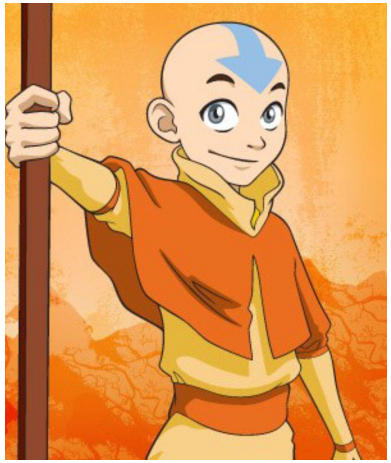
Intro to Cloud Security: Where to Start Patching Your Leaky Clouds

Cloud 102
Henry Canivel

whoami



- Currently an information security architect
- Security professional for 5+ years
- Developer background
- “Log Czar” sounds like a really cool job title
- Originally from the bay area, now in LA for ~2 years
- Interests: food things, travel, streaming, sports, learning new tech, mastering the 4 elements with a happy attitude

Today's Objective

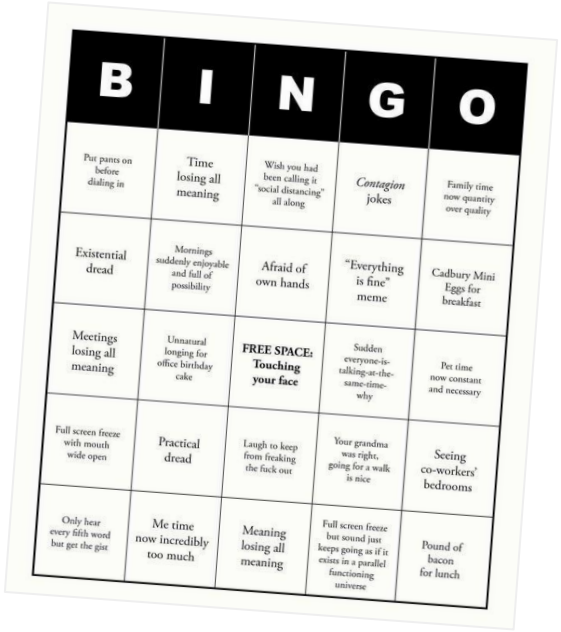
What are we gonna do today, Brain?

Agenda

- Quick cloud intro things
- Problems and Takeaways
- Cloud Risks
- Architectural Considerations
- Cloud Security Tools
- Guidance

This talk is NOT:

- Cloud migration strategy
- Cloud workload planning
- Incident Response
- AppSec
- Taking over the world, sorry



B	I	N	G	O
Put pants on before dialing in	Time losing all meaning	Wish you had been calling it "social distancing" all along	*Contagion* jokes	Family time now quantity over quality
Existential dread	Mornings suddenly enjoyable and full of possibility	Afraid of own hands	"Everything is fine" meme	Cadbury Mini Eggs for breakfast
Meetings losing all meaning	Unnatural longing for office birthday cake	**FREE SPACE: Touching your face**	Sudden everyone-is-talking-at-the-same-time-why	Pet time now constant and necessary
Full screen freeze with mouth wide open	Practical dread	Laugh to keep from freaking the fuck out	Your grandma was right, going for a walk is nice	Seeing co-workers' bedrooms
Only hear every fifth word but get the gist	Me time now incredibly too much	Meaning losing all meaning	Full screen freeze but sound just keeps going as if it exists in a parallel functioning universe	Pound of bacon for lunch

Know your **cloudy** terms

Some Buzzwordy words for Cloud

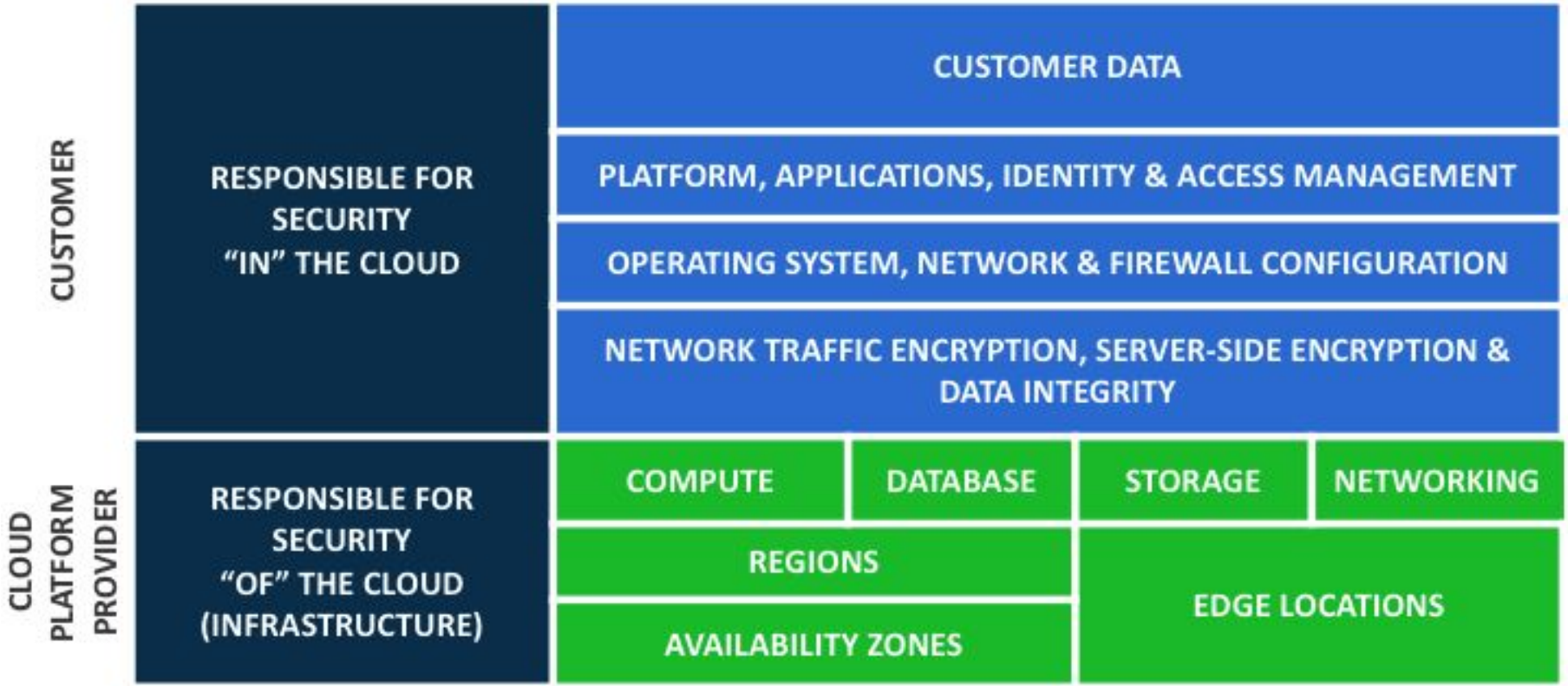
Common Cloud Terms

- Cloud Service Provider (CSP)
- Elasticity
- Private Cloud
- Public Cloud
- Serverless computing
- Software as a Service (SaaS)
- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)

Cloud Security Tool Categories

- Cloud Access Security Broker (CASB)
- Cloud Security Posture Management (CSPM)
- Cloud Workload Protection Platform (CWPP)

Shared Security Model


CUSTOMER
CLOUD PLATFORM PROVIDER
RESPONSIBLE FOR SECURITY "IN" THE CLOUD
RESPONSIBLE FOR SECURITY "OF" THE CLOUD (INFRASTRUCTURE)
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
NETWORK TRAFFIC ENCRYPTION, SERVER-SIDE ENCRYPTION & DATA INTEGRITY
COMPUTE
DATABASE
STORAGE
NETWORKING
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

Target Audience: IT/Security teams

Problems

- Lack of visibility
  - What is deployed
  - How are resources configured
  - Where they're located
  - When these events happened
- Cloud account sprawl
- Manual inspection
- Baselining consistent control verification
- … and more!

Intended Takeaways

- Crystalize areas of concern
- Identify plausible options
- Prioritize remediation
- Centralize visibility
- Identify
  - Critical assets
  - Publicly accessible resources
  - Ingress points and permissions
  - Who has access? (IAM principals)
  - Audit controls configured


START
HERE


WELCOME TO THE
PARTY, PAL.
IFC

THE FOUR HORSEMEN

OF ~~THE APOCALYPSE~~

CLOUD SERVICES

Cloud Service Portfolio

Compute Services			
Services	*AWS*	*Azure*	*GCP*
IaaS	Amazon Elastic Compute Cloud	Virtual Machines	Google Compute Engine
PaaS	AWS Elastic Beanstalk	App Service and Cloud Services	Google App Engine
Containers	Amazon Elastic Compute Cloud Container Service	Azure Kubernetes Service (AKS)	Google Kubernetes Engine
Serverless Functions	AWS Lambda	Azure Functions	Google Cloud Functions
Database Services			
Services	*AWS*	*Azure*	*GCP*
RDBMS	Amazon Relational Database Service	SQL Database	Google Cloud SQL
NoSQL: Key–Value	Amazon DynamoDB	Table Storage	Google Cloud Datastore Google Cloud Bigtable
NoSQL: Indexed	Amazon SimpleDB	Azure Cosmos DB	Google Cloud Datastore
Storage Service			
Services	*AWS*	*Azure*	*GCP*
Object Storage	Amazon Simple Storage Service	Blob Storage	Google Cloud Storage
Virtual Server Disks	Amazon Elastic Block Store	Managed Disks	Google Compute Engine Persistent Disks
Cold Storage	Amazon Glacier	Azure Archive Blob Storage	Google Cloud Storage Nearline
File Storage	Amazon Elastic File System	Azure File Storage	ZFS/Avere
Networking Services			
Services	*AWS*	*Azure*	*GCP*
Virtual Network	Amazon Virtual Private Cloud (VPC)	Virtual Networks (VNets)	Virtual Private Cloud
Elastic Load Balancer	Elastic Load Balancer	Load Balancer	Google Cloud Load Balancing
Peering	Direct Connect	ExpressRoute	Google Cloud Interconnect
DNS	Amazon Route 53	Azure DNS	Google Cloud DNS

What are the Primary Concerns Across the Cloud Service Categories?

Compute Services -

- Access control
- Asset management
- Location (zone)
- Integrity of critical business services and ops

Storage Service -

- Encryption
- Availability
- Backup strategy
- Public exposure, access controls

Database Services -

- Data access
- Compliance and Audit
- Object level control

Networking Services -

- Approved data flows/safelisted connection sources
- Standard network segmentation (QoS, trust zones)
- Nested controls

What about **Identity Management**?

Identity and Access Control Management

Principal - Person or application used to impersonate and make requests to execute actions or operations

Sample IAM objects include: user, group, role, policy, and identity provider objects

Request - Each request to the CSP management console includes the following: actions/operations, resources, principal, environment data, resource data

Authentication - Various methods to authenticate. Need to determine company strategy for approved methods.

Authorization - Need to know understand expected usage for the environment and roles to enforce as guard rails

Actions or operations - Identify all types of operations that may affect user permissions, per CSP

Resources - Other CSP objects, like storage buckets, other IAM objects, compute


WHAT AM I MISSING?

Some *(more advanced)* examples...

- Encryption/Key Management strategy
- Workload Management strategy
- Backup strategy
- Establish Baseline to determine configuration drift
- Third party tools/integrations
- Alignment with Corporate Initiatives
- ...


WHERE
TO
START
?

Recommendation: Isolate your problem(s) or tool(s)

- Cloud Access Security Broker (CASB)
  - Visibility of security for systems and data transfer to and from cloud services
  - Enterprise visibility of SaaS with custom capabilities to add PaaS and IaaS, contingent on the third-party tool
- Cloud Security Posture Management (CSPM)
  - Cloud configuration deployment and operational monitoring insights for IaaS to SIEM and analytics platforms
  - Aims to provide the enterprise with a coherent security and risk picture across multiple IaaS clouds
- Cloud Workload Protection Platform (CWPP)
  - Workloads deployed within cloud environments and in containers, and it also integrates with SIEM and analytics tools
  - Because it operates in the data plane, it can provide visibility of communications between workloads within IaaS clouds.

CASB vs. CSPM vs. CWPP

Table 4. Data Security Approaches Using Cloud Security Tools

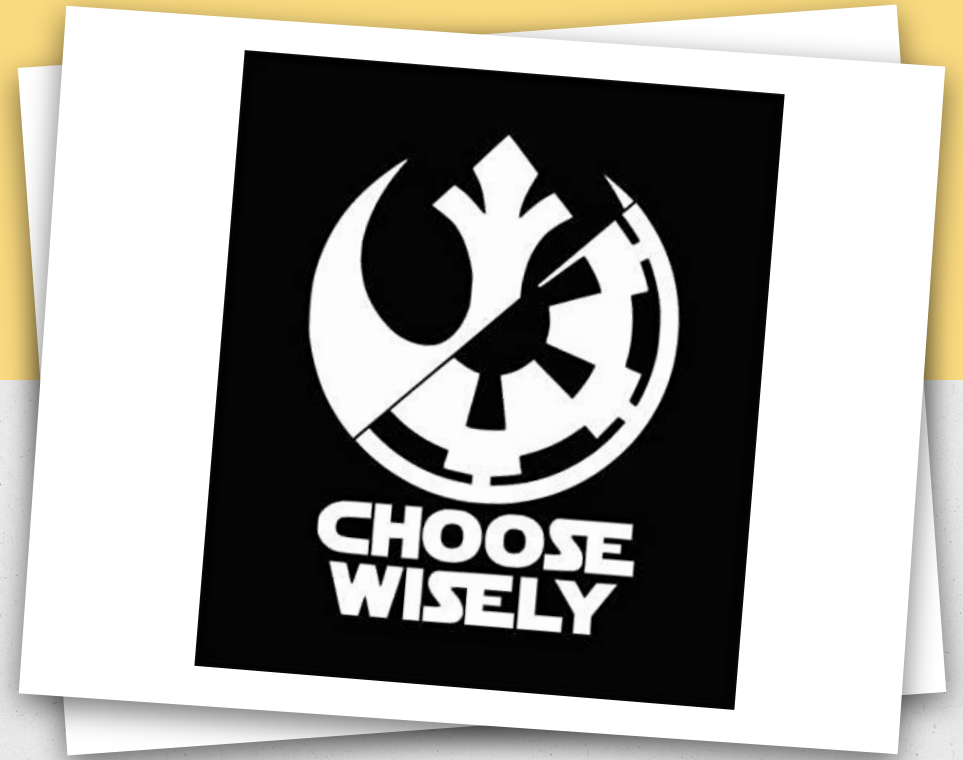
Cloud Security Tool Group	Data Security Capability	Operation
CASB	▪ Data loss prevention — basic DLP, regular expressions (regex), custom dictionary and so on ▪ Encryption in SaaS ▪ Encryption in transit ▪ Monitoring IaaS data storage configuration ▪ Assuring native data security is in place	Protects by encrypting data in transit. Protects at application layer by identifying and preventing unauthorized data transfer.
CSPM	▪ Monitoring IaaS data storage configuration ▪ Assuring native data security is in place (such as Transport Layer Security [TLS]) ▪ Key management oversight	Protects by assuring native and vendor data security controls are in place and operating correctly.
CWPP	▪ Data in transit ▪ Host encryption	Protects at the workload by encrypting the workload itself; some vendors encrypt unsecured data transfers between workloads.

Source: Gartner (August 2018)

Table 2. Deployment Approach Differences

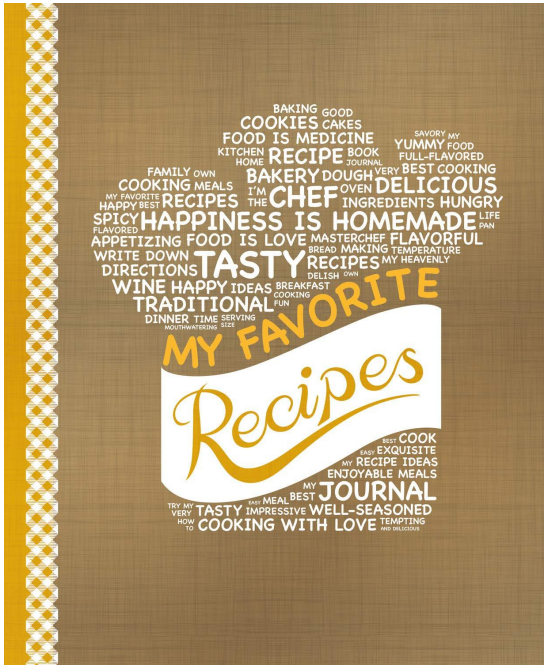
Tool Category	In-Environment/On Workloads	In-Line (Reverse or Forward Proxy)	Enterprise-Integrated	Out-of-Band/ Monitor Only
Cloud Security Posture Management	Some vendors support workload monitoring agent in IaaS	Not featured	Primary deployment pattern to integrate with cloud provider management APIs	Can be deployed to just monitor and alert; however, does need integration to gain access to data feeds
Cloud Access Security Broker	Some vendors support workload monitoring agent in IaaS	Primary deployment pattern for traffic monitoring, data protection and shadow IT discovery	Pattern for integrating with PaaS and SaaS services to support direct API control; some vendors integrate with IaaS cloud admin consoles	Can be deployed to just monitor and alert; needs integration to obtain access to data feeds
Cloud Workload Protection Platform	Primary deployment pattern, monitoring workloads from within environment; management can be in-environment or cloud-based.	Not featured	Can operate independently or integrate with enterprise systems, including cloud-native systems	Cannot be deployed to operate out-of-band; however, can operate in monitor and alert only

Source: Gartner (August 2018)


CHOOSE
WISELY

WHY CSPM (Cloud Security Posture Management)?

1. Initiate
2. Baseline
3. Automate



WHY Cloud Security Posture Management (for me)?

- Minimize impact to developer workloads
- Visibility to environment, users, assets, control policies
- Critical for detection & monitoring, incident response:
  - Assets & Identities
  - Environment/service ownership
  - Visibility >> Action
- Driven by multi-discipline decision-making (for action)
- Programmatic support to enrich SIEM

Sample CSPM tools

Open Source

- Aqua Security - Cloudspoit
- Cloud-custodian
- Cloud-reports
- cs-suite
- CyberArk - AWStealth
- Duo Labs - cloudmapper
- prowler
- Salesforce - policy_sentry
- ScoutSuite

Vendor

- Alert Logic
- BMC
- Cavirin
- CloudCheckr
- DivvyCloud
- Dome9
- Fugue
- Komiser
- Palo Alto Networks Prisma Cloud
  - Formerly Evident.io, RedLock
- Saviynt
- Turbot

References

Links for days

References

URLs

https://aws.amazon.com/blogs/security/how-to-use-trust-policies-with-iam-roles/
https://github.com/MarkSimos/MicrosoftSecurity/blob/master/Azure%20Security%20Compass%201.1/AzureSecurityCompasslhttps://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF
https://www.nist.gov/topics/cloud-computing-virtualization
https://csrc.nist.gov/Topics/technologies/cloud-computing-and-virtualization
https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp
https://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/WebHome
https://www.cisecurity.org/blog/shared-responsibility-cloud-security-what-you-need-to-know/
https://medium.com/@ubersecurity/part-1-aws-continuous-monitoring-f39f81ea6801
https://medium.com/@ubersecurity/part-2-aws-monitoring-case-studies-9fbc613aff28
https://medium.com/bridgecrew/terragoat-vulnerable-by-design-terraform-training-by-bridgecrew-524b50728887
https://summitroute.com/downloads/aws_security_maturity_roadmap-Summit_Route.pdf
https://rhinosecuritylabs.com/gcp/iam-privilege-escalation-gcp-cloudbuild/
https://cloudsecurityalliance.org/blog/2019/10/01/cloud-security-posture-management-why-you-need-it-now/

training

https://aws.amazon.com/training/course-descriptions/security-fundamentals/
https://www.aws.training/Details/eLearning?id=49720

References

tools

https://github.com/toniblyx/my-arsenal-of-aws-security-tools
https://github.com/salesforce/cloudsplaining
https://cloudonaut.io/show-your-tool-parliament/
https://github.com/mykter/aws-security-cert-service-notes
https://www.marcolancini.it/2020/blog-tracking-moving-clouds-with-cartography/
https://github.com/cloud-custodian/cloud-custodian
https://github.com/toniblyx/prowler
https://github.com/duo-labs/cloudmapper
https://github.com/tensult/cloud-reports
https://github.com/cyberark/SkyArk/tree/master/AWStealth
https://github.com/salesforce/policy_sentry
https://komiser.io/
https://cloudsploit.com/
https://www.skyhighnetworks.com/product/skyhigh-for-amazon-web-services/
https://github.com/nccgroup/ScoutSuite
https://github.com/SecurityFTW/cs-suite