

RSA®Conference2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: CSV-T10

CONFESSIONS OF A CLOUD SECURITY CONVERT

Michael Farnum

Solutions Architect Manager

Set Solutions

@m1a1vet



#RSAC

Alternative Titles



- The Adventures of a Network Security Guy to Find the Cloud
- There and Not Back Again... Because I Got Lost in the Cloud. Whose Computer Is This Again?
- That time when a network security guy moved to application security at about the time when cloud was really maturing and getting popular and how he missed a bunch of stuff and the cloud scared him and he didn't trust it and some people had to drag him kicking and screaming to the cloud so he would admit he was wrong...



The Quest!

I'm a geek...



... and kind of a dork too.



Using D&D as a metaphor for My Quest



- I view each challenge as a monster that I had to fight
- Each monster has a challenge rating (CR)
- CRs usually are calculated based on 4 party members
- CR of each monster did not necessarily get higher as I moved through my quest (at least, not the way I see it)
- So, without further ado, I present to you...

Securelantia



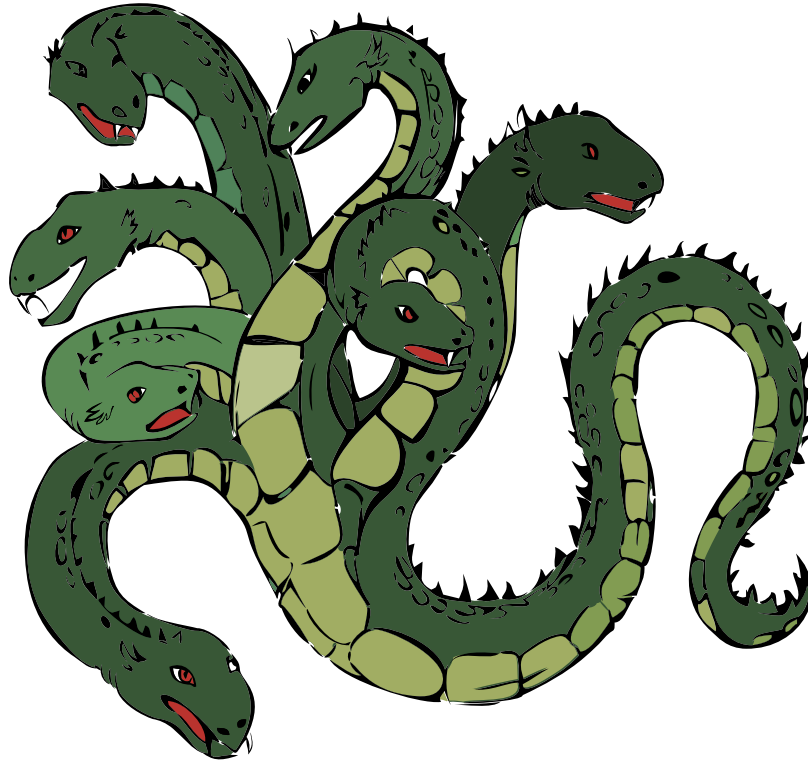
King Ogre of Prejudice



Earth Elemental of the Perimeter



Hydra of Confusion



Shadow Dragon of Data Protection



Future Monsters



Your Hero!



More Like...



Securelantia



King Ogre of Prejudice (CR = 7)



- Trusting the cloud PERSONALLY, not professionally
- It just FELT wrong
- Who could get to my stuff?
- **Full paranoia mode**

How Quickly We Change...



Carol
@Carols10cents



1998:

- Don't get in strangers' cars
- Don't meet ppl from internet

2016:

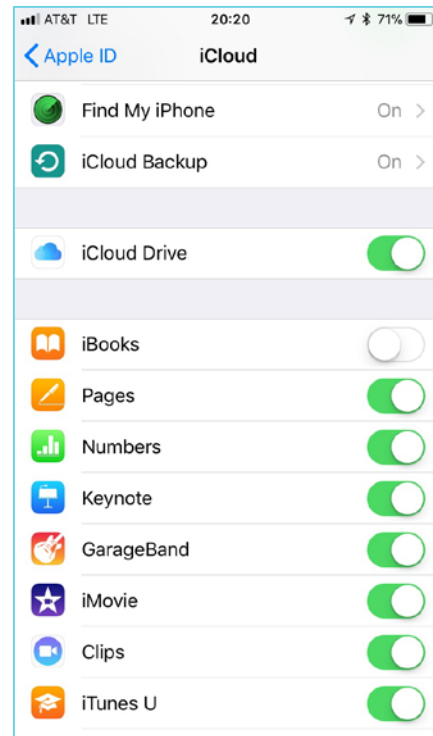
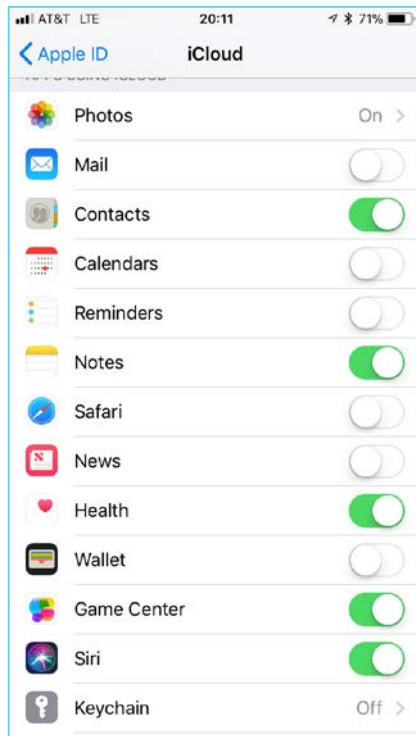
- Literally summon strangers from internet to get in their car

7/2/16, 01:17

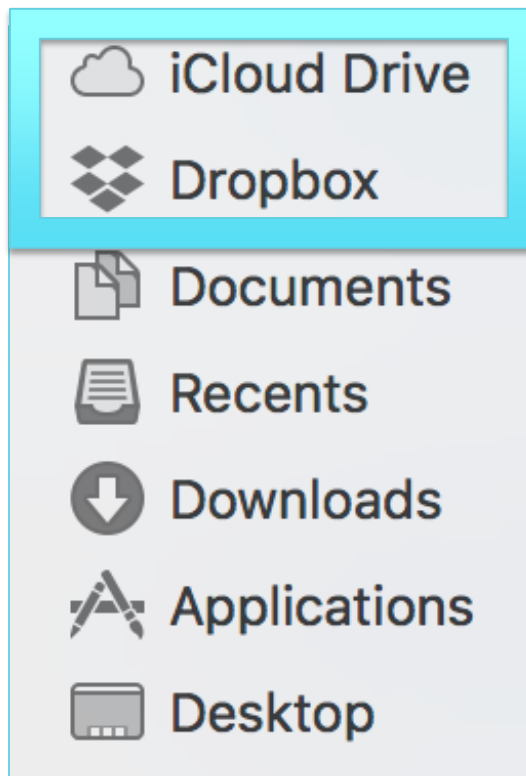
How Quickly We Change...



#RSAC



How Quickly We Change...



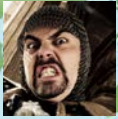
How I Killed the King Ogre



- Took some time
- No major iCloud breaches (some compromised accounts)
- Saw that Cloud was not going away
- Took some measures to use the Cloud securely
- Realized that potential gains outweighed the risks



Securelantia



Earth Elemental of the Perimeter (CR = 5)

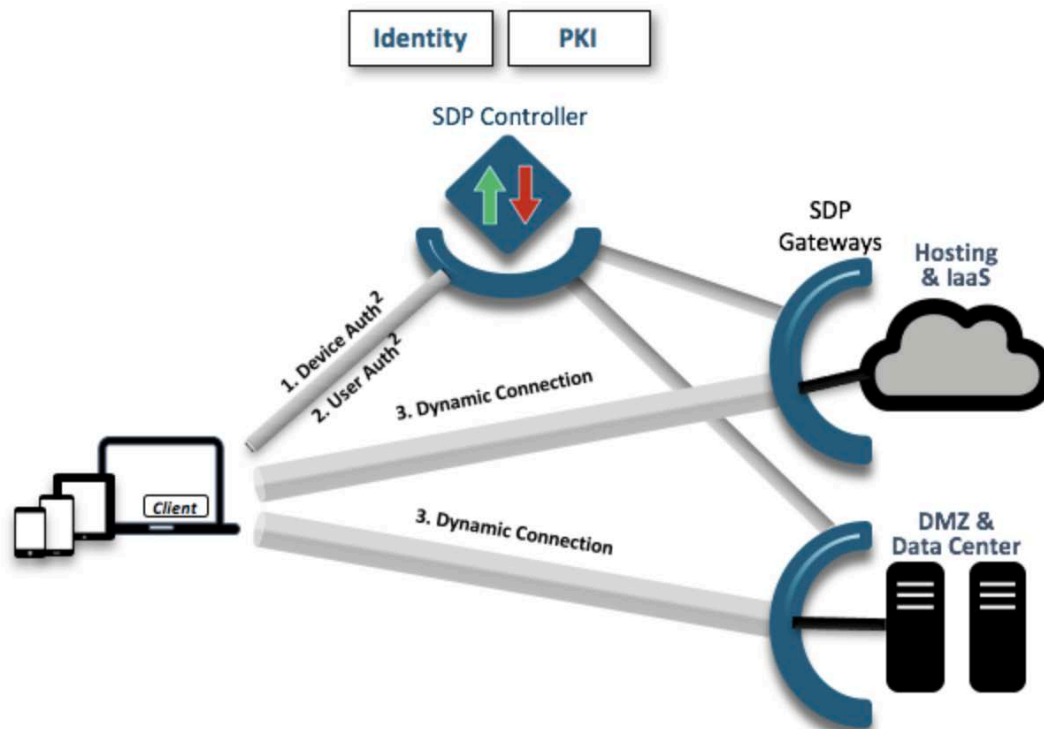


- I had already been primed for this
 - Mobile endpoints were already prevalent
 - Did the perimeter actually disappear or did it really just change?
- Software-defined perimeter was my biggest challenge

The wall never fell...



Software-Defined Perimeter



https://cloudsecurityalliance.org/group/software-defined-perimeter/#_overview

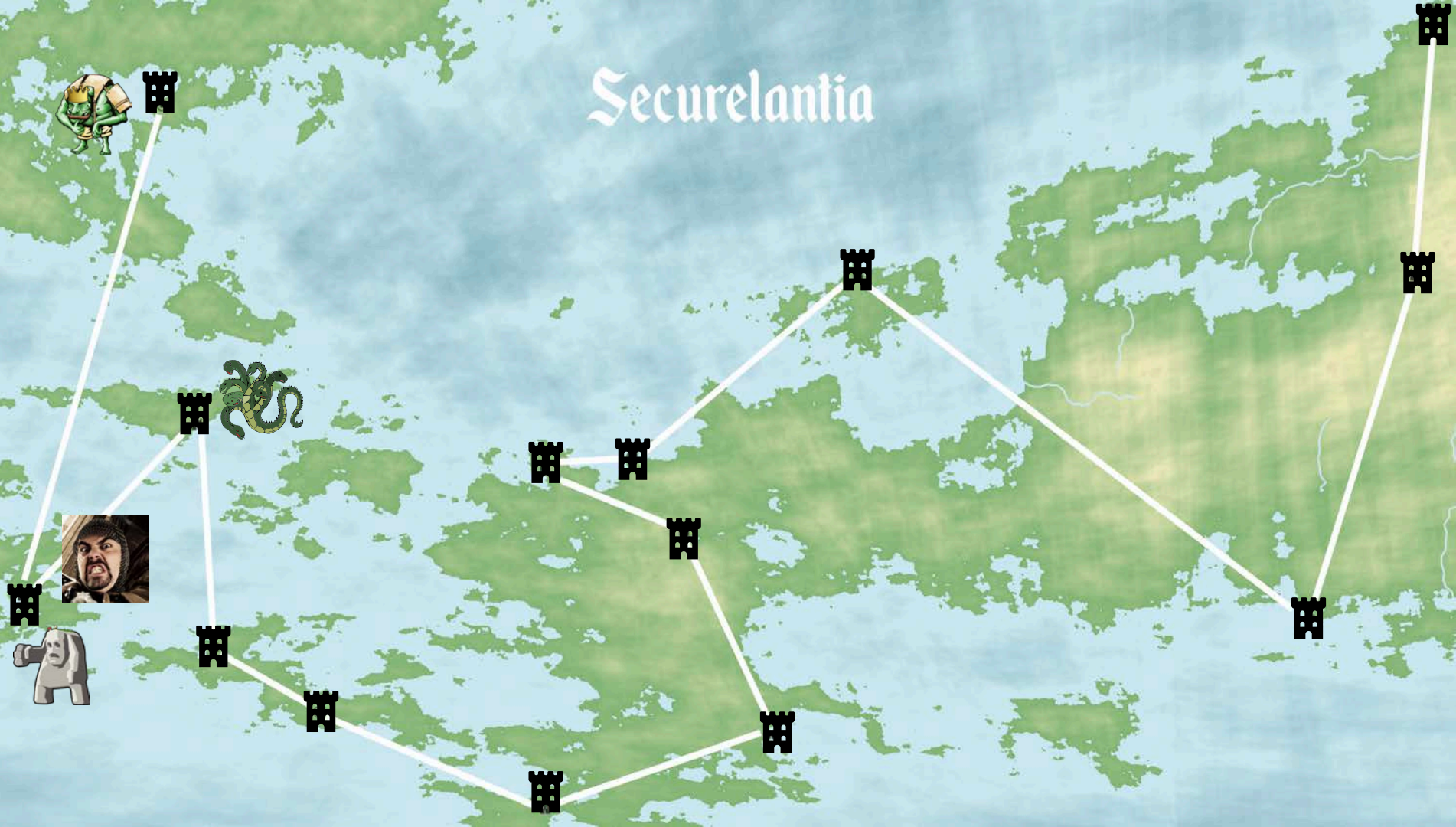
How I Killed the Earth Elemental



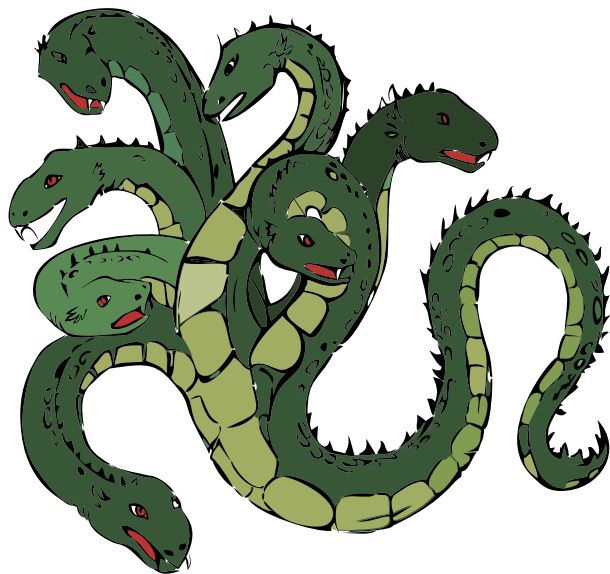
- Reviewed how I had previously defined perimeter
- Studied up on software-defined perimeter
- Looked at vendors that specialize here
 - Zscaler
 - Palo Alto (Global Protect)



Securelantia



Hydra of Confusion (CR = 9)



- Figuring out provider services
 - IaaS
 - SaaS
 - PaaS
 - WTFaaS
- High number of services and speed of innovation of providers
- **BILLING, BILLING, BILLING**

What Kind of “aaS” Do I need?



- IaaS – Infrastructure as a Service
 - AWS, Azure, GCP
 - Provides you the computing infrastructure, physical or virtual machines and other resources
- SaaS – Software as a Service
 - Salesforce, Office 365, GoToMeeting, Netflix
 - Provides access to application software, with no need to install, setup, and run the application
- PaaS – Platform as a Service
 - AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com
 - Provides computing platforms which typically include operating system, programming language execution environment, database, web server, etc.

Amazon Web Services

Compute topics continue on next slide



#RSAC



Amazon EC2



Amazon ECR



Amazon ECS



Amazon Lightsail



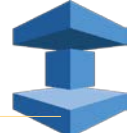
Amazon
RDS



Amazon
DynamoDB



Amazon DynamoDB
Accelerator



Amazon
ElastiCache



Amazon
VPC*



AWS Batch



AWS Elastic
Beanstalk



AWS
Lambda



Elastic Load
Balancing*



AWS DMS



Amazon
Redshift



AWS Direct
Connect



Amazon
S3



Amazon
EFS



Amazon
Glacier



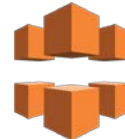
AWS Storage
Gateway



AWS Snowball*



Elastic Load
Balancing*



Amazon
CloudFront



Amazon
VPC

Microsoft Azure

Compute topics continue on next slide



#RSAC



Google Cloud Platform



#RSAC



Compute Engine



App Engine



Container Engine



Container Registry



Cloud Functions



Cloud IAM



Cloud Resource Manager



Cloud Security Scanner



Cloud Platform Security



Cloud Virtual Network



Cloud Load Balancing



Cloud CDN



Cloud Interconnect



Cloud DNS



BigQuery



Cloud Dataflow



Cloud Dataproc



Cloud Datalab



Cloud Pub/Sub



Genomics



Cloud Storage



Cloud Bigtable



Cloud Datastore



Cloud SQL



Persistent Disk



Cloud Machine Learning



Vision API



Speech API



Natural Language API



Translation API



Jobs API

AWS billing is like getting attacked by birds



Crazy Billing Example



- S3 Glacier
 - “...extremely low-cost cloud storage service for data archiving and long-term backup.”
- Example of restoring from Glacier
 - Restore pricing “starts at \$.01 / GB”
 - So, $\$0.01 / \text{GB} * 1\text{TB} = \10
 - Currently, you can retrieve 10 GB of your Amazon Glacier data per month for free
 - In the past, on any given day, you were allowed to restore a maximum of 1/30th of 5% of your total Glacier storage (ie: 5% per month but prorated daily)*

* <http://davidsimic.com/2016/07/18/amazon-s3-pitfalls-how-to-innocuously-rackup-a-1797-bill-restoring-1tb-of-data-in-amazon-s3/>

AWS Billing Nightmare



- Ryan Hellyer* – Wordpress developer
 - AWS access keys got compromised (on GitHub)
 - Found hundreds of EC2 instances running in multiple regions
 - AWS billing is **not updated in real time**
 - ~\$6000 bill (likely got a concession)

* <https://wptavern.com/ryan-hellyers-aws-nightmare-leaked-access-keys-result-in-a-6000-bill-overnight>

How I Killed the Hydra



- Stopped trying to understand everything or keep up with it all
- Started with what I knew best
- Surrounded myself with all things Cloud
 - Podcasts
 - Articles
 - Videos
- Billing
 - Created alerts



Securelantia



Shadow Dragon of Data Protection (CR=13)



- Who secures what?
- S3 buckets
- Increase from one or two ingress/egress points to virtual ∞
- Securing the deployment
 - Existing security vs New security
- Shadow IT

Who Secures What?



- SaaS
 - Provider is primarily responsible for the security of the platform (physical security, infrastructure, and application security)
 - You are responsible for how you use the application
- PaaS
 - Similar security model to SaaS, except in some network and application controls
- IaaS
 - Essentially, they secure the cloud, you secure what's in the cloud
 - **Shared Responsibility Model**

S3 buckets (Magic File Canisters in the Sky)



- File/object storage
- Good for static websites
- Can be encrypted
- Can be setup to track changes and recover lost files
- **Not publicly accessible by default...**

Create bucket



1

Name and region

2

Set properties


3

Set permissions

4

Review

Name and region

Bucket name 



M

Bucket name must not contain uppercase characters

Bucket name must start with a lowercase letter or number


Bucket name must be between 3 and 63 characters long

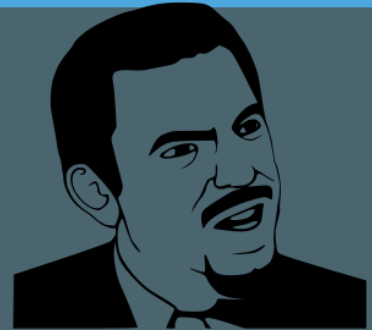
Create bucket



- 1 Name and region
- 2 Set properties
- 3 Set permissions
- 4 Review

Name and region

Bucket name 



mytestbucket

Bucket name already exists

Create bucket



- 1 Name and region
- 2 Set properties
- 3 Set permissions
- 4 Review

Name and region

Bucket name 

my_

invalid characters



Bucket name contains invalid characters '_'

Create bucket



- 1 Name and region
- 2 Set properties
- 3 Set permissions
- 4 Review

Name and region

Bucket name 

my-test-rsa-bucket



Region

US East (N. Virginia)



Create bucket



Name and region



Set properties



Set permissions



Review

Versioning

Keep multiple versions of an object in the same bucket.

[Learn more](#)



Disabled

Server access logging

Set up access log records that provide details about access requests.

[Learn more](#)



Disabled

Tags

Object-level logging

Manage users

User ID ⓘ

Objects ⓘ

Object permissions ⓘ

m1a1vet(Owner)

☒ Read

☒ Write

☒ Read ☒ Write



Access for other AWS account

+ Add account

Account ⓘ

Objects ⓘ

Object permissions ⓘ

Manage public permissions

Do not grant public read access to this bucket (Recommended)



m1a1vet(Owner)

☒ Read

☒ Write

☒ Read ☒ Write



Access for other AWS account

+ Add account

Account ⓘ

Objects ⓘ

Object permissions ⓘ

Manage public permissions

Grant public read access to this bucket



This bucket will have public read access.

Everyone in the world will have read access to this bucket.

and yet...

S3 Misconfigurations



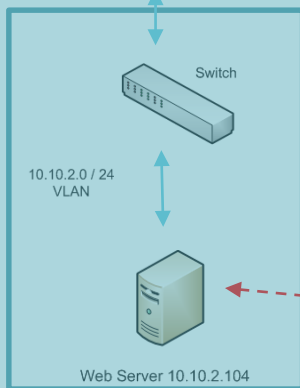
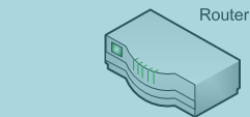
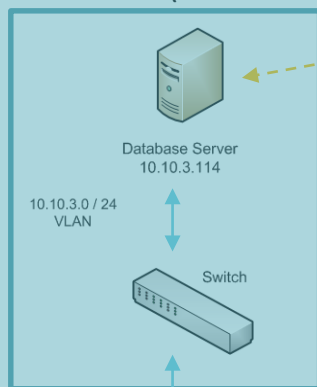
- 25+ major S3 misconfigurations since December 2016 (maybe more) that caused public exposure of very sensitive data
- UpGuard starting finding S3 bucket misconfigs around mid-2017
- BTW, I started really digging into cloud about that same time...
 - **CORRELATION DOES NOT EQUAL CAUSATION**(just wanted to clear that up)
- Verizon, Accenture, Time Warner, Viacom, WWE, US voter data

How to Deploy the Workload



- Can be similar to traditional networking (VPC)
 - Files, database, applications, etc.
 - Deployment can be very similar
 - Essentially, treat cloud like an off-premise DC
- But deployment can also be radically different...
 - Server-less architecture
 - Decoupling of services
 - Fast deployment (DevOps)
 - Autoscaling
 - Latency and geolocation planning

Traditional Data Center (10.10.0.0 / 16)

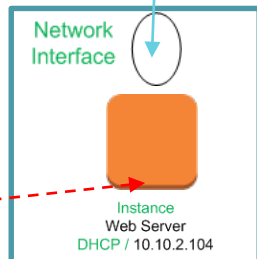
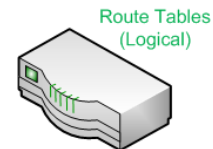
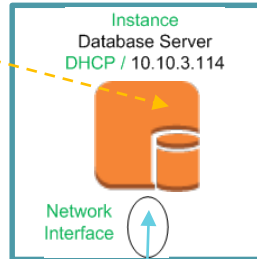


Database Server

- Low number of ingress/egress points
- Less room for config error

Web Server

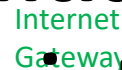
VPC (10.10.0.0 / 16)



10.10.2.0 / 24 Subnet

Increase in Potential Ingress/Egress Points

- High number of ingress/egress points
- A lot of room for config error



Elastic IP
52.43.39.122



Security Group
Database Servers)



Security Group
(Web Servers)



Same as billing...
but with friggin' wasps



Securing the Deployment – Then vs Now?



- Old Security – Does it still work in the Cloud?
 - Firewalls (Next gen FWs = visibility, but can create chokepoints)
 - WAF (visibility)
 - Network penetration testing (make sure permissions are in place)
 - Dynamic application security testing (make sure permissions are in place)
 - Patch Management (major differences– use AMIs/VMs)
 - Vulnerability Assessments (make sure permissions are in place)
- New Security – Is it really new?
 - CASB (cloud access security broker)
 - Different vendors with different foci
 - Cloud Workload Protection Platforms
 - UEBA and SIEM
 - Traditional security vendors moving to the cloud



- Cloud makes deployments easier for you... and for your users
- Marketing departments are VERY good at deploying apps in the cloud (well... their provider is good at it)
- They are tasked with keeping the pipeline full
- Often collect data that is potentially sensitive in nature
- How do you know where it is?

How I Killed the Shadow Dragon



- **Learned Shared Responsibility Model**
- S3
 - Studied granular permissions
 - Tested permissions
 - Developed strong IAM principles and practices
- Align with business requirements
 - Don't want to hamstring the flexibility of cloud
 - Can't ignore real data security requirements
 - Had to compromise
 - Look at newer vendors



How I Killed the Shadow Dragon



- Testing
 - Used pre-authorized testing vendors when possible
 - Used provider services if available **and** adequate
- Shadow IT
 - Worked on how to partner with the business owners
 - How can I become their preferred method of delivery?
 - Used automation and orchestration to build in flexible AND secure delivery (Formation templates, Terraform, etc.)



Securelantia



Securelantia



Summary of The Quest



- The Quest ain't over... not by a long shot
- Constant learning... more than ever (new monsters keep popping up)
- The biggest monster is stubbornness
- Call BS when needed (on vendors AND yourself)
- Have courage and have fun
- Keep your sword sharp and your armor polished

Future Beasts to Slay



- Logging
- Compliance
 - Regulations
 - Current policy
- Keeping track of assets
- **And others**



Using My Quest to Slay Your Monsters



- Remember lessons from security past to security now
 - Be part of the solution... don't be the Monster of No
- Start thinking about the perimeter differently
 - Inside-out or Upside-down (yes, that is a ***Stranger Things*** reference)
- Surround yourself with cloudiness
 - Podcasts, webcasts, newsletters, Twitch (yes, Twitch)
 - Go get certified (A Cloud Guru is awesome)
- Use the tools the IaaS provider gives you
 - Billing alerts are a job-saver

Using My Quest to Slay Your Monsters (cont.)



- Read the FAQs (<https://aws.amazon.com/faqs/> and others)
- Don't forget the prime benefit of the Cloud: Flexibility
 - Rebuilding your on-premise DC in someone else's DC is NOT the point
 - Security can hamstring as much as help... don't try to do security the same way in the Cloud as in your DC
 - Learn the Shared Responsibility Model
 - Look at new and old vendors
- Be determined to be your company's main provider



Q&A

Or you can just shake your head, laugh at me, and slowly walk out of the room... either way... it's cool...