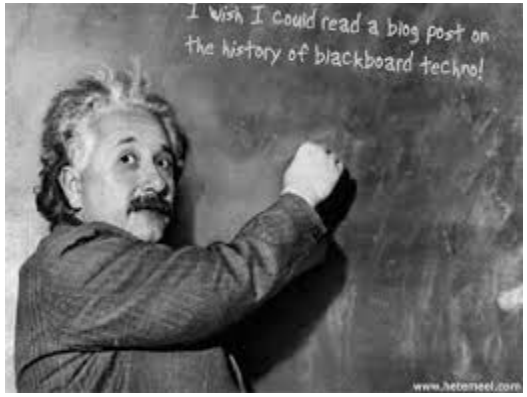
Security Camp 2016
Cloud Security

August 18, 2016

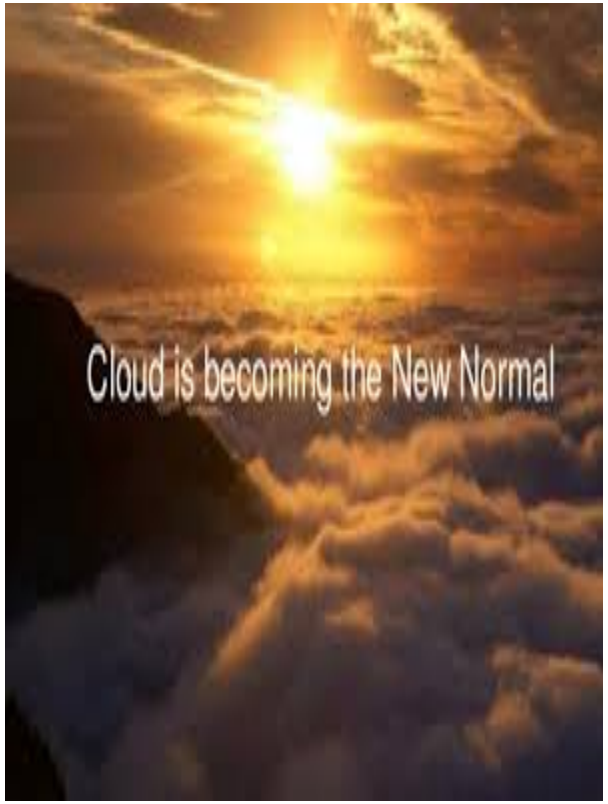
BOSTON UNIVERSITY

What I'll be discussing

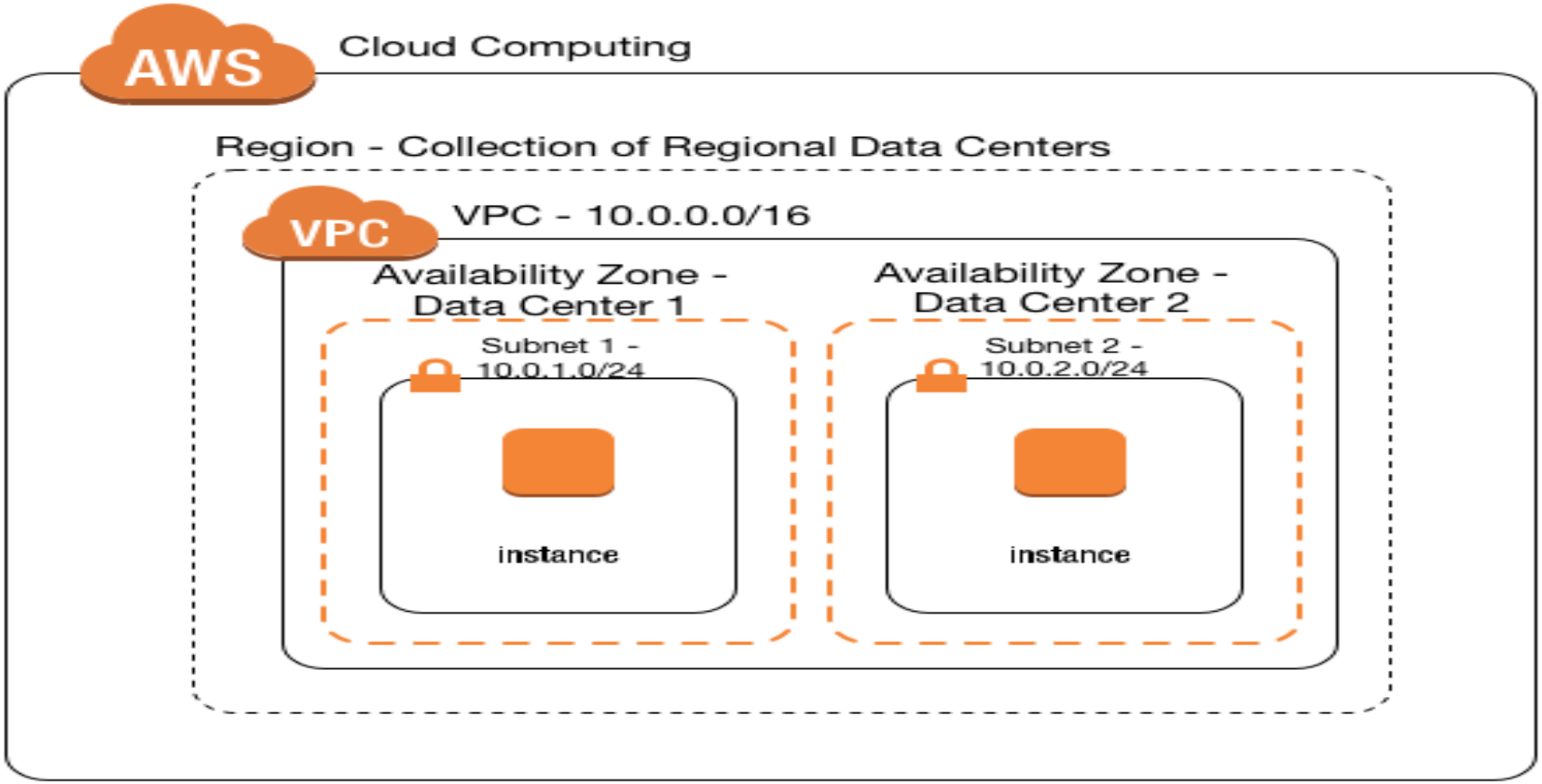
- Cloud Security Topics
  - Cloud overview
  - The VPC and structures
  - Cloud Access Methods
  - Who owns your data?
  - Cover your Cloud trail?
  - Protection approaches
  - Encryption?
  - Breach?
  - EXIT stage left?
  - Not covering OS level stuff
  - No Containerization stuff



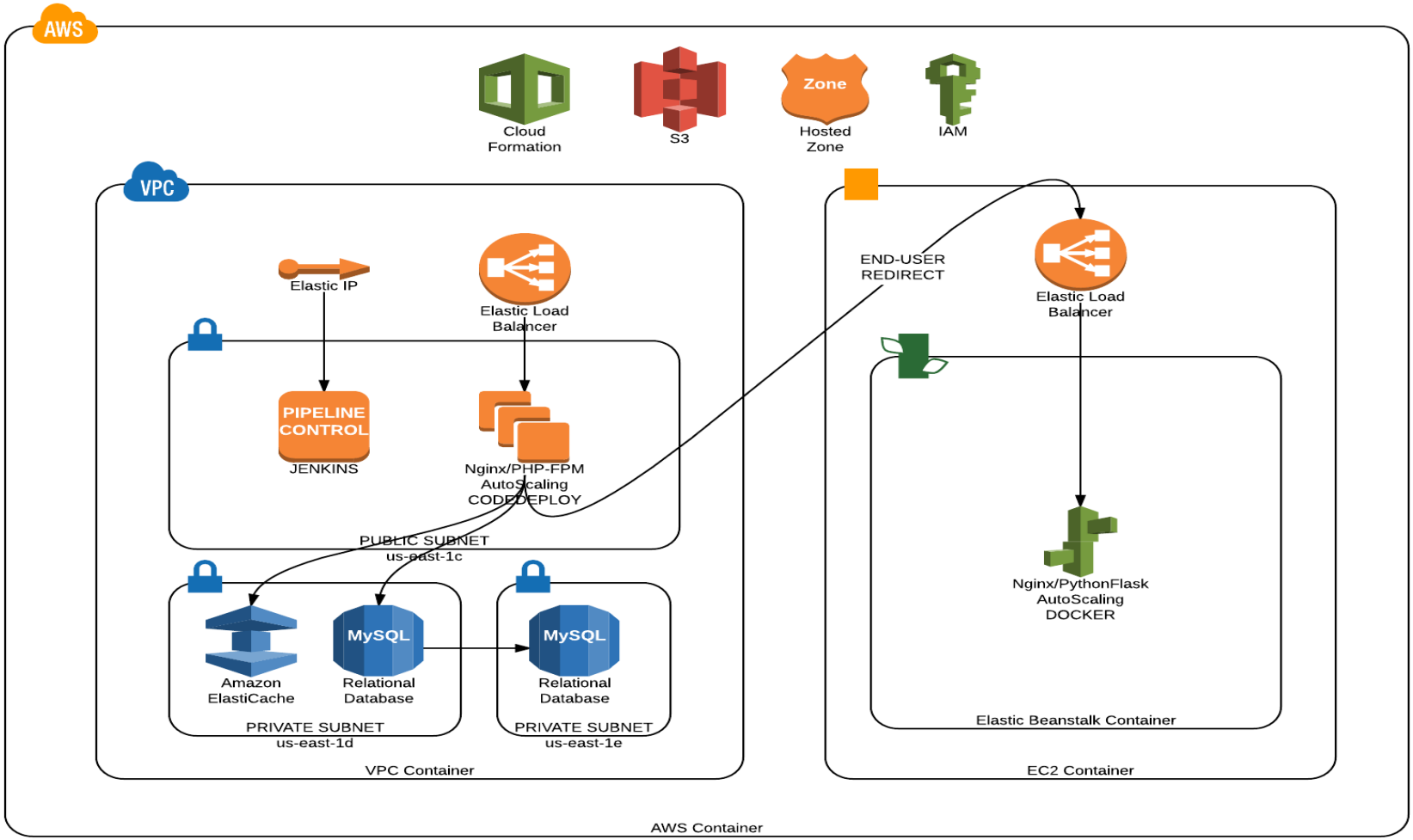
Cloud 101- The Cloud



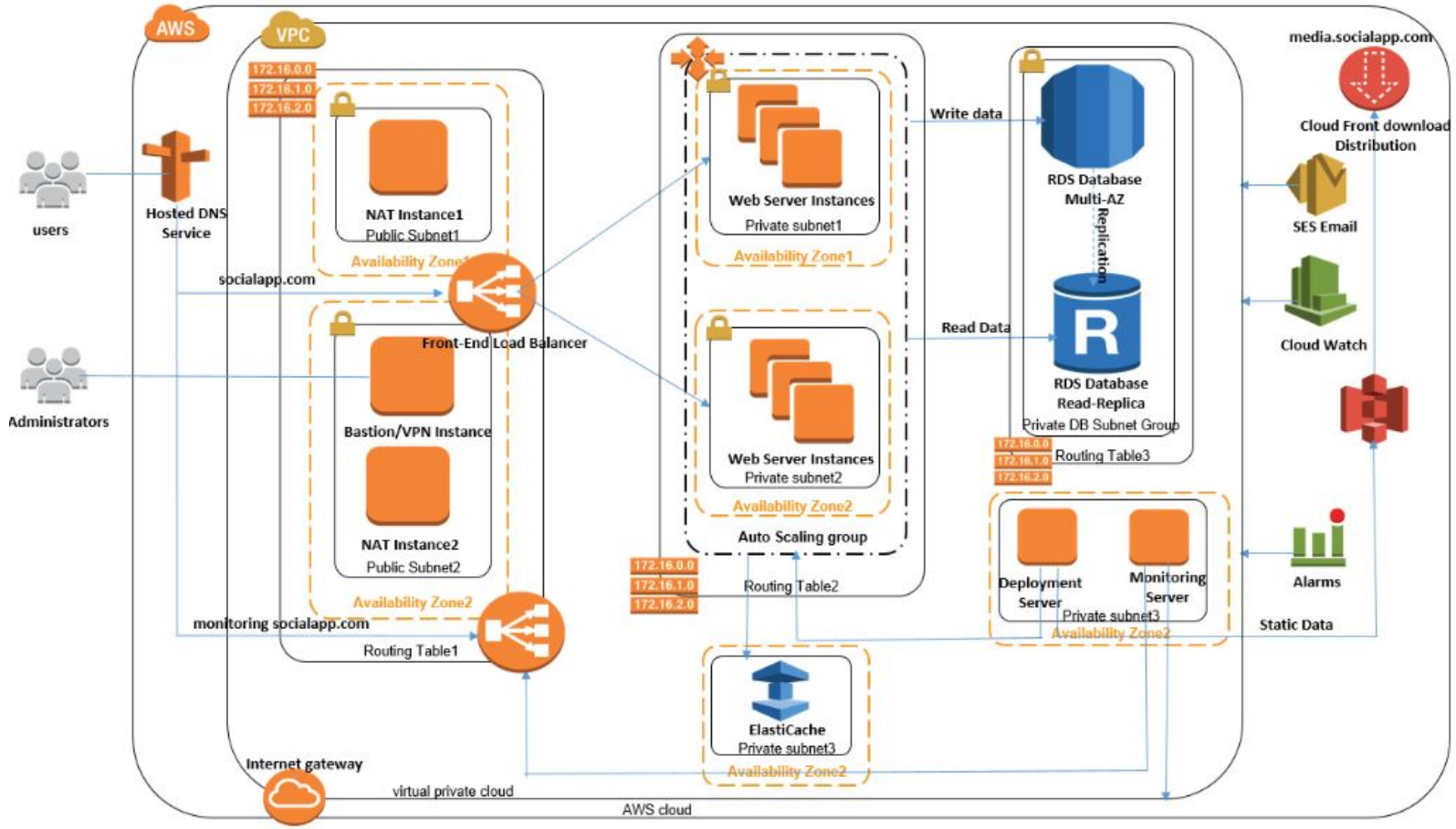
Cloud 201 – The VPC



More complicated example



Cloud Access Methods

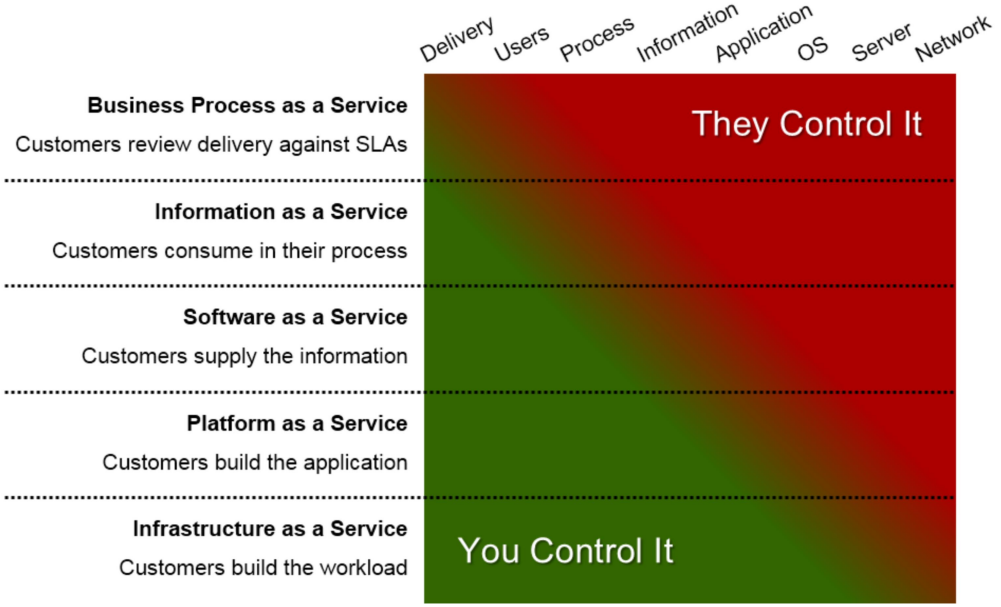


Who owns your data?

Cloud Security Models

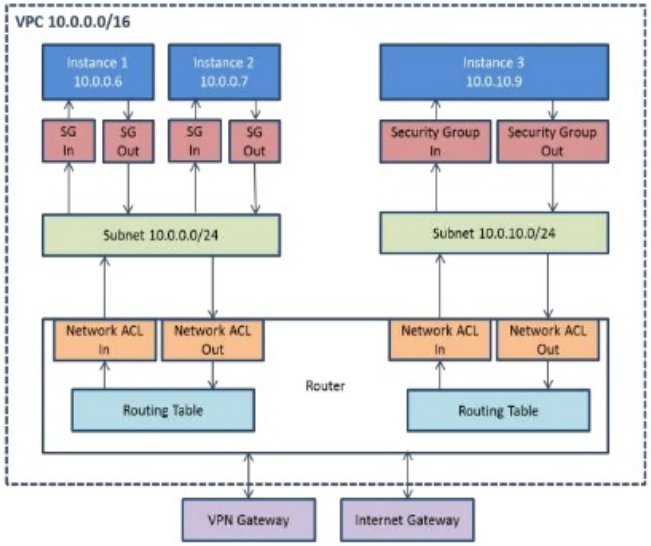
Understand the shared responsibility model

- Ensure cloud consumers and BU teams represent the shared security model for cloud in projects.

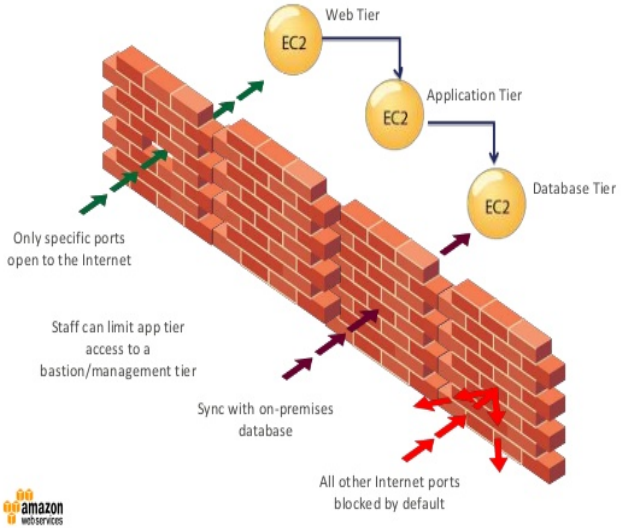


Cloud environment separation

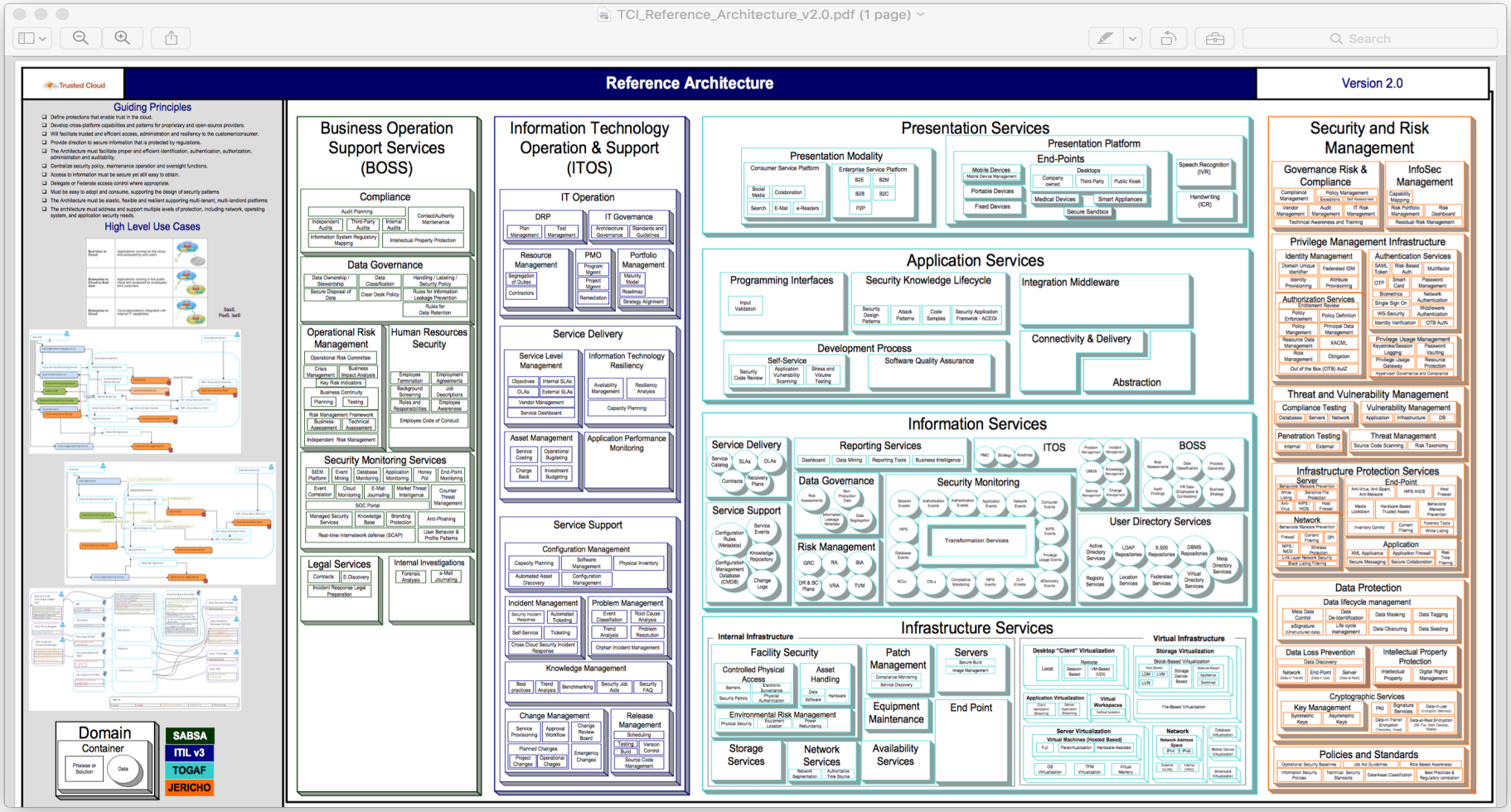
VPC Network Security Controls



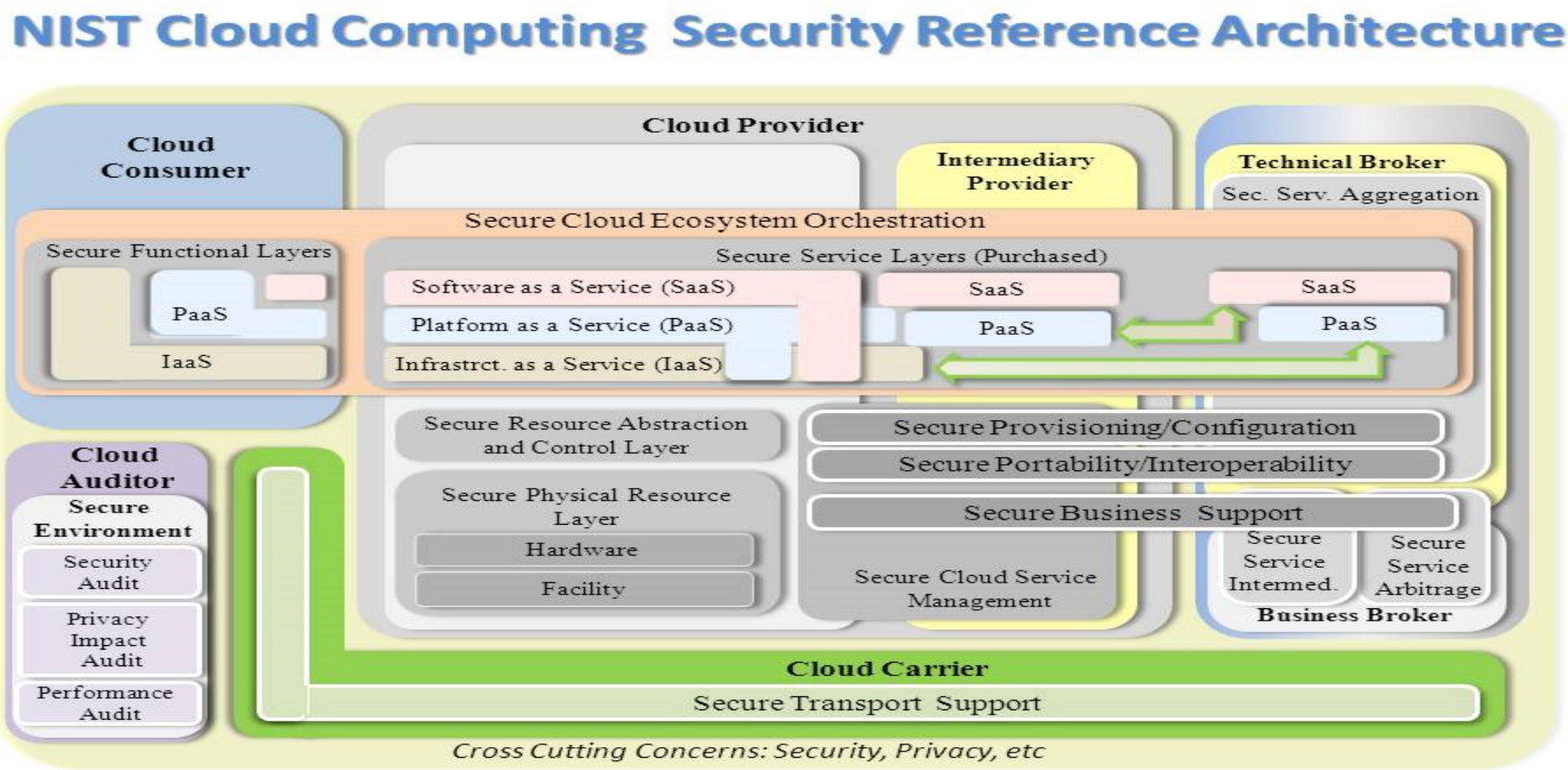
VPC Security Groups



Cloud Computing Reference Architecture 2.0



Cloud Security Reference Architecture

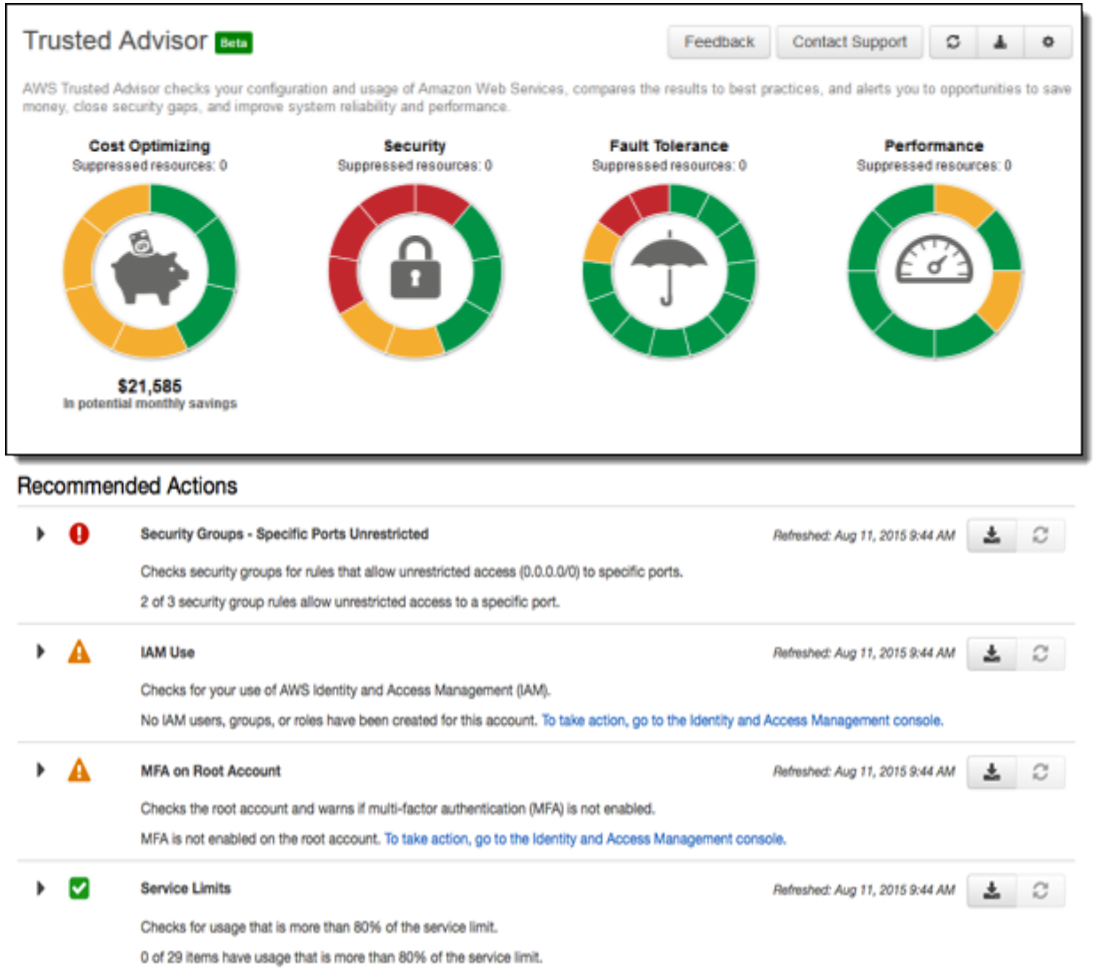


Cloud Security Topics

- **Require Encryption in transit and at rest from cloud providers**
  - Bi directionally and from cloud to cloud (use appropriate service s3,rds,etc.)
    - AWS AZ to AZ, Region to Region ARE NOT ENCRYPTED
  - Use EBS Encryption for block encryption
  - Strong encryption options required
  - Some providers require extra tools (SaaS, IaaS)
  - Start with CSP Managed Keys (Simplified) but study a CloudHSM
    - FIPS 140-2 Level 2 certified
    - Highly secure flash device (AWS Indicates it is NOT a key management system)

Cloud Security Workloads

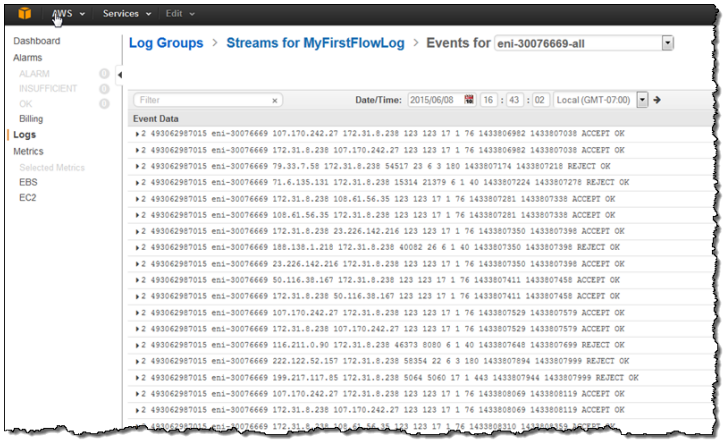
- **Require cloud workloads to be vulnerability scanned**
  - Superior providers have toolsets for workload and instance level scanning. Require their use.
  - Require all custom BU created templates to be security scanned prior to use and over a frequency
  - Review vulnerability disclosures from CSP
  - Review instance security

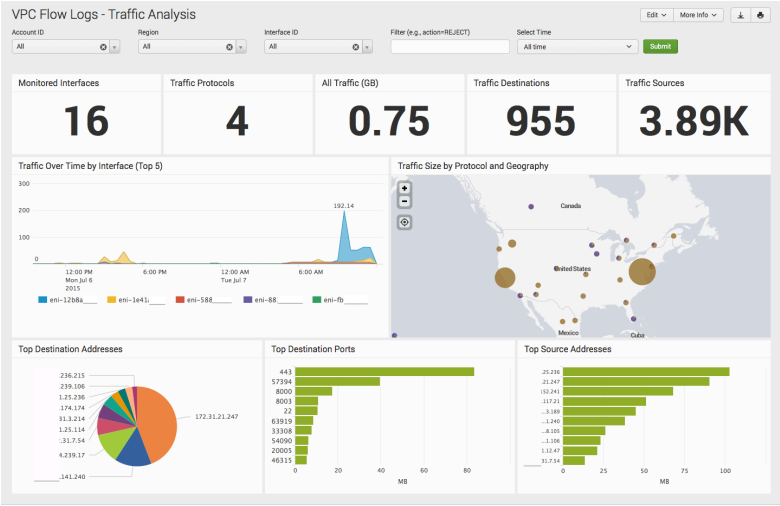


BOSTON UNIVERSITY

Cloud Security History Lesson

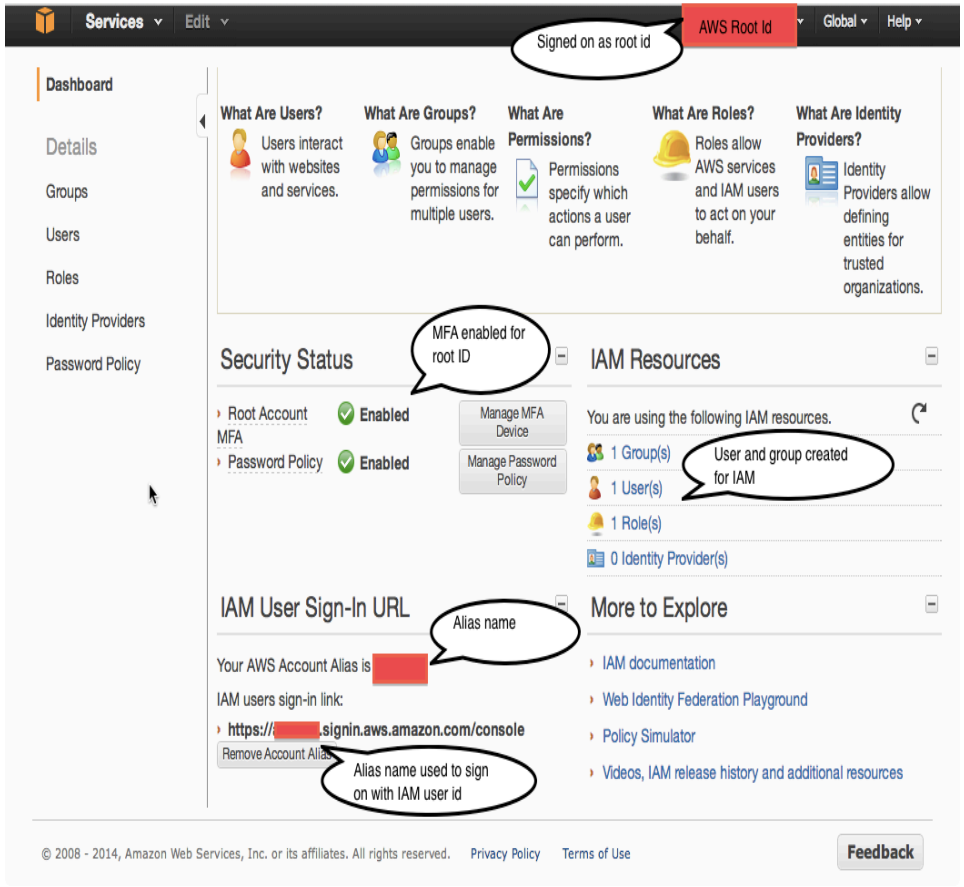
- **Require activation of logs and send them to the security target**
  - cloud trails, VPC flowlogs for AWS – Require xx days in archsite and yy days at provider
  - Only cost is S3 storage of the log files – Build into project budgets





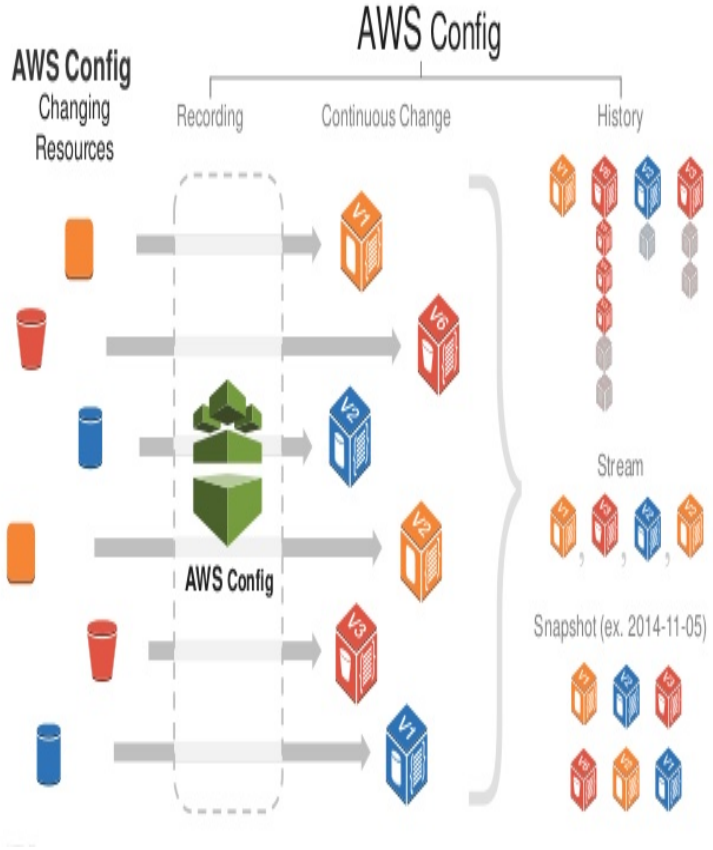
Cloud Security IAM

- **Require IAM for access to the provider and multi-factor authentication**
  - Make person responsible for the architecture document and implement IAM policy
  - Extract and store ROOT Keys within Enterprise Architecture and Systems Cloud Team
  - Federate IAM when possible
  - Use RBAC where possible
  - Ensure MFA is enabled and audit on a regular frequency



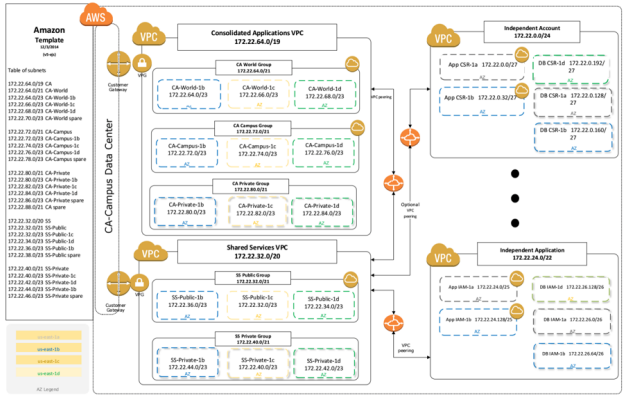
Cloud Security ITIL

- **Require strong access for actions requiring infrastructure changes**
  - Changes to the infrastructure must be documented and communicated via RFC to change manager and approved
  - Changed to VPC IGW/Peering must be approved by your central security team



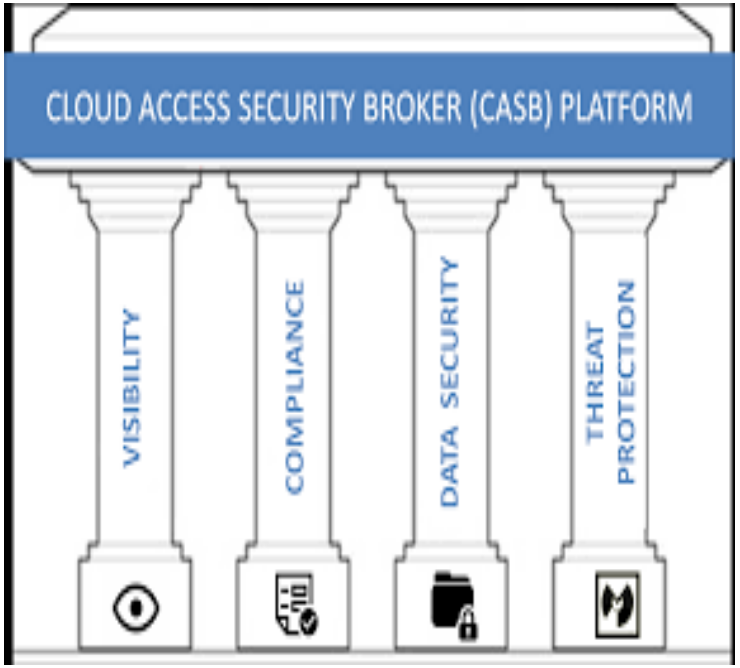
Cloud Security forensics

- **Require security groups and private subnets that peer to send logs "home"**
- **Log (for example)**
  - **API Calls**
  - **CloudTrail**
  - **Console**
  - **S3, EC2, Other**
  - **Elastic Load Balancer Logs**
  - **Cloud Front Content client facing logs**
- **Monitoring and alerting (for example)**
  - **Advanced metering infrastructure changes**
  - **ACL security rule changes**
  - **EBS volumes made public**
  - **ANY monitoring disabled**
  - **CloudTrail logging disabled**
  - **Limits alert or too many instances created, started**
  - **ANY new users created and credentials assigned**
  - **IAM adds of users to groups , account policy changed**
  - **API access keys created/deleted/rotated**
  - **If not federated / user password changed**
  - **DB instance deleted**
  - **Cost optimization changes including, bill increases / resources**
  - **Password guessing attempts**
  - **Encryption Keys created/enabled/deleted**
  - **Implement autonomic thread based on velocity or known bad IP**
- **Implement an account de-provisioning policy for breach or staff separation**

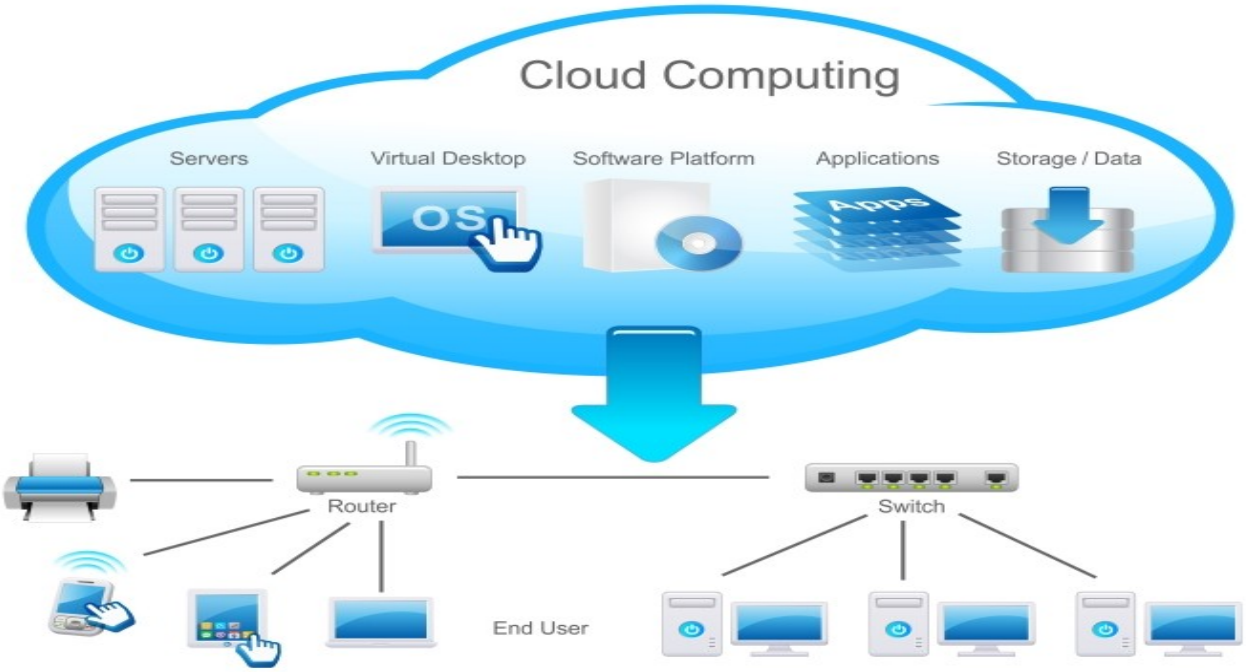


Cloud Security Tooling

- **Require regular cloud scanning reports (SaaS, IaaS, etc.)**
  - Contracts should include the language
  - Cloud providers will produce reports or EA&S teams
- **Evaluate the use of Cloud Access Security Brokers**
  - Provide API level protection to cloud service environments.
  - Apply pressure to current security vendors to provide native support for CSPs.
- **Ensure you have exit language in your contracts providing a grace period for post contract termination retrieval of data**

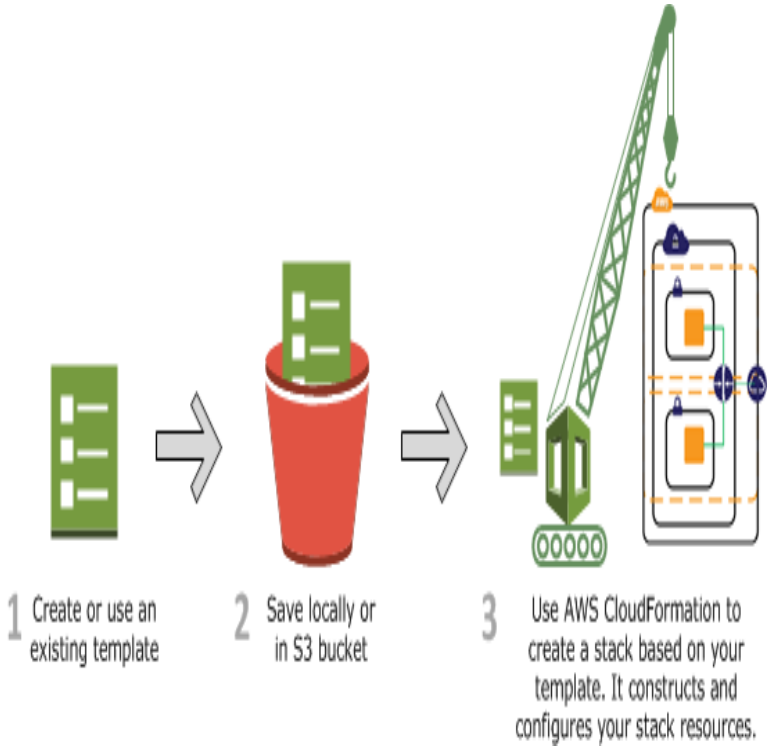


- Network Integration Considerations:
  - Internet2
  - VPN/IPSEC
  - NAT
  - Routing
  - Proxy
  - Public vs Private IP
  - Reporting
  - Security



Cloud Security Strategy

- **Standardize platform creation using architecture patterns and Change Detection**
- **Ensure cloud workloads are not exposed to patching delays**
  - Adopt an ephemeral approach to instance patching utilizing automation
  - Set a requirement in days (Max XX?) for patch application.
  - Adopt managed services where possible and contractually lock patch frequencies
- **Create a breach workflow**
  - Assume a compromise will occur and develop a workflow with responsibilities and signoffs
  - Understand notification process for CSP e.g. aws-security@amazon.com
- **Educate and ensure cloud consumers share the security model for cloud deployments**
- **Ensure you use tagging in CSP**
  - Metadata on cloud assets allow searchable rapid intelligence



Cloud Security Wrap up

Questions?

- Who owns your data?
- Logging up and down the stack
- End to End Encryption – Always
- Ensure backups of configuration data (CLI Exports and CloudFormation)
- Use Multiple Cloud Provider datacenters
- Your Cloud Security Policy enterprise wide
- Evaluate your position quarterly
- Review security bulletins
- What are your backup frequencies and last restoration validation?
- Do your homework

Cloud Security

Reference Notes

- AWS Service Organization Control
- Cloud Security Alliance
- AWS Security Roadshow
- AWS Security Bulletins
- Microsoft Azure Publications
- AWS PGP Public Key for notifications
- Gartner Technical Professional Advice G00260748