AWS Security Best Practices

Denver (ISC)² Chapter
May 17, 2018, Denver, CO

DENVER

GTRI
IS NOW ZIVARO

Scott Hogg, CTO GTRI
CCIE #5133, CISSP #4610, CCSP, CCSK
AWS Certified Solutions Architect – Professional
AWS Certified Network and Security - Specialty (ANS & SCS)

Today's Agenda

1. Shared Responsibility Model
2. AWS Security Measures and Best Practices
3. Live Demonstration of AWS Security
4. Cloud Security Certifications
5. Summary, Resources, and Q&A

Shared Responsibility Model

Cloud Shared Security Responsibility – A Sliding Scale

- Customer bears more responsibility with IaaS than SaaS

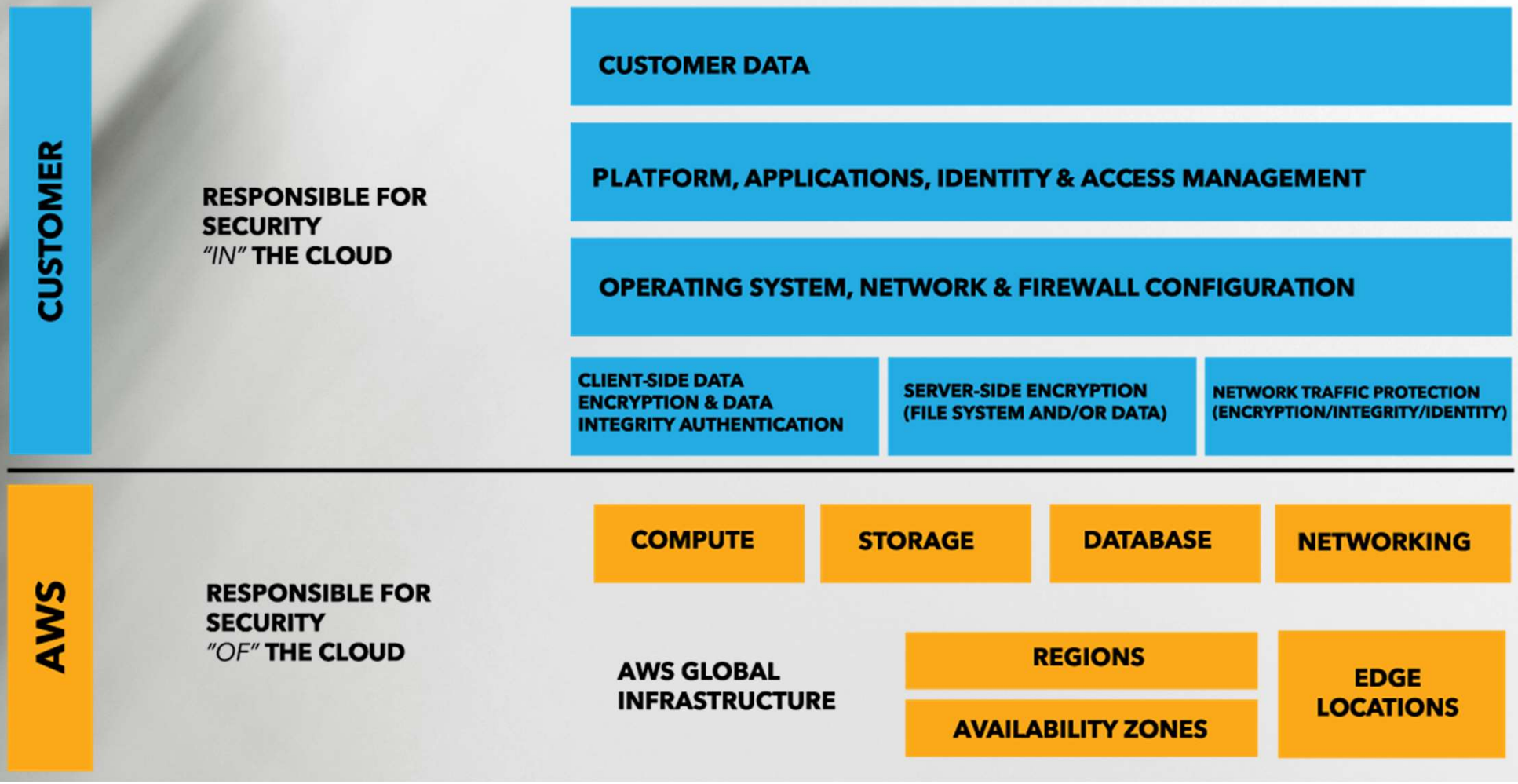
	IaaS	PaaS	SaaS
Security GRC			
Data Security			
App Security			
Platform Security			
Infrastructure Security			
Physical Security			

Enterprise Responsibility

Shared Responsibility

Provider Responsibility

AWS Shared Responsibility Model



AWS Compliance Certifications and Accreditations

Concerns About AWS Security

- A breach of the Cloud Service Provider's infrastructure can lead to a "Hyperjacking" event whereby many customer's data is exposed
- Examples of CSP Data Breaches:
  - Code Spaces goes out of business in June 2014 after AWS infrastructure hack
  - Dropbox breach in October 2014, compromising 7M passwords held for Bitcoin ransom
  - Worcester Polytechnic Institute (WPI) claims cross-VM RSA key recovery in AWS, October 2015
  - Datadog password breach for their AWS customers in July 2016
  - OneLogin breach of AWS infrastructure due to insecure keys in May 2017
  - RNC leaks 1.1TB of data on 200M people via Deep Root Analytics on S3 bucket June 2017
  - World Wrestling Entertainment leaked 3M customer info unprotected AWS S3 bucket July 2017
  - Verizon leaked 14M customer data by Nice Systems on weak AWS S3 bucket July 2017
  - Alteryx breached AWS infrastructure, 123M U.S. households in October 2017

AWS Security Measures

Identity and Access Management (IAM)

- Stringent Identity and Access Management (IAM) practices are a MUST
- Use IAM policies to control users, groups, permissions, and accounts that run services on AWS resources – Rotate Access Keys & Secrets used for API calls
- Security Token Service (STS) is web service that grants requests for temporary, limited privilege credentials for IAM users/roles
- No one should be using the master payer account, root privileges should not be used, developer accounts need only specific privileges, create general use accounts for each sys-admin or service accounts, configure password policy
- Use Multi-Factor Authentication (MFA) for master account & admin accounts
- Federated identity access for management console and APIs
  - SAML 2.0, OpenID Connect (OIDC), AWS Microsoft AD Connector (ADFS)

Security Technical Implementation Guides (STIGs)

- You are only as secure as your EC2 Instances base Amazon Machine Images (AMIs) (manage systems with templates not individually)
- Build your own secure images off a default AMIs or import your own hardened AMI based on your preferred STIG
- Save the AMIs, and reuse them for other applications and services
- Don't store security keys within your stored or shared (community) images
- AWS Marketplace also offers hardened images
  - DISA STIGs exist for most OSs (not yet Ubuntu)
  - Center for Internet Security (CIS) Benchmarks
  - Buddha Labs offers hardened images (DISA STIG)
  - Anitian, DeepCyber, SteelCloud, among others

CIS™

ANITIAN

DeepCyber

SteelCloud®

Virtual Private Clouds (VPCs)

- VPCs create enclaves of virtually-separated systems supporting application segmentation, don't just punt and use the default VPC
- Network Access Control Lists (NACLs) are like router ACLs (not-stateful, directional, applied to a subnet), tend to be fairly coarse
- Security Groups (SGs) are like firewalls (fully stateful whitelist behavior applied to EC2 instance ENI, highly restrictive inbound, outbound typically allowed)
- Put different systems into separate subnets and Availability Zones (AZs) and security groups (load balancers, web servers, databases)
- Carefully document your use of the Internet Gateway (IGW), Egress-Only Internet Gateway (EOIGW), Virtual Private Gateway (VGW) , and Customer Gateway (CGW)
- VPC Flow Logs capture IP traffic on VPC interfaces for deeper analysis

AWS Connectivity

- Securely establish connectivity to your AWS Management VPC
  - Use encryption and control source IP addresses connecting to your VPC
  - Establish IPsec tunnel-mode VPN connection to your Virtual Private Gateway (VGW)
  - IKE v1 (No IKE v2), AES-256, SHA-1, DH Group 2, PFS, DPD (Enhanced AWS VPN AES-256, SHA2(256), DH 14-18, 22, 23, 24, NAT-T)
  - Supports static routes or eBGP dynamic routing (propagated)

- Direct Connect is a dedicated private physical link to your VPC
  - Within an AWS data center or via WAN service provider
  - Supports 802.1Q VLAN tagging, eBGP-only dynamic routing
- Primary Direct Connect and backup VPN can be used in combination for added resiliency

Backup & Disaster Recovery

- Utilize the built-in AWS services to assist with backups & restoration
  - RDS instances are automatically backed up (default 7 days, up to 35 days)
  - EBS snapshots are incremental backups stored on S3
  - Use S3 Bucket Policies to control account and user-level access to your S3 files
  - S3 Versioning, MFA delete, S3 Logs – bucket logging, S3 event notifications
  - S3 Lifecycle policies can automatically migrate older files to Glacier
  - Glacier can be used for long-term archives within vaults, but it is slow and expensive to retrieve
- Plan for and design for failure
  - Multi-AZ architectures, e.g. NLB with auto-scale-groups, Multi-AZ RDS, DynamoDB
  - Multi-region architectures, CloudFront, Route 53, S3 Cross-Region Replication (CRR)

Encryption

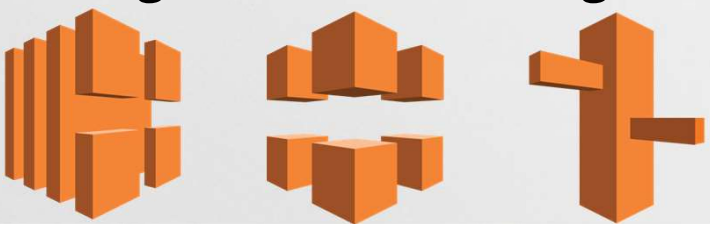
- Encryption services are provided by AWS, but it is up to you to operate them securely and protect the keys
- You can manage and control the keys yourself or let AWS handle it for you
- Server Side Encryption (SSE) is freely available for storage (S3, EBS, Snapshots)
- AWS Key Management Service (KMS) is a managed symmetric key service
  - You retain control of your regional Customer Master Key (CMK)
  - S3 SSE-KMS encryption of objects leverages KMS and your CMK
- Cloud Hardware Security Modules (HSMs) are AWS managed physical hardware appliances available for storing your self-managed symmetric and asymmetric keys
- AWS Certificate Manager (ACM) helps easily create and manage public certs

Web Application Firewall (WAF)

- Managed WAF service to protect your web applications (e.g. OWASP Top 10)
  - Integrates with the Application Load Balancer (ALB) or CloudFront CDN
- Configured by rules that inspect CF traffic
  - Conditions = match IPs, strings, regex, etc.
  - Rules = contain conditions with Boolean logic
  - Web ACLs = contain rules and actions (allow, block, count) (default rule = allow all)
- AWS WAS Managed Rules configure your WAF with threat intel from vendors such as: Trend Micro, Imperva, Fortinet, Alert Logic, F5, TrustWave
- AWS WAF Security Automations offer CloudFormation Templates to launch Lambda functions that monitor and dynamically configure the WAF service
- AWS Firewall Manager can be used to managed WAF configurations across accounts/regions

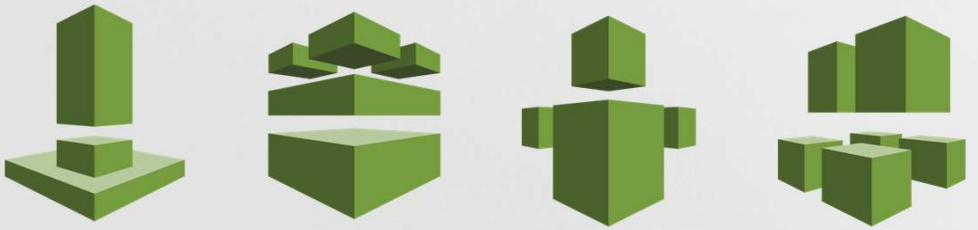
DDoS Mitigation

- AWS provides standard DDoS, MITM, IP spoofing, port-scanning, packet sniffing for VPCs
- AWS Shield Standard||Advanced can also assist with mitigating DDoS attacks
- Use auto-scaling policies to absorb a DDoS attack by rescaling the instance size with “Enhanced Networking” or scaling the pool of EC2 instances with ELB
- ELB can only forward sane TCP connections – SYN floods and other DDoS packets (UDP reflection, ICMP flood) are dropped
- AWS CloudFront with AWS WAF can block attacks from AWS edge locations
- AWS Route 53 can absorb DNS flooding attacks through shuffle sharding and anycast striping



Security Management & Visibility

- AWS offers several services to help you managed your security
- Amazon Inspector performs an automated security assessment, compares your operations to best practices, gives you prioritized remediation steps
- AWS Config Rules helps you monitor your resource inventory and perform change management and monitor changes recorded by AWS Config
- AWS Trusted Advisor reviews your security settings with you and provides areas for improvement (cost, HA, performance, etc.) Full version for Business and Enterprise Support plans
- AWS EC2 Systems Manager can help you keep your systems patched/maintained



Security Management & Visibility (Cont.)

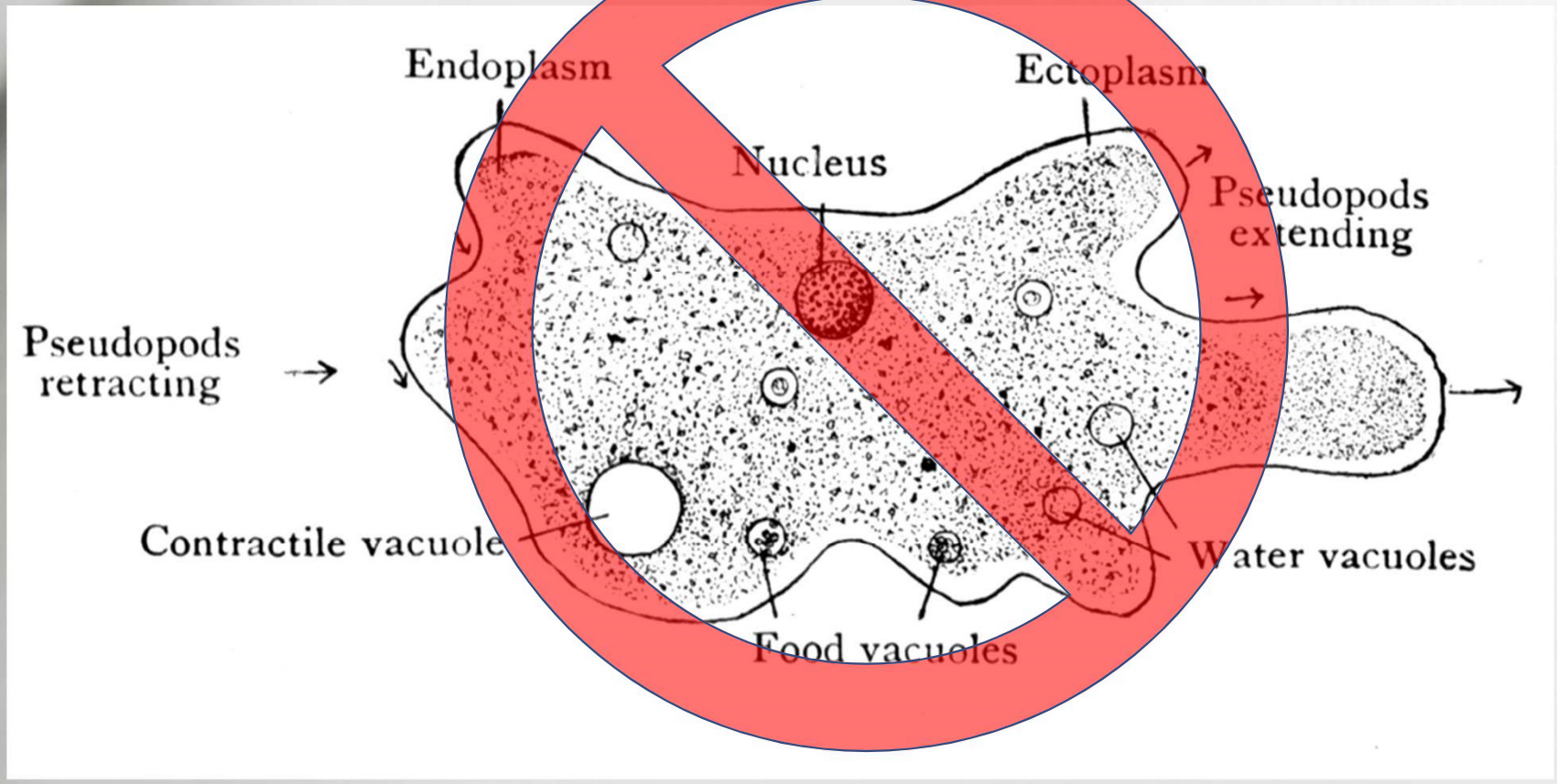
- AWS CloudWatch Logs gives you visibility to your services, metrics, logs, alarms, etc. (standard 5 minute polling, detailed 1 minute polling) ~10 minute latency
- AWS CloudWatch Events provides near real-time changes (Events, Rules, Targets)
- AWS CloudTrail provides detailed logging and auditing service, records API events, API call history, change tracking for compliance or forensics (encrypt the data)
- VPC Flow Logs show you network traffic traversing your VPC subnets
- Amazon Macie AI-powered service discovers PII and prevents data loss
- You can easily report abuse and vulnerabilities, AWS will also proactively notify you of issues

AWS Security Marketplace

- AWS has a security ecosystem whereby you can acquire additional security components to compliment your public cloud (BYOL, pricing based on EC2 instance these run on)
- AWS Marketplace offers many popular cloud security vendor Add-Ons
  - Cisco, Palo Alto Networks, Check Point, Fortinet, Juniper, Splunk, Alert Logic, Trend Micro, Symantec, Sophos, McAfee, Barracuda, VyOS, 40Cloud, Intel Security, Okta, Gemalto, SafeNet, Imperva Incapsula, F5, A10, Avi Networks, Brocade, OpenVPN, Pulse Secure, Soha, Aviatrix, Qualys, Tenable, Rapid7, Radware, Dome9, Evident.io, Threat Stack, HyTrust, Kali, Sift Security, Aqua, Allgress, & numerous others
- You can “Test Drive” security solutions in AWS & see if you like them

Live Demonstration of AWS Security

No Amoebas!


Endoplasm
Ectoplasm
Nucleus
Pseudopods extending
Pseudopods retracting
Contractile vacuole
Water vacuoles
Food vacuoles

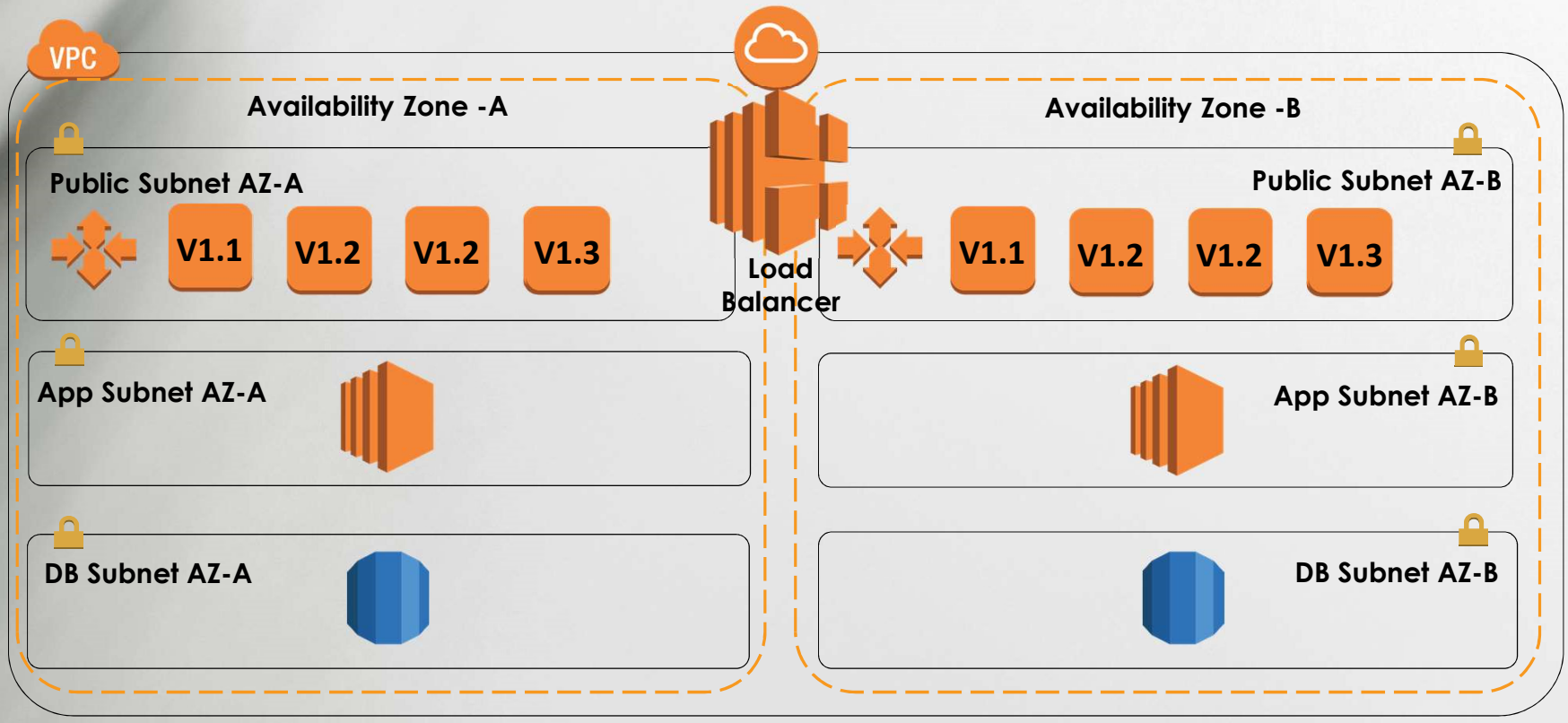
Scriptable Infrastructure – Security as Code

- If you're using the "AWS Management Console", you're doing it wrong!
- Take a page from the DevOps handbook and AUTOMATE!
- NIST AWS CloudFormation Templates (CFTs)
- Ansible playbooks with Boto3 and Python
- AWS CLI Commands, Newer (1.15.X) == Better
- Automate your compliance checking, patching
- Create a CI-CD pipeline for hardened images: STIG-a-TRON

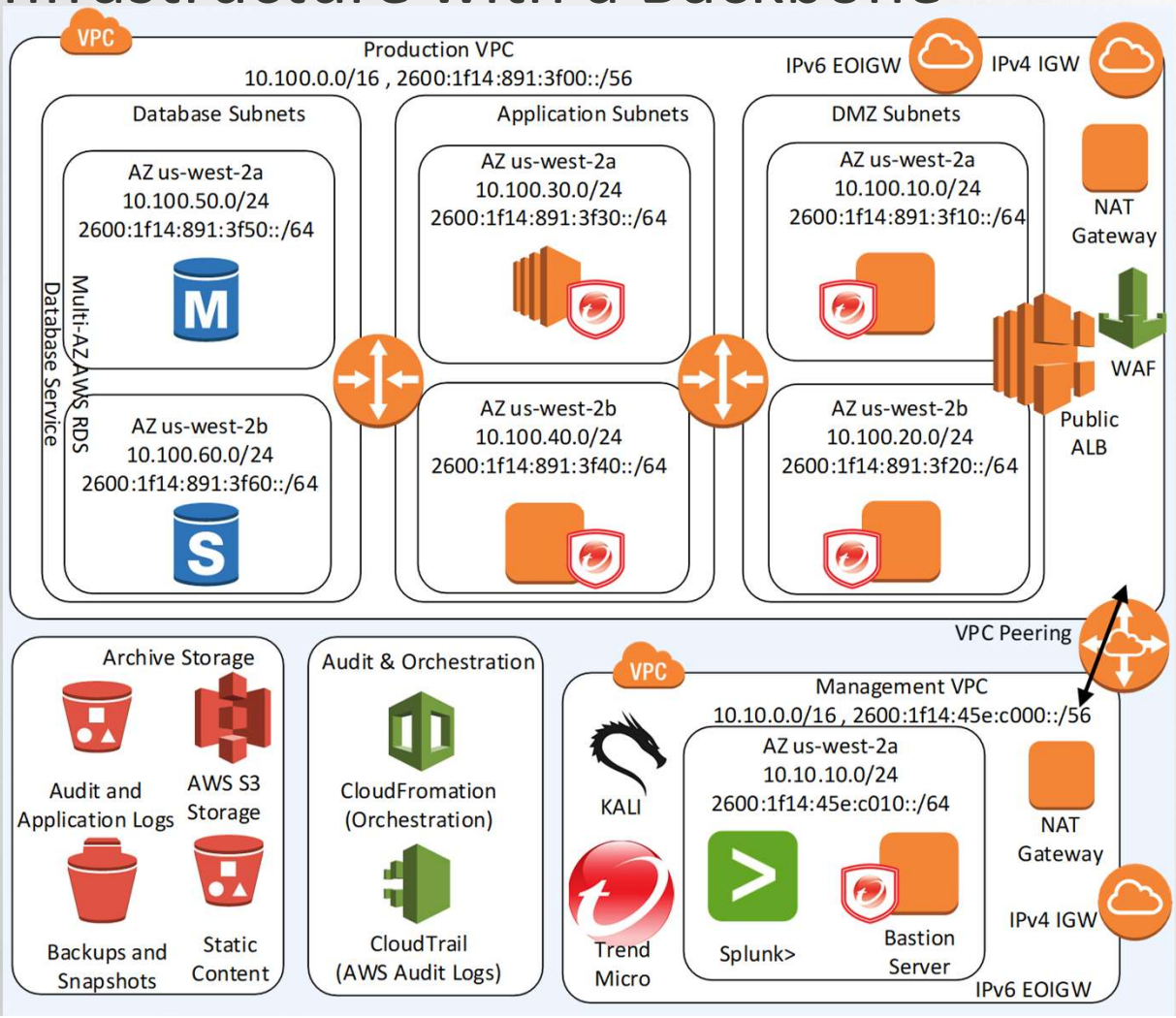


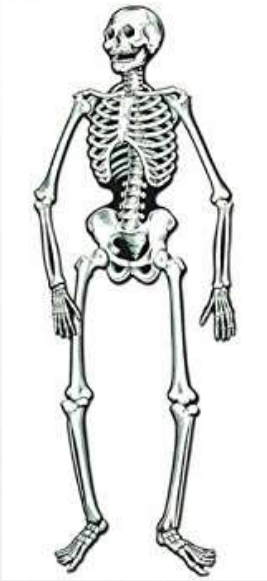



Cloud Security Through Elasticity



Cloud Infrastructure with a Backbone





Cloud Security Certifications

Certificate of Cloud Security Knowledge

- The CSA created a certification for individuals
- Validates that someone has the understanding and skills to help protect an organization who is consuming cloud services
- The CCSK shows you the best practices and things to consider when protecting cloud-based assets
- The CCSK domains provide a holistic cloud security controls framework
- Even if you don't pursue the certification their free documentation provides great advice on cloud security

CCSK Body of Knowledge Domains

- CCSK Guidance V4 has 14 domains

1. Cloud Computing Concepts and Architectures
2. Governance and Enterprise Risk
3. Legal Issues, Contracts and Electronic Discovery
4. Compliance and Audit
5. Information Governance
6. Management Plane and Business Continuity
7. Infrastructure Security
8. Virtualization and Containers
9. Incident Response
10. Application Security
11. Data Security and Encryption
12. Identity Entitlement, and Access Management
13. Security-as-a-Service
14. Related Technologies

(ISC)^2 Certified Cloud Security Professional (CCSP)

- CSA and (ISC)^2 collaborated on developing a new cloud certification that builds upon the CCSK

CCSP℠ brought to you by (ISC)^2 and CSA cloud security alliance®

CCSP℠ | Certified Cloud Security Professional

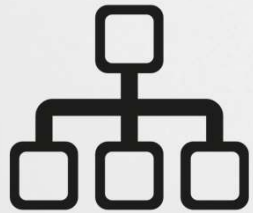
$(ISC)^2$ Certified Cloud Security Professional (CCSP)

- The CCSP Common Body of Knowledge (CBK) consists of the following six domains:
  1. Architectural Concepts & Design Requirements
  2. Cloud Data Security
  3. Cloud Platform & Infrastructure Security
  4. Cloud Application Security
  5. Operations
  6. Legal & Compliance

Summary, Resources, and Q&A

Final Thoughts & Recommendations

- If you have good InfoSec hygiene in your on-premises IT infrastructure, you can have good cloud security operations.
- Cloud services can be less secure, equally secure, or more secure than your traditional on-premises data center.
- Use automation methods whenever possible - DevOps!
- Create AWS accounts with structure – No Amoebas!
- Use built-in AWS security features and services rather than trying to build-your-own
- Leverage No||Low-cost resources available, AWS FREE-Tier account to learn and test security



Valuable (but FREE) AWS Security Resources

- Journey Through the Cloud - Security Best Practices on AWS – Ian Massingham
  - https://www.youtube.com/watch?v=rXPyGDWKHIo
- Advanced Security Best Practices Masterclass
  - https://www.youtube.com/watch?v=zU1x5SfKEzs
- Watch recordings of 2017 AWS re:Invent conference security, compliance & identity sessions
  - https://www.youtube.com/playlist?list=PLhr1KZpdzukcGVzIVFTy-j358ZoK9cvrF
- AWS Security by Design (SbD)
  - https://aws.amazon.com/compliance/security-by-design/
- AWS Security Whitepapers – AWS Security Center
  - http://aws.amazon.com/security/
- Introduction to AWS Security - July 2015
  - https://d0.awsstatic.com/whitepapers/Security/Intro_to_AWS_Security.pdf
- AWS: Overview of Security Processes – May 2017
  - https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf
- AWS Well Architected Framework Security Pillar – Nov ‘17
  - https://d0.awsstatic.com/whitepapers/architecture/AWS-Security-Pillar.pdf
- AWS Security Best Practices – August 2016
  - https://d0.awsstatic.com/whitepapers/aws-security-best-practices.pdf
- AWS: Risk and Compliance, May 2017
  - https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf
- AWS Cloud Adoption Framework Security Perspective – June 2016
  - https://d0.awsstatic.com/whitepapers/AWS_CAF_Security_Perspective.pdf

Questions and Answers

- Are there any questions?
- Thank you very much for your time.
- Feel free to contact me if ever I can ever be of service to you.
  - SHogg@GTRI.com 303-949-4865 @ScottHogg

GTRI®
···· IS NOW ZIVARO ····