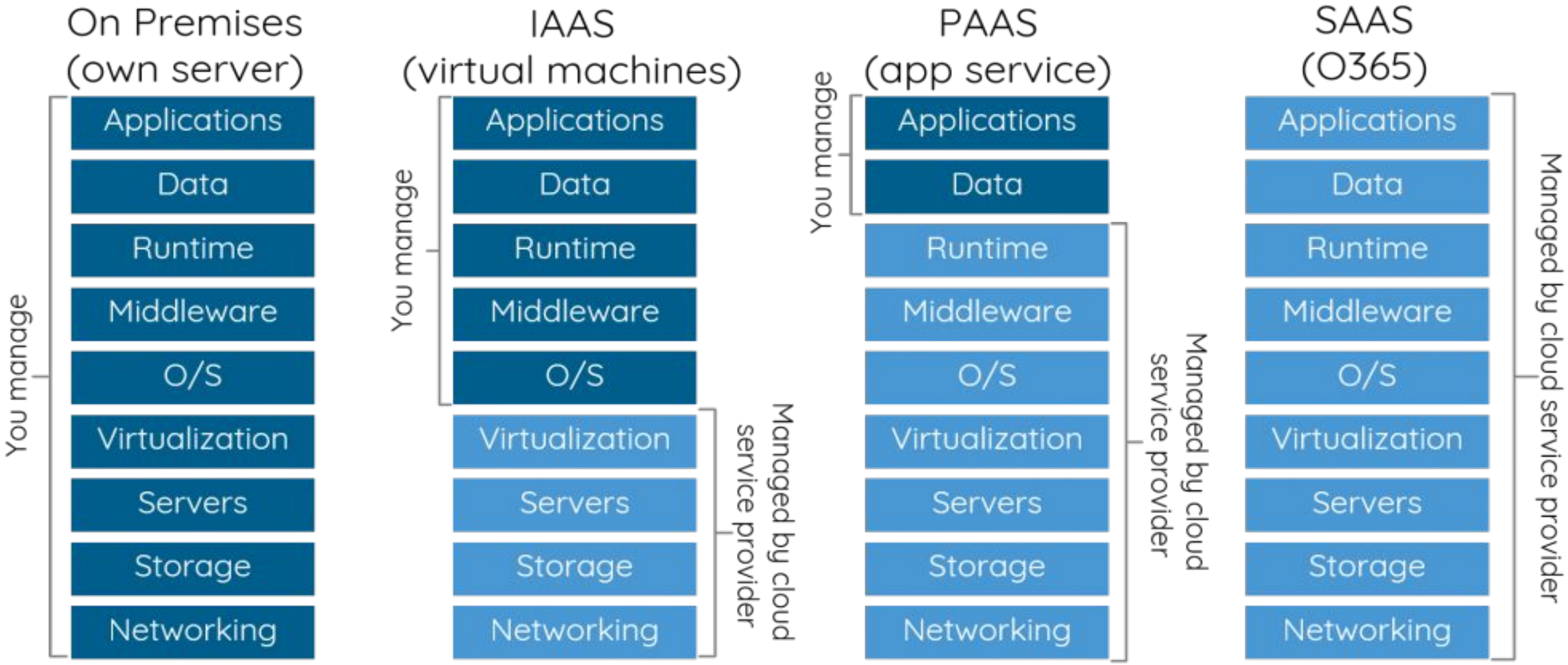
- ✓ **SOC Examinations** [SOC 1, SOC 2, SOC 3, SOC for Cybersecurity]
- ✓ **Healthcare Compliance** [HIPAA/HITECH, HITRUST]
- ✓ **Certification to ISO** [ISO 27001, 27017, 27018]
- ✓ **Government Assessments** [FedRAMP, DFARS, NIST 800-53]
- ~~✓~~ **PCI Compliance**
- ~~✓~~ **Penetration Testing**
- ✓ **IT Governance, Risk, and Compliance**
- ✓ **Virtual CISO Services**

Cloud Updates and Trends

Cloud Models



Cloud Models — Who is *responsible* for what?



On Premises (own server)

You manage

- Applications
- Data
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

IAAS (virtual machines)

You manage

- Applications
- Data
- Runtime
- Middleware
- O/S

Managed by cloud service provider

- Virtualization
- Servers
- Storage
- Networking

PAAS (app service)

You manage

- Applications
- Data

Managed by cloud service provider

- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

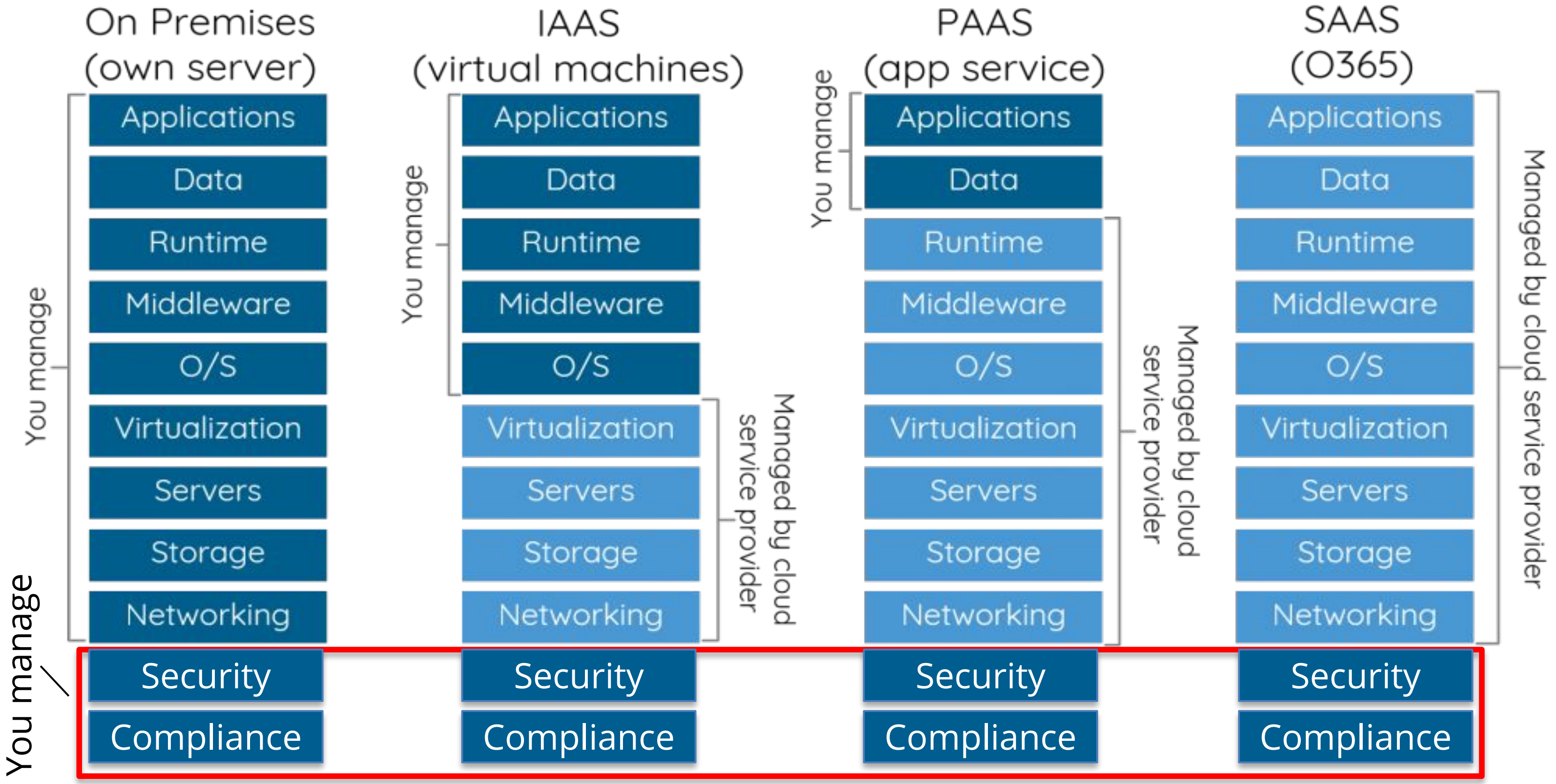
SAAS (O365)

Managed by cloud service provider

- Applications
- Data
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

Source: Multiple; http://cloudonmove.com/iaas-paas-saas-what-do-they-mean/

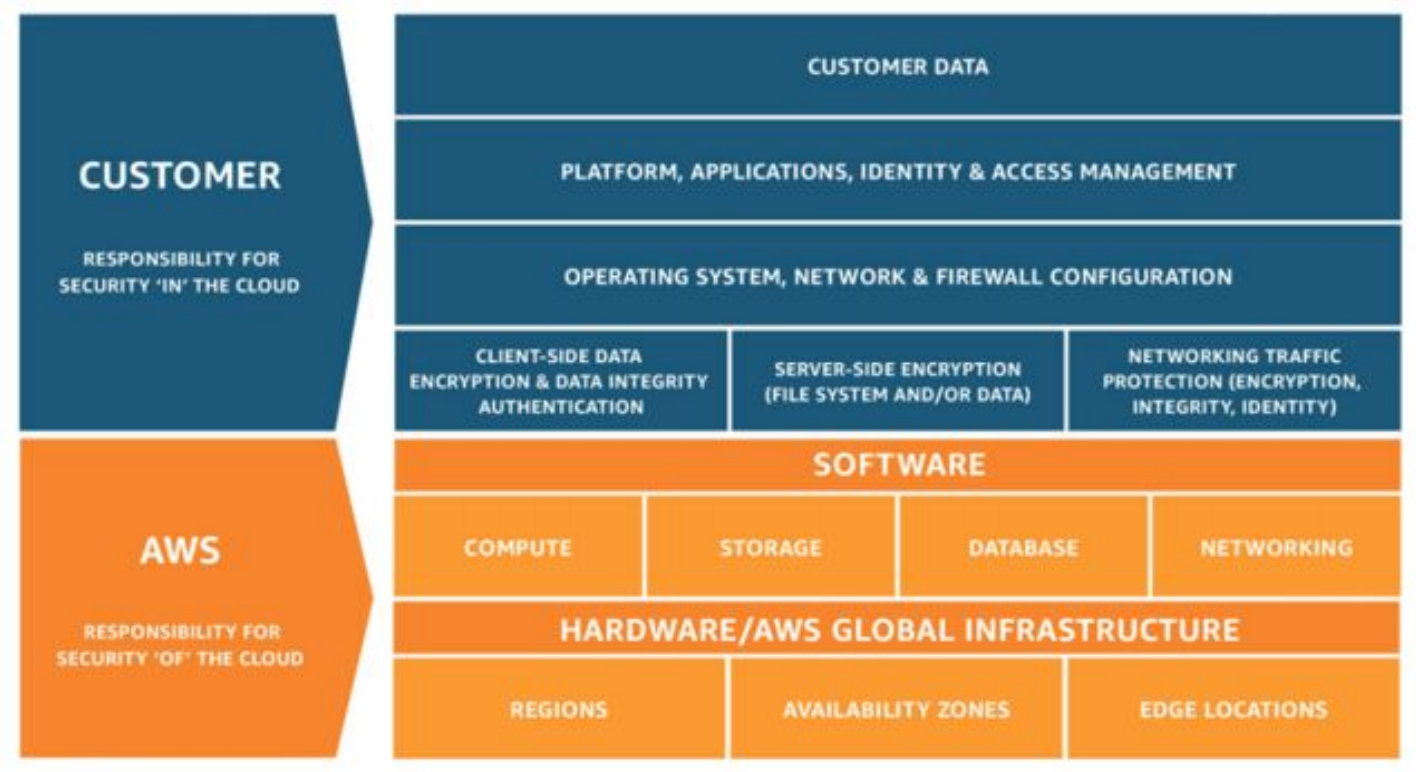
Cloud Models — Who is *accountable* for what?



On Premises (own server)	IAAS (virtual machines)	PAAS (app service)	SAAS (O365)
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking
Security	Security	Security	Security
Compliance	Compliance	Compliance	Compliance

You manage
You manage
Managed by cloud service provider
You manage
Managed by cloud service provider
Managed by cloud service provider
You manage

Shared Responsibility Model — AWS



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

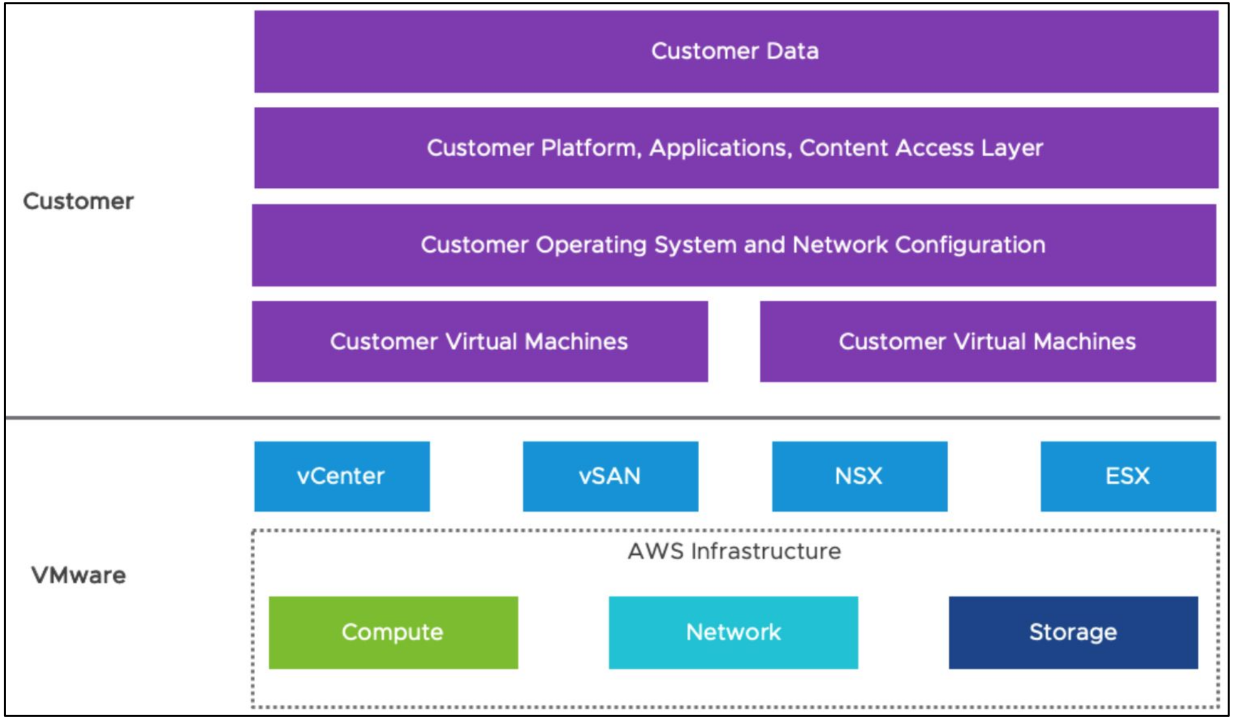
COMPUTE	STORAGE	DATABASE	NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS	AVAILABILITY ZONES	EDGE LOCATIONS

Source: https://aws.amazon.com/compliance/shared-responsibility-model/

Shared Responsibility Model — VMware Cloud on AWS



Customer

Customer Data

Customer Platform, Applications, Content Access Layer

Customer Operating System and Network Configuration

Customer Virtual Machines

Customer Virtual Machines

VMware

vCenter

vSAN

NSX

ESX

AWS Infrastructure

Compute

Network

Storage

Source:https://docs.vmware.com/en/VMware-Cloud-on-AWS/solutions/VMware-Cloud-on-AWS.39646badb412ba21bd6770ef62ae00a2/GUID-31CC90E5EB22075B2313FA674D567F2A.html

Knowledge Check #1

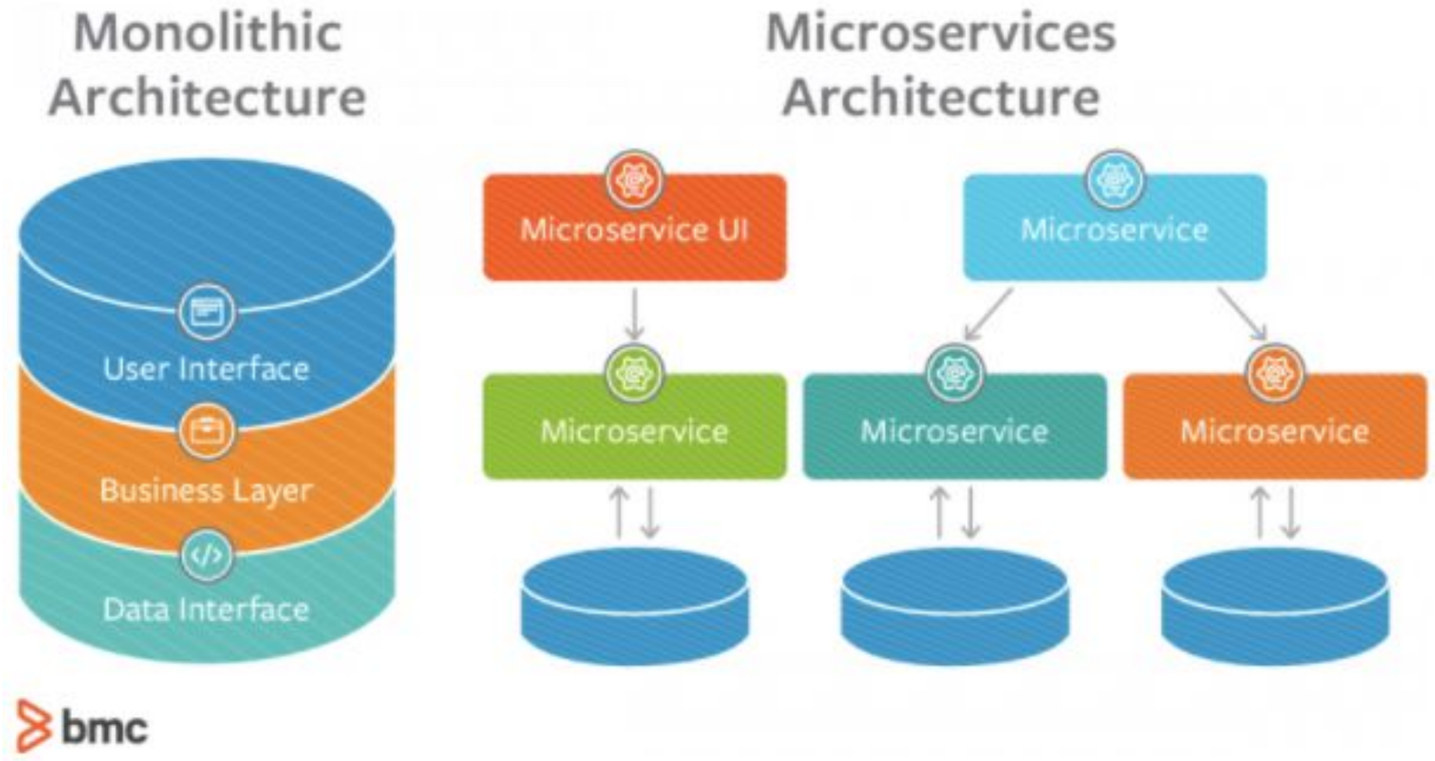
History of the Cloud — Is history repeating itself?

- 1950s Mainframes (“Time-Sharing”)
- 1960s “Intergalactic Computer Network”
- 1970s UNIX Era and opensource
- 1980s PC Era
- 1990s Distributed Computing Environment
- 1999 Salesforce (applications over the Internet)
- 2006 Elastic compute cloud (EC2)
- 2009 Web 2.0 – Browser based applications

Emerging Trends — Is history repeating itself?

- Hybrid cloud to edge computing (real time processing)
- Deplatforming and decentralization of data processing
- Monolithic architectures to a Microservice architecture

Emerging Trends — Microservices



Emerging Trends — Microservices

- …the microservice architectural style is an approach to developing a single application as a suite of small services, each running in its own process and communicating with lightweight mechanisms, often over HTTP resources or API.

  - Martin Fowler

Emerging Trends — Microservices

Security — Feeling secure vs. reality

“Security is two different things: it’s a feeling, and it’s a reality. And they’re different.” — Bruce Schneier

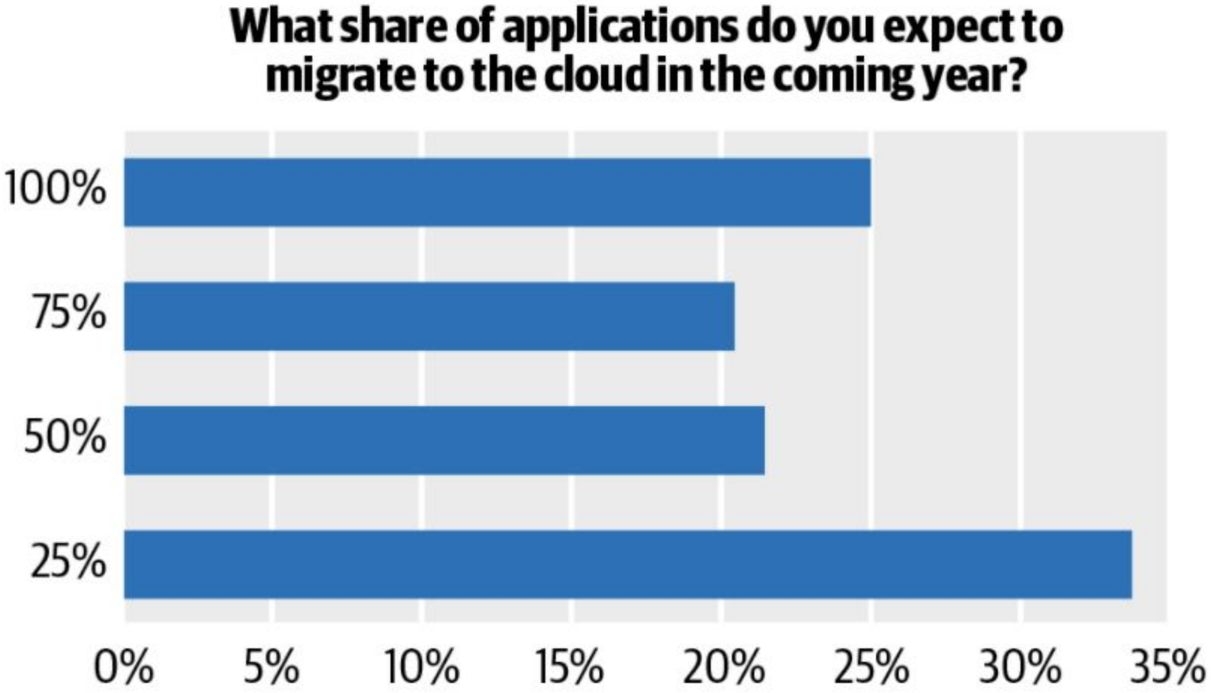
Compliance vs. Security—is there a difference? Is compliance more a feeling of real security vs. reality?

reality.....

Compliance + Security = Trust

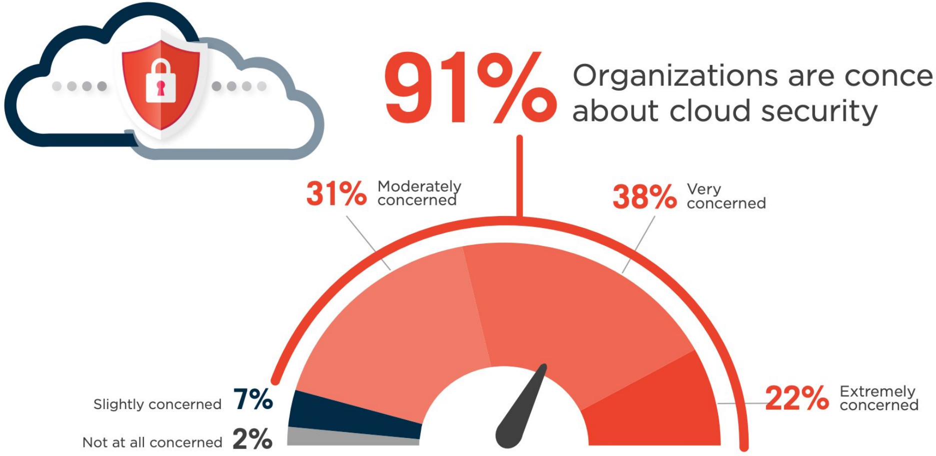
Knowledge Check #2

Cloud Adoption

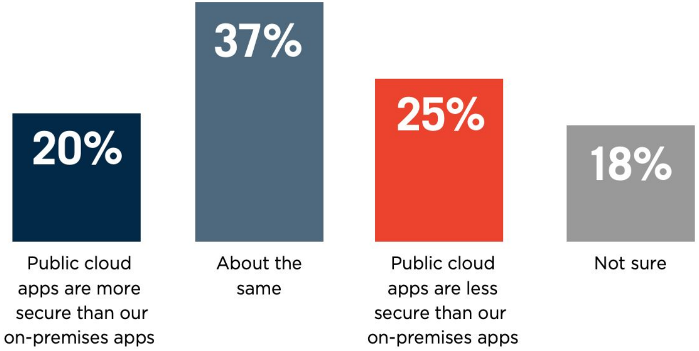


Source: https://www.oreilly.com/radar/cloud-adoption-in-2020/

Cloud Adoption — Are organizations *still* concerned about cloud security and compliance?



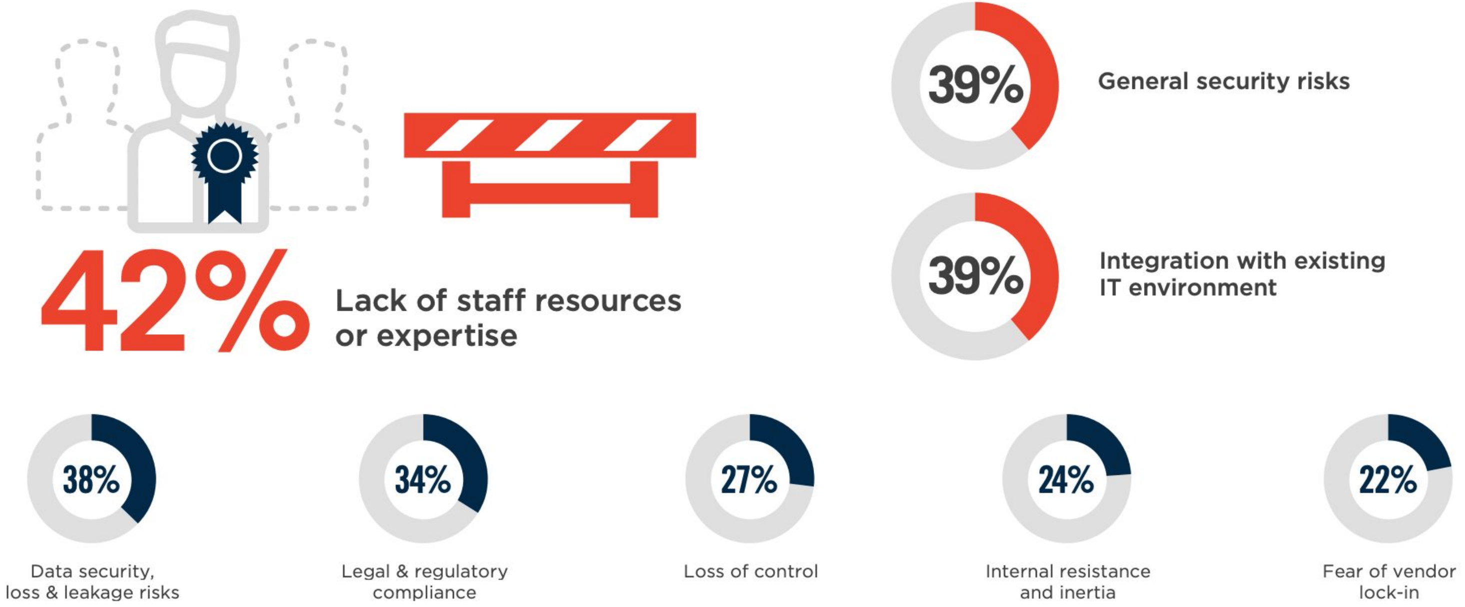
57% believe that cloud apps are as secure or more secure than on-premises applications,



2018 Spotlight Report Crowd Research Partners

Cloud Adoption — (Most) cloud solutions offer better security, but skills are needed

What are the biggest barriers holding back cloud adoption in your organization?



2018 Spotlight Report Crowd Research Partners

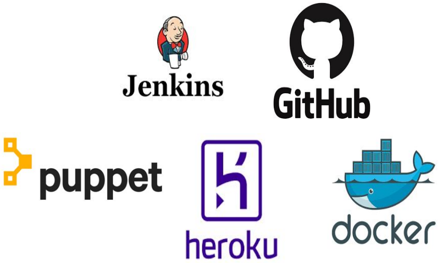
Cloud Models — What are the risks?

SaaS Applications (People/Goods)

- Account hijacking
- Inadequate identity and credential management (i.e., managed by the business)
- Accounts hard coded in third party applications
- External sharing of data

IaaS (Roads)

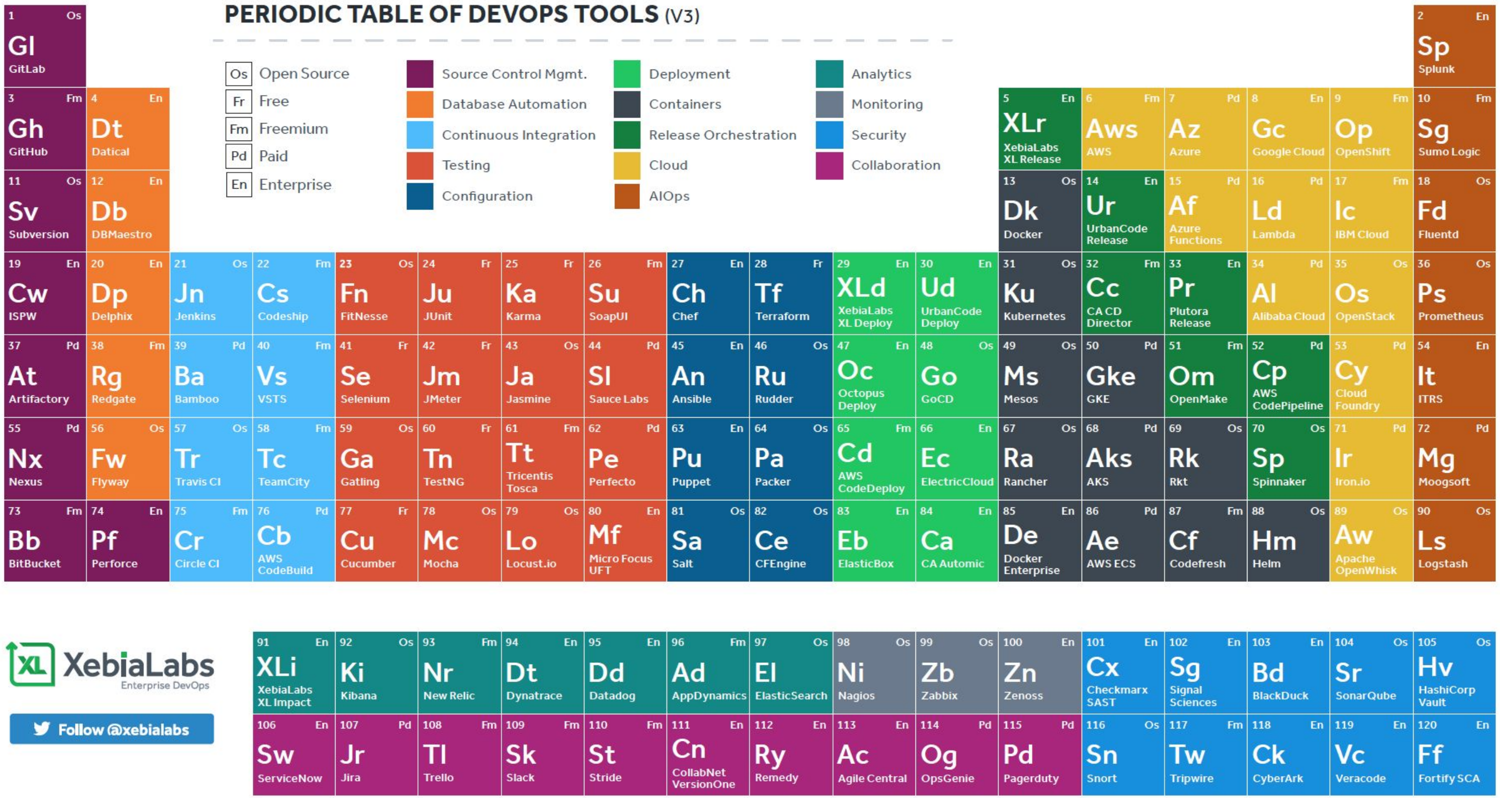
- Abuse of services
- External sharing of data
- Mismanaged account keys
- Insecure APIs; more APIs to manage and less “servers”
- Platform managed by Developers, engineers, and the business vs. IT



DevOps and Other Platforms (Vehicles)

- When DevOps is not integrated as a DevSecOps
- Lack of attention to powerful service account that orchestrates entire ecosystems
- Resources change often (i.e., immutable infrastructures)

Cloud Models — DevOps tools (risk and opportunity)



PERIODIC TABLE OF DEVOPS TOOLS (V3)

- Os Open Source
- Fr Free
- Fm Freemium
- Pd Paid
- En Enterprise

- Source Control Mgmt.
- Database Automation
- Continuous Integration
- Testing
- Configuration
- Deployment
- Containers
- Release Orchestration
- Cloud
- AIOps
- Analytics
- Monitoring
- Security
- Collaboration

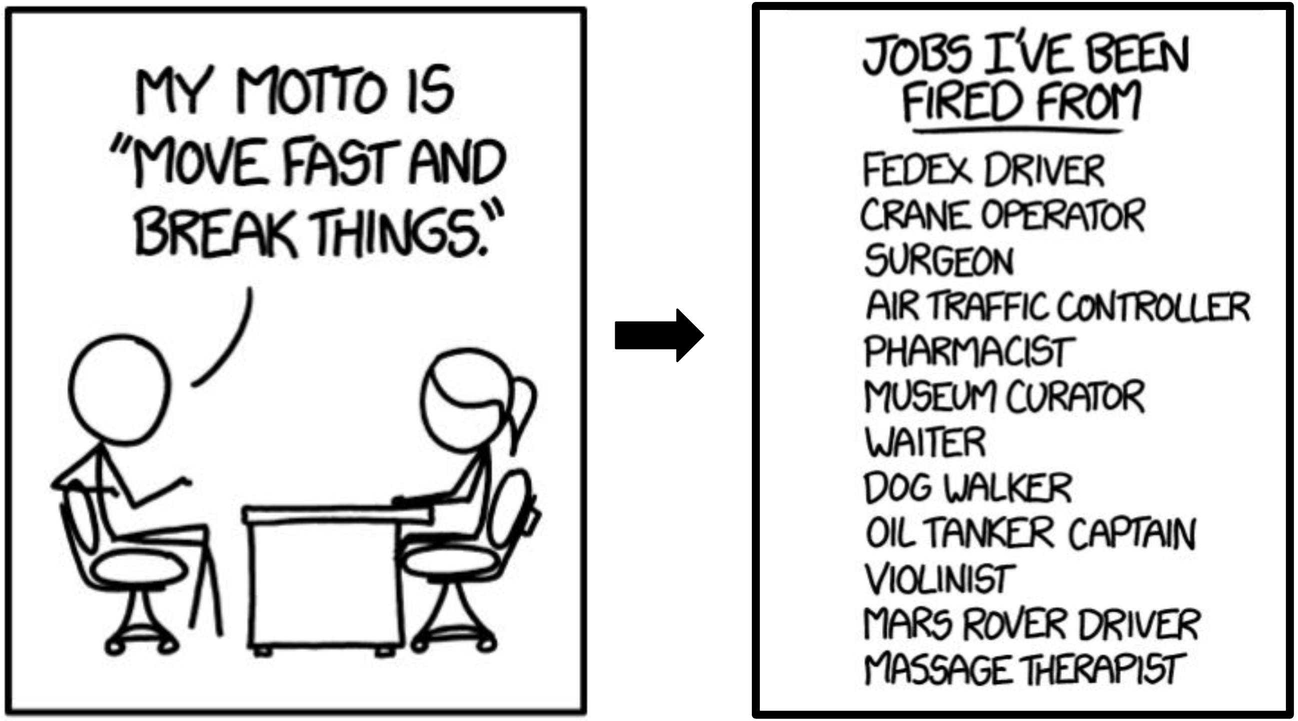
1 Os Gl GitLab																	2 En Sp Splunk
3 Fm Gh GitHub	4 En Dt Datical											5 En XLr XebiaLabs XL Release	6 Fm Aws AWS	7 Pd Az Azure	8 En Gc Google Cloud	9 Fm Op OpenShift	10 Fm Sg Sumo Logic
11 Os Sv Subversion	12 En Db DBMaestro											13 Os Dk Docker	14 En Ur UrbanCode Release	15 Pd Af Azure Functions	16 Pd Ld Lambda	17 Fm Ic IBM Cloud	18 Os Fd Fluentd
19 En Cw ISPW	20 En Dp Delphix	21 Os Jn Jenkins	22 Fm Cs Codeship	23 Os Fn FitNesse	24 Fr Ju JUnit	25 Fr Ka Karma	26 Fm Su SoapUI	27 En Ch Chef	28 Fr Tf Terraform	29 En XLd XebiaLabs XL Deploy	30 En Ud UrbanCode Deploy	31 Os Ku Kubernetes	32 Fm Cc CA CD Director	33 En Pr Plutora Release	34 Pd Al Alibaba Cloud	35 Os Os OpenStack	36 Os Ps Prometheus
37 Pd At Artifactory	38 Fm Rg Redgate	39 Pd Ba Bamboo	40 Fm Vs VSTS	41 Fr Se Selenium	42 Fr Jm JMeter	43 Os Ja Jasmine	44 Pd Sl Sauce Labs	45 En An Ansible	46 Os Ru Rudder	47 En Oc Octopus Deploy	48 Os Go GoCD	49 Os Ms Mesos	50 Pd Gke GKE	51 Fm Om OpenMake	52 Pd Cp AWS CodePipeline	53 Pd Cy Cloud Foundry	54 En It ITRS
55 Pd Nx Nexus	56 Os Fw Flyway	57 Os Tr Travis CI	58 Fm Tc TeamCity	59 Os Ga Gatling	60 Fr Tn TestNG	61 Fm Tt Tricentis Tosca	62 Pd Pe Perfecto	63 En Pu Puppet	64 Os Pa Packer	65 Fm Cd AWS CodeDeploy	66 En Ec ElectricCloud	67 Os Ra Rancher	68 Pd Aks AKS	69 Os Rk Rkt	70 Os Sp Spinnaker	71 Pd Ir Iron.io	72 Pd Mg Moogsoft
73 Fm Bb BitBucket	74 En Pf Perforce	75 Fm Cr Circle CI	76 Pd Cb AWS CodeBuild	77 Fr Cu Cucumber	78 Os Mc Mocha	79 Os Lo Locust.io	80 En Mf Micro Focus UFT	81 Os Sa Salt	82 Os Ce CFEngine	83 En Eb ElasticBox	84 En Ca CA Automic	85 En De Docker Enterprise	86 Pd Ae AWS ECS	87 Fm Cf Codefresh	88 Os Hm Helm	89 Os Aw Apache OpenWhisk	90 Os Ls Logstash
		91 En XLi XebiaLabs XL Impact	92 Os Ki Kibana	93 Fm Nr New Relic	94 En Dt Dynatrace	95 En Dd Datadog	96 Fm Ad AppDynamics	97 Os El ElasticSearch	98 Os Ni Nagios	99 Os Zb Zabbix	100 En Zn Zenoss	101 En Cx Checkmarx SAST	102 En Sg Signal Sciences	103 En Bd BlackDuck	104 Os Sr SonarQube	105 Os Hv HashiCorp Vault	
		106 En Sw ServiceNow	107 Pd Jr Jira	108 Fm Tl Trello	109 Fm Sk Slack	110 Fm St Stride	111 En Cn CollabNet VersionOne	112 En Ry Remedy	113 En Ac Agile Central	114 Pd Og OpsGenie	115 Pd Pd Pagerduty	116 Os Sn Snort	117 Fm Tw Tripwire	118 En Ck CyberArk	119 En Vc Veracode	120 En Ff Fortify SCA	

XebiaLabs
Enterprise DevOps

Follow @xebialabs

Source: https://xebialabs.com/periodic-table-of-devops-tools/

Cloud Models — “Infrastructure as a Code”



Source: https://xkcd.com/1428/

Cloud Models — “Infrastructure as a Code”

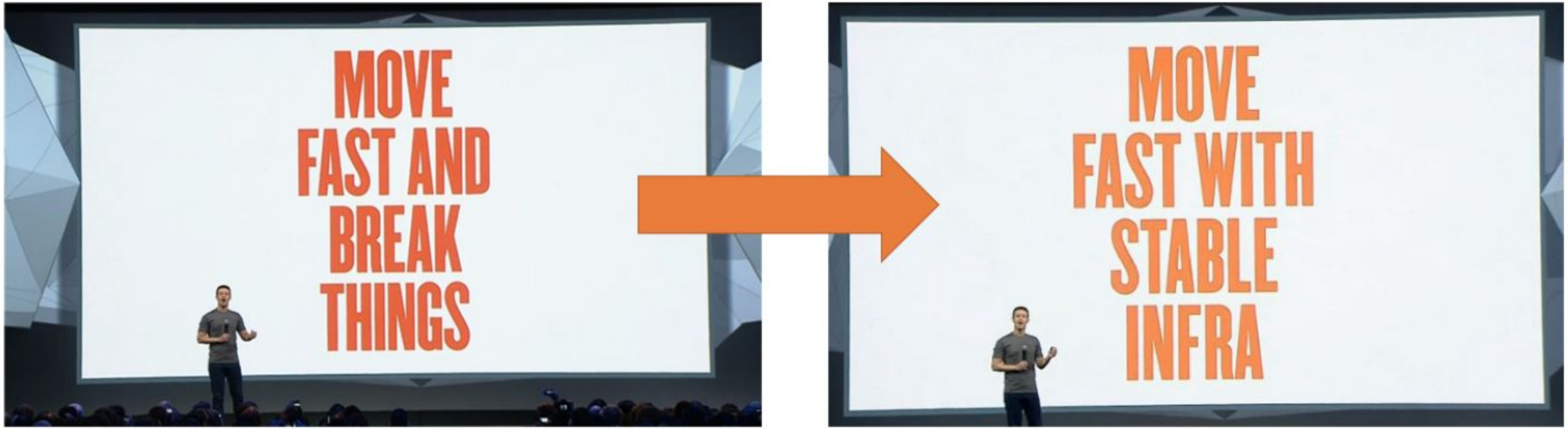


Image: Facebook

Cloud Models — “Security as a Code”

- Velocity of change enabled by DevOps demanded DevSecOps
- “Infrastructure as Code” has enabled “Security as Code”
- Using Continuous Integration and Continuous Delivery as control backbone

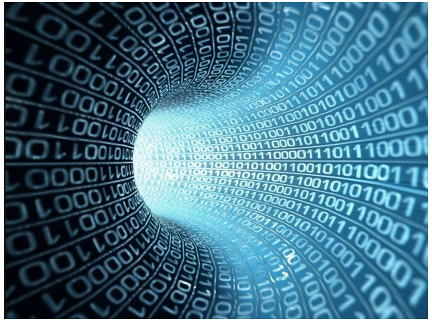
Data Matters — The new oil

Gold Rush

(1849)

Oil Boom

(20th Century)



Data Exhaust

(Now)

Cost of a breach,
according to Ponemon:

$3.86M (global average)

Time to identify/contain: 280 days

$380/record (healthcare)

$245/record (financial services)

Discussion

- What are your current challenges or concerns when it comes to the cloud?
- What do you care about?
- What don’t you care about?

Knowledge Check #3

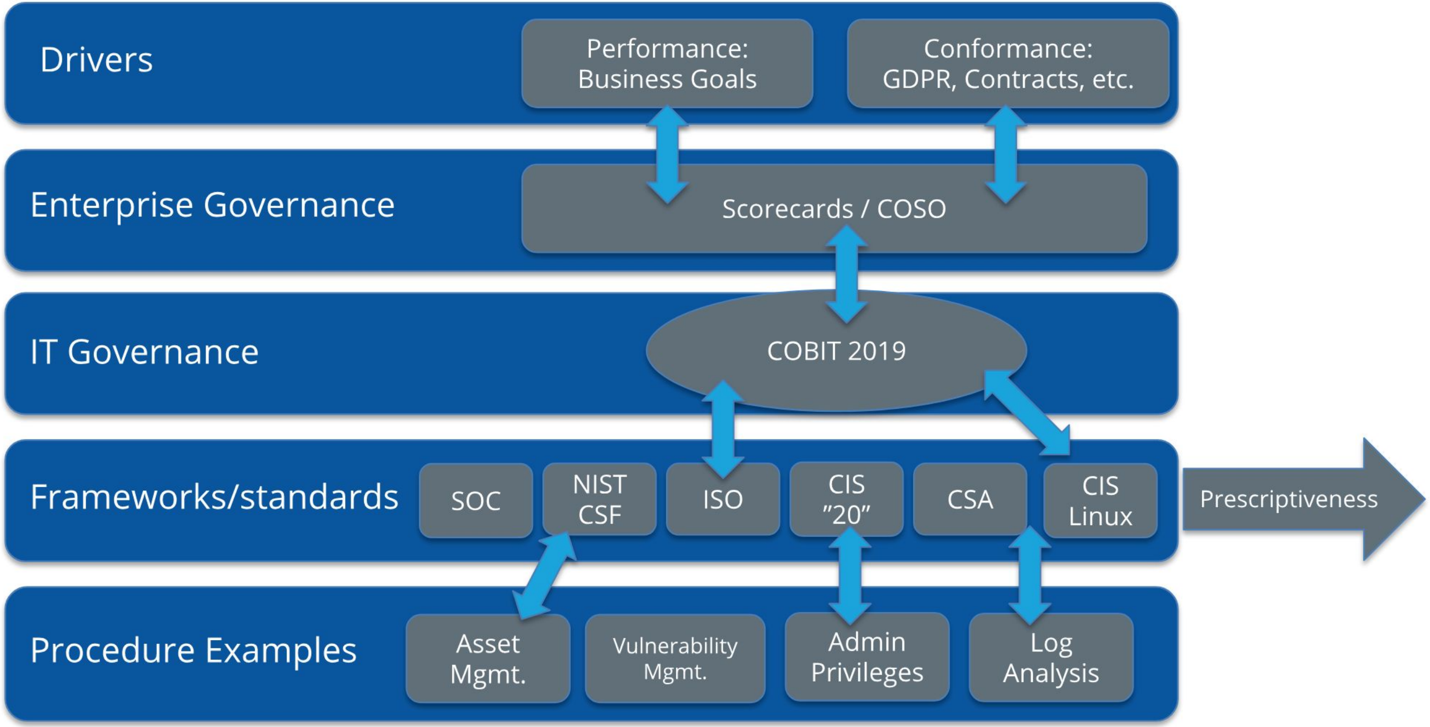
Industry Regulations and Framework Application

Key Frameworks, Regulations, and Reporting — Many choices

Frameworks	Regulations/Industries	Reporting/Certifications
• COBIT 2019 • SOC for Cybersecurity • NIST CSF 1.1 • ISO 27001, 27017, 27018 • CIS Critical Security Controls • Cloud Security Alliance (CSA)	• GDPR (“opt-in”) • CCPA (“opt-out”) • PCI DSS • DFARS • GLBA • New York Cybersecurity DFS • HIPAA / HITECH • FISMA • FFIEC	• HITRUST • FedRAMP • SOC 1, SOC 2, SOC 3 • ISO 27001, 27017, 27018 • ISO 27701 (Privacy) • PCI DSS 3.2.1 • CSA STAR

Key Frameworks, Regulations, and Reporting —

Using COBIT to integrate frameworks and align IT to business



Source: Modified from COBIT

Key Frameworks, Regulations, and Reporting —
Regulatory Considerations

GDPR	HIPAA	PCI 3.2.1
• Data inventory / reduce scope • Controller, processor, recipient • Incident definition and reporting (i.e., 72 hour rule) • Subject Access Rights (SAR) Request • Individual rights to compensation • Cloud processor due diligence of their customers (i.e., controllers) • Old expressed consents that are inadequate	• Data inventory / reduce scope • Incident definition and reporting (i.e., 60 days to secretary) • Using Cloud to process ePHI without a BAA in place • Encryption is good, but does not exempt you or CSP from HIPAA rules • Data retention and disposal SLAs	• Data inventory / reduce scope • Segmentation (VPCs) • Tokenization • P2PE

Key Frameworks, Regulations, and Reporting — Leveraging and Reviewing SOC Reports

Scope	Report	Summary	Applicability
Internal Control Over Financial Reporting	SOC 1	• Detailed report for users and their auditors • Once referred to as SSAE 16	• Focused on controls that support financial reporting
Operational Controls	SOC 2	• Detailed report for user organizations, their auditors, and specified parties	Broad variety of systems focused on the following categories: Security, Availability, Confidentiality, Processing Integrity, Privacy + Additional Criteria in SOC 2 (i.e., HIPAA)
	SOC 3	• Short report that can be more generally distributed	
Entire Entity	SOC for Cybersecurity	• Reporting framework over an entire entity's cybersecurity risk management program and related controls	• Can have other specific uses such as management reporting to a board or audit committee • Demonstrate and communicate due diligence and due care in the entity's cybersecurity program

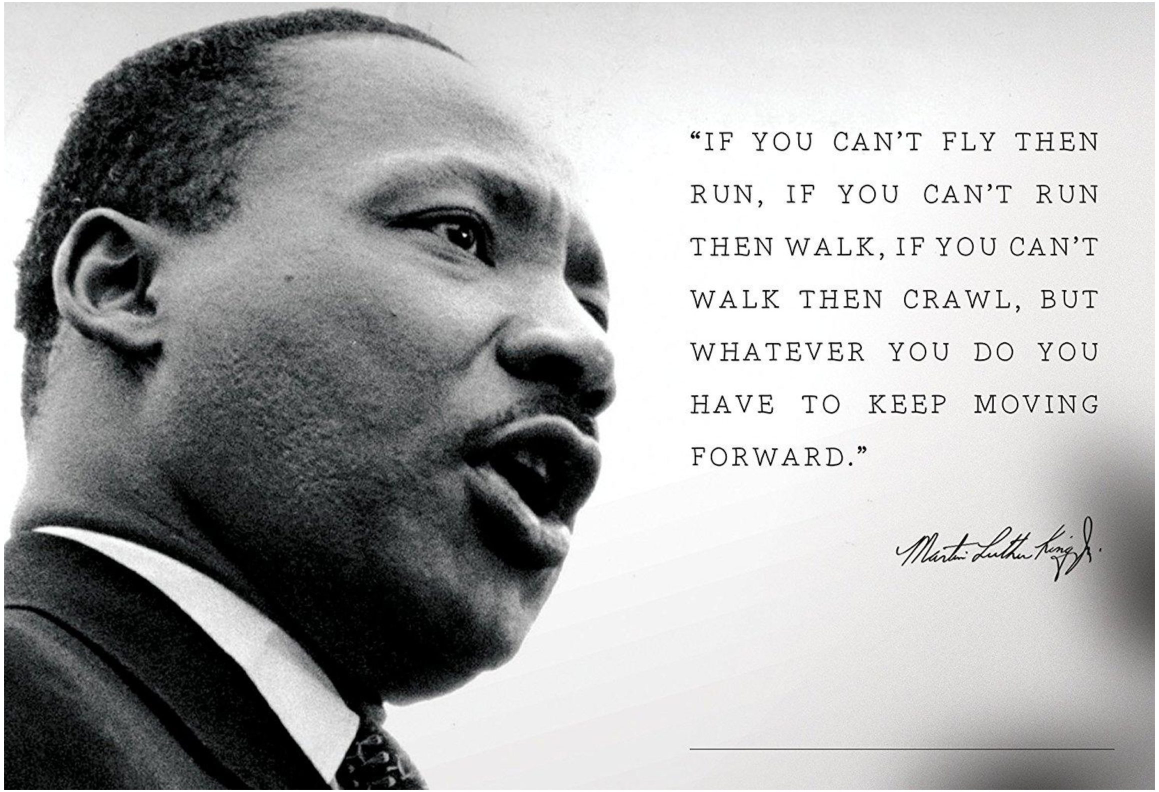
Key Frameworks, Regulations, and Reporting —
Leveraging and Reviewing SOC Reports

- **Management’s assertion (usually section 1)**
- **Auditor’s opinion (usually section 2)**
    - Unqualified (clean), qualified, adverse, disclaim
    - Scope / criteria used
    - “Carve out” or “inclusive” of subservice organizations
    - Type 1 or Type 2
- **System Description (usually section 3)**
    - Does the system include your relied system
    - Complementary user entity control
    - Complementary subservice organization controls
- **Controls and tests of controls (usually section 4)**
    - Any exceptions
    - Any controls missing that do not address your risks of using the service organization
    - Criteria used in the examination
- **Other Information (usually section 5)**

Knowledge Check #4

Key Risks and Controls

Cloud Controls — Maturity Process



"IF YOU CAN'T FLY THEN RUN, IF YOU CAN'T RUN THEN WALK, IF YOU CAN'T WALK THEN CRAWL, BUT WHATEVER YOU DO YOU HAVE TO KEEP MOVING FORWARD."

Martin Luther King Jr.

Cloud Controls — “Lean InfoSec” Controls

box G Suite
workday Office 365

SaaS Applications (People/Goods)

- Multi-factor authentication
- Log resources / workflow public shares
- Store encryption keys of your data in separate cloud environments
- SAML / SSO / Federated Identity Management
- Consider a CASB

amazon web services Microsoft Azure
Google Cloud Platform

IaaS (Roads)

- Automatically rotate access keys after use
- Patching with continuous deployment / immutable infra

Jenkins GitHub
heroku docker

DevOps and other Platforms (Vehicles)

- Automated testing
- Vulnerability / pen test non production environments
- Endpoint management for those with tools on the endpoint
- “Infrastructure as code” process!
- API security

Cloud Controls — Microservices

- Common Control Considerations
  - API hygiene including inventory, testing, auditing
  - Authenticate API consumption (i.e., API key, access token, short lived certs)
  - Credential and key management
  - Rate limit for protection of DDoS and availability issues
  - Use of open API frameworks
  - Inject chaos (Netflix Chaos Monkey)
  - Reduce single points of failure
  - Encrypt all traffic
  - Logging and monitoring

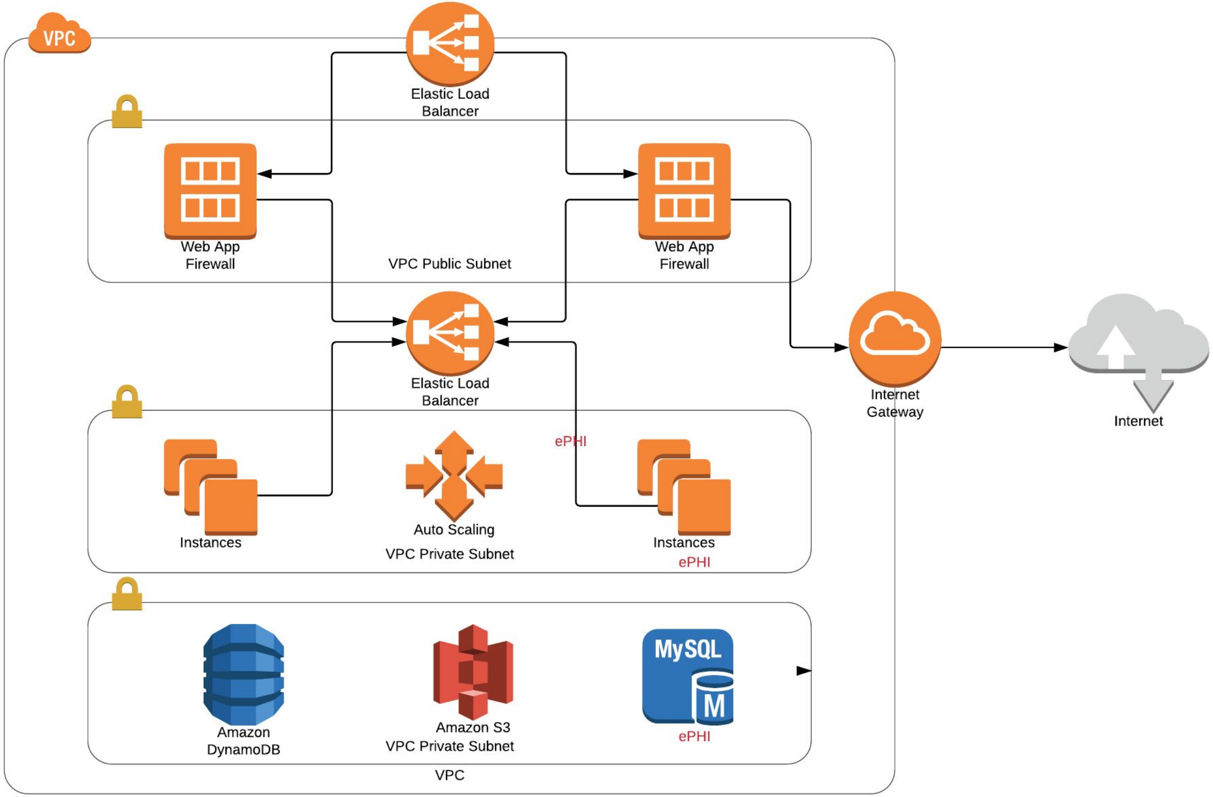
Cloud Controls — Basic Lean InfoSec

- Common Control Considerations
  - Endpoint and mobile device management
  - Use the latest version of OS and internet connected applications
  - Disallow weak passwords (both by policy and system enforcement)
  - Encryption, Encryption, Encryption
  - Multi-factor authentication
  - Phishing protections
  - Baseline security hardening
  - Whitelisting
  - Don’t expose systems to the public internet
  - Hire the hackers before the bad guys

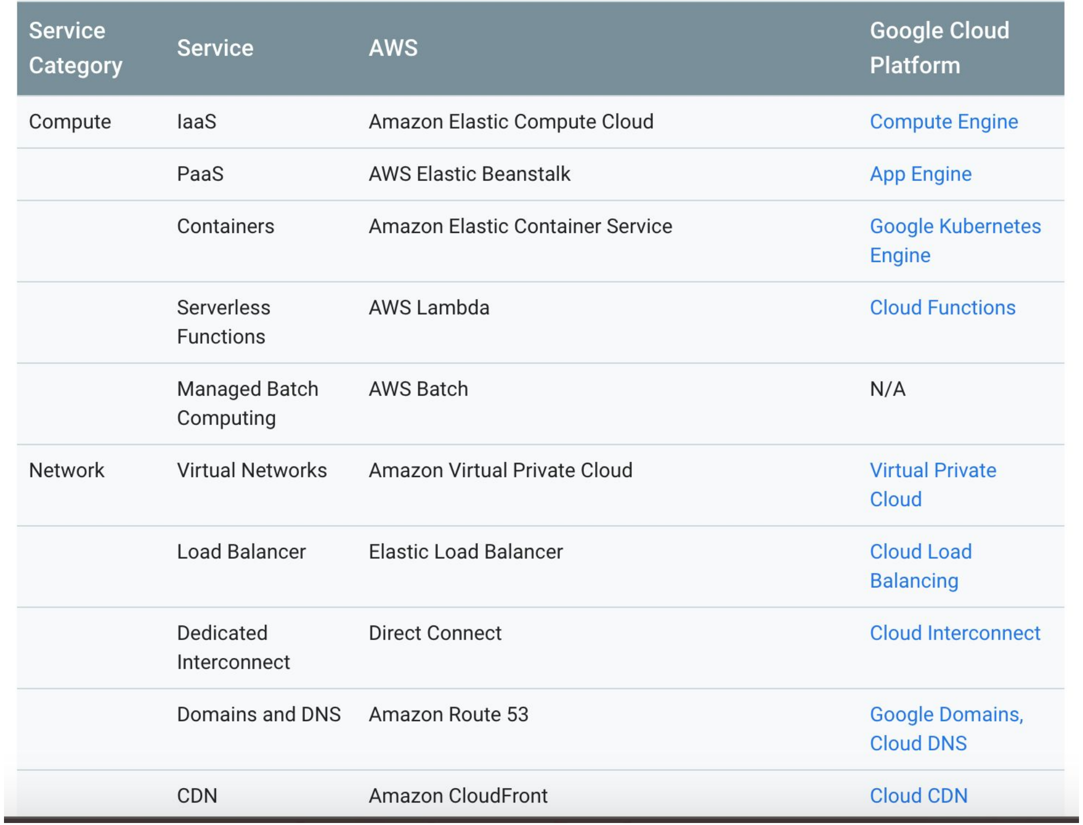
Protecting AWS Workloads

AWS Best Practices — Basics

- Common Elements
  - VPC - Network
  - EC2 - Servers
  - RDS - Database
  - S3 - Storage
  - Load balancer
  - CloudWatch
  - CloutTrails
  - AWS Lambda
  - AWS ECS (i.e. Fargate) and serverless compute



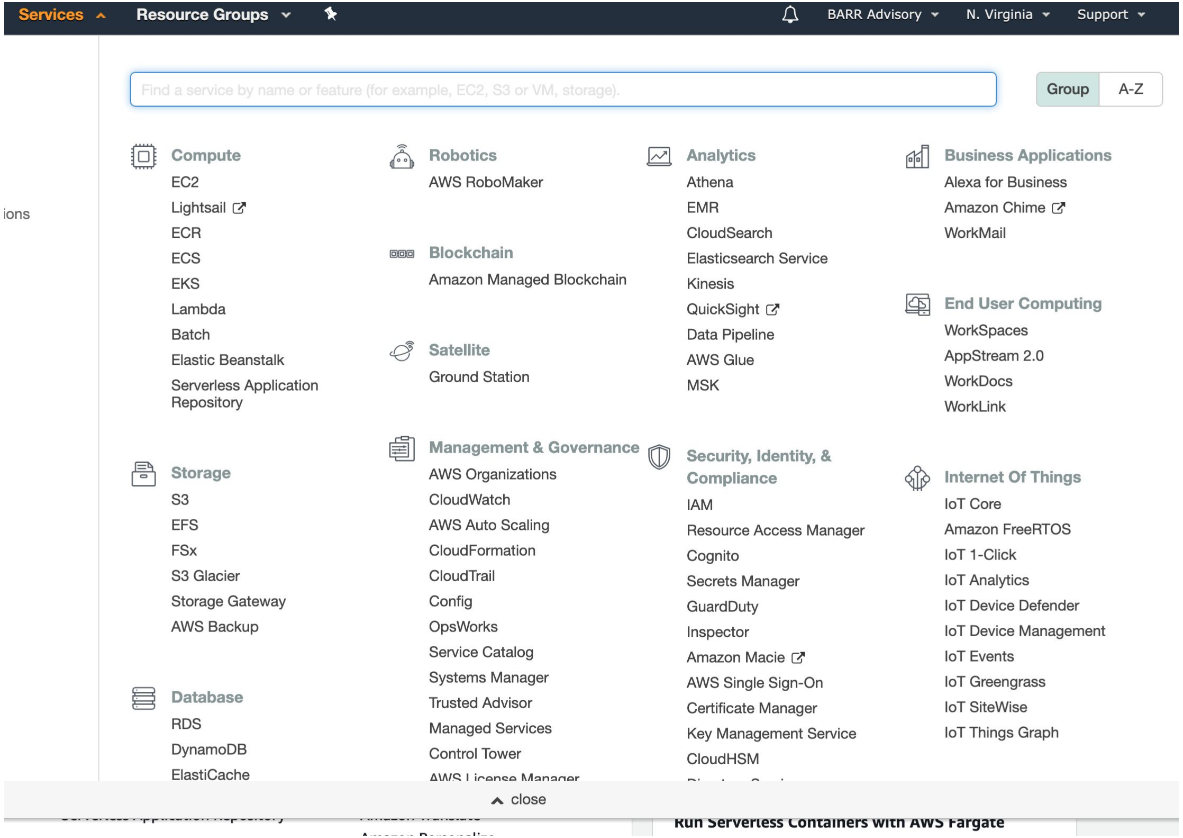
AWS Best Practices — AWS to GCP translation



Service Category	Service	AWS	Google Cloud Platform
Compute	IaaS	Amazon Elastic Compute Cloud	Compute Engine
	PaaS	AWS Elastic Beanstalk	App Engine
	Containers	Amazon Elastic Container Service	Google Kubernetes Engine
	Serverless Functions	AWS Lambda	Cloud Functions
	Managed Batch Computing	AWS Batch	N/A
Network	Virtual Networks	Amazon Virtual Private Cloud	Virtual Private Cloud
	Load Balancer	Elastic Load Balancer	Cloud Load Balancing
	Dedicated Interconnect	Direct Connect	Cloud Interconnect
	Domains and DNS	Amazon Route 53	Google Domains, Cloud DNS
	CDN	Amazon CloudFront	Cloud CDN

Source: https://cloud.google.com/free/docs/map-aws-google-cloud-platform

AWS Best Practices — Basics

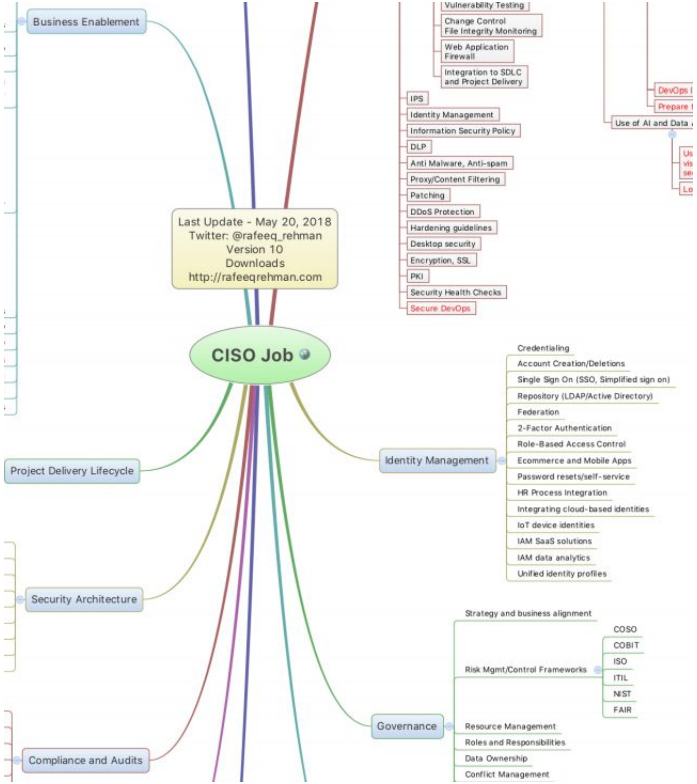


AWS Best Practices — Example Domains

- Governance
- Technical
  - Network configuration
  - Asset management
  - Access control
  - Change
  - Incident management
  - Disaster recovery

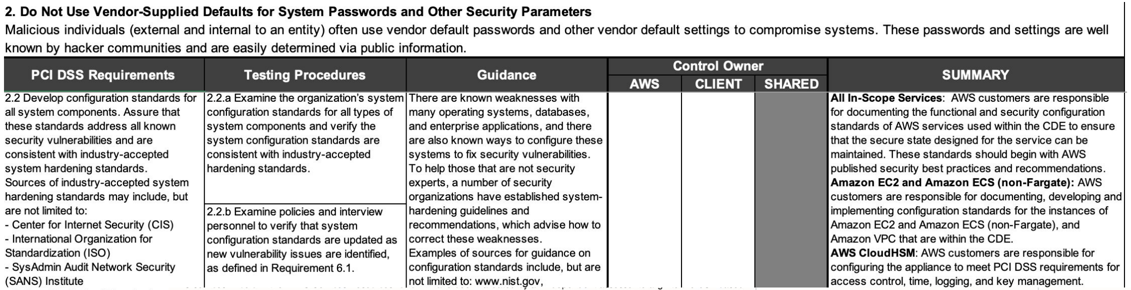
AWS Best Practices — Governance

- Know the roles and responsibilities
  - CEO - set the culture
  - CISO - MindMap - own the program
    - Define the policies
  - CIO - Sanctioned vs. unsanctioned IT
  - CFO / COO - not just about the budget
  - Legal - include InfoSec in contract review
  - CAE - deploy automated testing



AWS Best Practices — Governance

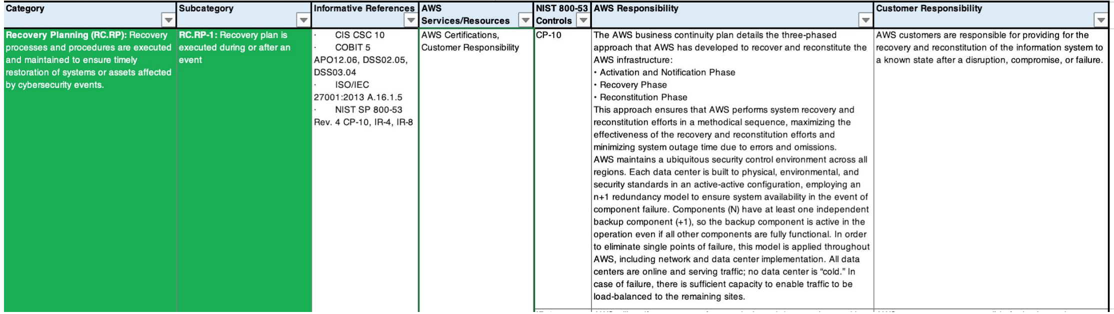
- Review shared responsibilities matrix for your requirements
  - PCI
  - NIST CSF
  - HIPAA
  - Whitepapers



2. Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

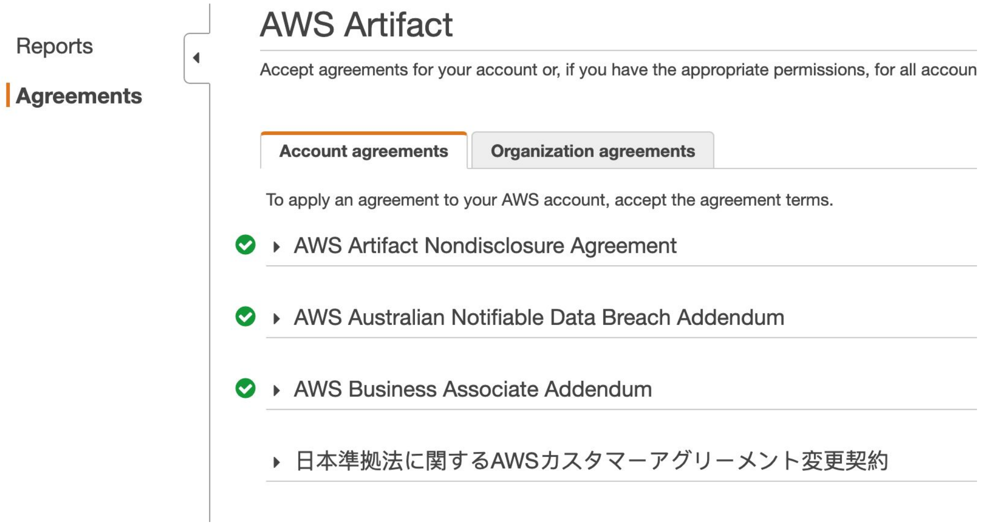
PCI DSS Requirements	Testing Procedures	Guidance	Control Owner			SUMMARY
			AWS	CLIENT	SHARED	
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: - Center for Internet Security (CIS) - International Organization for Standardization (ISO) - SysAdmin Audit Network Security (SANS) Institute - National Institute of Standards Technology (NIST).	2.2.a Examine the organization's system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards. 2.2.b Examine policies and interview personnel to verify that system configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.1.	There are known weaknesses with many operating systems, databases, and enterprise applications, and there are also known ways to configure these systems to fix security vulnerabilities. To help those that are not security experts, a number of security organizations have established system-hardening guidelines and recommendations, which advise how to correct these weaknesses. Examples of sources for guidance on configuration standards include, but are not limited to: www.nist.gov,			▨	**All In-Scope Services**: AWS customers are responsible for documenting the functional and security configuration standards of AWS services used within the CDE to ensure that the secure state designed for the service can be maintained. These standards should begin with AWS published security best practices and recommendations. **Amazon EC2 and Amazon ECS (non-Fargate):** AWS customers are responsible for documenting, developing and implementing configuration standards for the instances of Amazon EC2 and Amazon ECS (non-Fargate), and Amazon VPC that are within the CDE. **AWS CloudHSM**: AWS customers are responsible for configuring the appliance to meet PCI DSS requirements for access control, time, logging, and key management.



Category	Subcategory	Informative References	AWS Services/Resources	NIST 800-53 Controls	AWS Responsibility	Customer Responsibility
Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after an event	· CIS CSC 10 · COBIT 5 APO12.06, DSS02.05, DSS03.04 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8	AWS Certifications, Customer Responsibility	CP-10	The AWS business continuity plan details the three-phased approach that AWS has developed to recover and reconstitute the AWS infrastructure: • Activation and Notification Phase • Recovery Phase • Reconstitution Phase This approach ensures that AWS performs system recovery and reconstitution efforts in a methodical sequence, maximizing the effectiveness of the recovery and reconstitution efforts and minimizing system outage time due to errors and omissions. AWS maintains a ubiquitous security control environment across all regions. Each data center is built to physical, environmental, and security standards in an active-active configuration, employing an n+1 redundancy model to ensure system availability in the event of component failure. Components (N) have at least one independent backup component (+1), so the backup component is active in the operation even if all other components are fully functional. In order to eliminate single points of failure, this model is applied throughout AWS, including network and data center implementation. All data centers are online and serving traffic; no data center is "cold." In case of failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.	AWS customers are responsible for providing for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

AWS Best Practices — Governance

- Execute key compliance artifacts
  - GDPR DPA is part of terms
  - HIPAA BAA
  - Nondisclosure
  - SLA requirements



AWS Artifact

Accept agreements for your account or, if you have the appropriate permissions, for all accoun

To apply an agreement to your AWS account, accept the agreement terms.

✓ AWS Artifact Nondisclosure Agreement

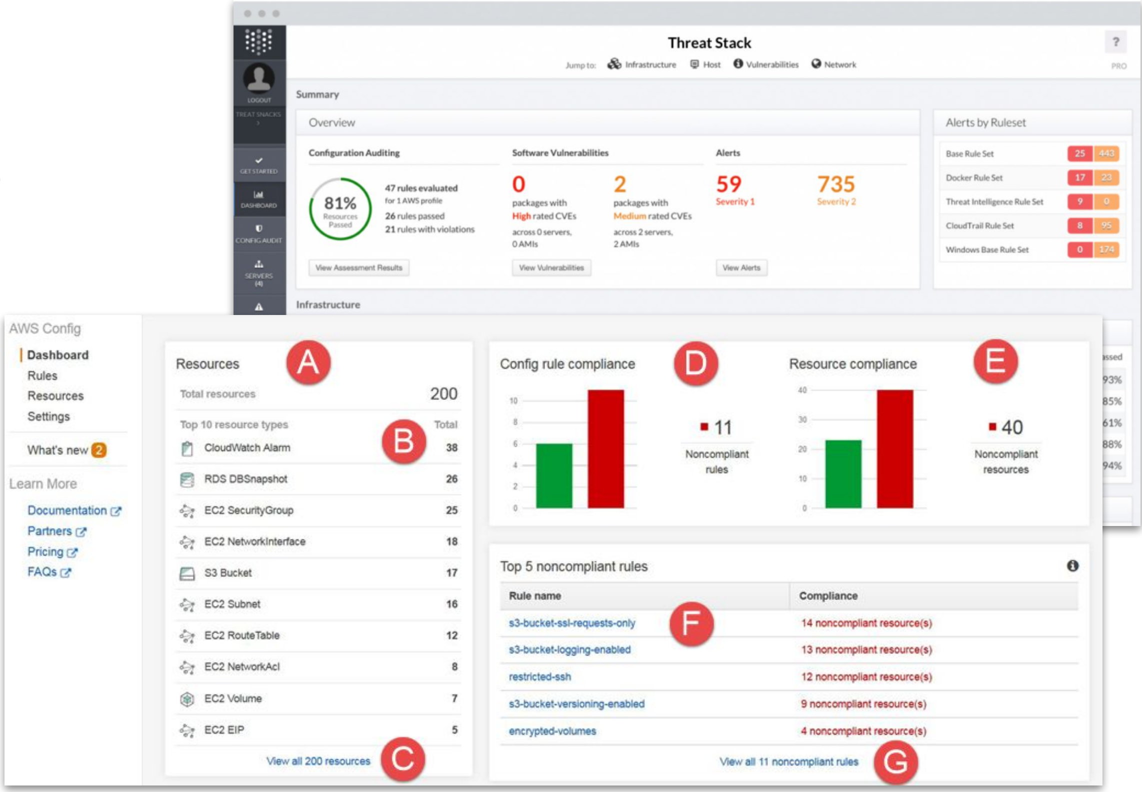
✓ AWS Australian Notifiable Data Breach Addendum

✓ AWS Business Associate Addendum

日本準拠法に関するAWSカスタマーアグリーメント変更契約

AWS Best Practices — Governance

- Determine monitoring
  - Open source vs. enterprise
  - Define baselines
  - Document architecture
    - How many accounts?
    - Multi tenant?
  - Determine org accounts
  - Determine billing set up
  - Leverage AWS Lambda
  - Consider other tools such as AWS Inspector, Config, Guard Duty, Macie, Secrets



Threat Stack

Jump to: Infrastructure · Host · Vulnerabilities · Network

Summary

Overview

Configuration Auditing: 81% Resources Passed. 47 rules evaluated for 1 AWS profile; 26 rules passed; 21 rules with violations. View Assessment Results

Software Vulnerabilities: 0 packages with High rated CVEs across 0 servers, 0 AMIs; 2 packages with Medium rated CVEs across 2 servers, 2 AMIs. View Vulnerabilities

Alerts: 59 Severity 1; 735 Severity 2. View Alerts

Infrastructure

Alerts by Ruleset

Base Rule Set	25	443
Docker Rule Set	17	23
Threat Intelligence Rule Set	9	0
CloudTrail Rule Set	8	95
Windows Base Rule Set	0	174

AWS Config

Resources — Total resources: 200

Top 10 resource types	Total
CloudWatch Alarm	38
RDS DBSnapshot	26
EC2 SecurityGroup	25
EC2 NetworkInterface	18
S3 Bucket	17
EC2 Subnet	16
EC2 RouteTable	12
EC2 NetworkAcl	8
EC2 Volume	7
EC2 EIP	5

View all 200 resources

Config rule compliance: 11 Noncompliant rules

Resource compliance: 40 Noncompliant resources

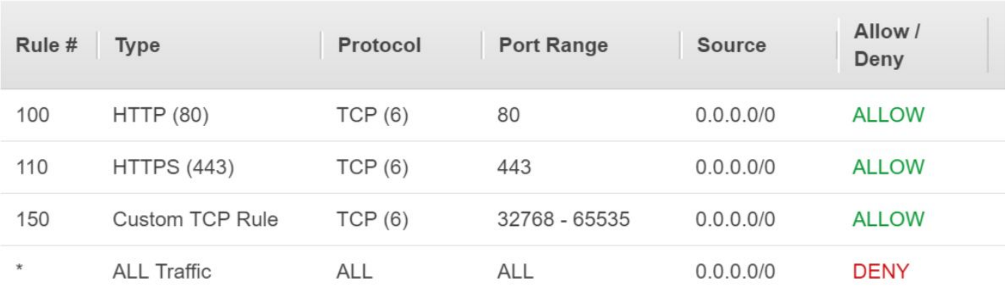
Top 5 noncompliant rules

Rule name	Compliance
s3-bucket-ssl-requests-only	14 noncompliant resource(s)
s3-bucket-logging-enabled	13 noncompliant resource(s)
restricted-ssh	12 noncompliant resource(s)
s3-bucket-versioning-enabled	9 noncompliant resource(s)
encrypted-volumes	4 noncompliant resource(s)

View all 11 noncompliant rules

AWS Best Practices — Network configuration

- CIS Benchmarks
  - 4.1/2 Ensure no security groups allow ingress from 0.0.0.0/0 to port 22 or 3389 (even better is not not allow ingress outside of console using systems manager or entirely serverless compute)
  - 4.3 Ensure VPC flow logging is enabled in all VPCs
  - 4.4 Ensure the default security group of every VPC restricts all traffic
  - 4.5 Ensure routing tables for VPC peering are "least access"
- Group services in VPC
  - Web facing service >
  - Internal services
  - Bastion host subnet for SSH



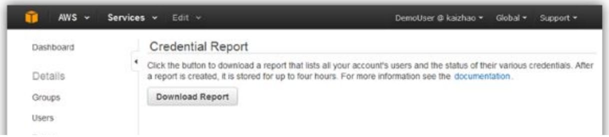
Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	HTTP (80)	TCP (6)	80	0.0.0.0/0	ALLOW
110	HTTPS (443)	TCP (6)	443	0.0.0.0/0	ALLOW
150	Custom TCP Rule	TCP (6)	32768 - 65535	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

AWS Best Practices — Asset Management

- Use the asset tagging feature in AWS
- Determine standard build images used and how they are hardened
- Data retention and classification considerations
  - S3 > "Management" Tab > "Lifecycle" subtab
  - AWS Macie - Machine Learning Data Classification and DLP

AWS Best Practices — Access Control

- Review credentials report (i.e., root use, access key use, password use)



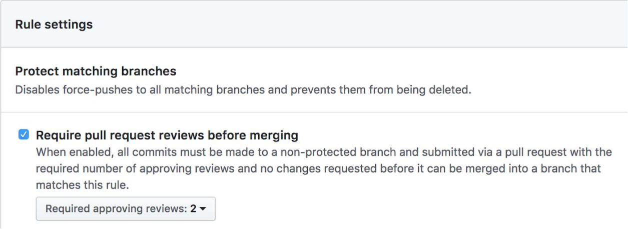
Credential Report

Click the button to download a report that lists all your account's users and the status of their various credentials. After a report is created, it is stored for up to four hours. For more information see the documentation.

- Root
  - Turn logging and MFA on; revoke access key, and do not use for daily tasks
  - Revoke root access keys and only use for initial IAM set up (do not use roo
- Attach policies to roles and groups, not users
- Be aware of S3 buckets open to public; establish policies
- Automatically rotate access keys and remove password sys accounts
- API Mgmt ("Bool" : { "aws:MultiFactorAuthPresent" : "True"}
- Leverage secrets manager to ensure no hard coded secrets

AWS Best Practices — Change Control

- Use branch protection with source code
- DevSecOps and automated testing

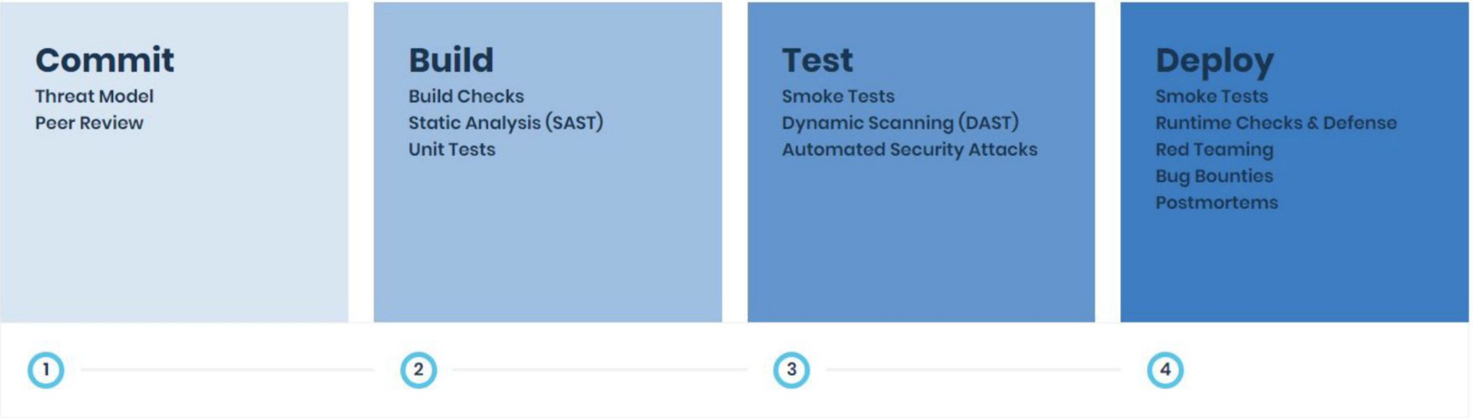


Rule settings

Protect matching branches
Disables force-pushes to all matching branches and prevents them from being deleted.

☑ **Require pull request reviews before merging**
When enabled, all commits must be made to a non-protected branch and submitted via a pull request with the required number of approving reviews and no changes requested before it can be merged into a branch that matches this rule.

Required approving reviews: 2 ▾



Commit
Threat Model
Peer Review

Build
Build Checks
Static Analysis (SAST)
Unit Tests

Test
Smoke Tests
Dynamic Scanning (DAST)
Automated Security Attacks

Deploy
Smoke Tests
Runtime Checks & Defense
Red Teaming
Bug Bounties
Postmortems

1 2 3 4

Source: VerSprite

AWS Best Practices — Incident Management

- Integrate AWS (i.e., CloudTail/CloudWatch with SIEM / Security analytics tools)
- Ensure CloudTrail is enabled in all regions with integration to CloudWatch
- Ensure S3 buckets where logs exist are not public
- Enable log metrics (i.e., unauthorized APIs, console sign-in without MFA, VPC changes, root sign in, etc.)

AWS Best Practices — BCP/DR

- Enable multi-AZ in RDS
- Determine if multiple regions are required
- Business impact assessment
- Data transferability
- RPO and RTO definitions

Contact Us

Brad Thies

Principal, BARR Advisory

+1 (913) 579-8314

bthies@barradvisory.com

BARR ADVISORY