

Managing Thunderstorms

How I Learned to Stop Worrying and Love the Cloud

Alex Dow

GCIH|SCF|CISSP|OPST



MIRAI

Talk Parameters

What I am Going to Talk About

- What is Cloud?
- My Cloud Objections
- A Shift in Paradigm
- Cloud = Better Sec?
- The Future

What I am Not Going To Talk About

- Azure, GCP
- Private Cloud
- All the AWS Things
- Cloud Optimization and Saving Money

\$ cat ~/.life_history

- 90's – Computers & The Internet!
- 2004 – Bell Canada GSOC in Ottawa
- 2008 – Olympic SOC & HoneyNet
- 2010 – Consulting (SecOps Architecture, SOC's, IR)
- 2013 – The Mainland Advanced Research Society (BSides)
- 2015 – Cloud Curious
- 2017 – Mirai Security, SANS Instructor



What is Cloud?

Old Definitions

- Someone else's computer
- Shared hosting (single host)
- Virtual private servers
- Shared DC (Dedicated or CoLo)
- Managed Applications

New Definitions

- Pay as you go compute, storage and applications
- Highly available, accessible and pooled resources
- On-demand, scalable, elastic
- Provisioning velocity
- Self Service and powerful APIs
- Decoupling us from layers of IT

Cloud 101: SaaS, IaaS and PaaS; Oh My!

- Software as a Service (SaaS)
 - Subscription based software
 - Ex: Dropbox, Quickbooks Online, Salesforce, Office 365, GSuite, ServiceNow
- Infrastructure as a Service (IaaS)
 - Virtualized hardware
 - Ex: EC2, LightSail and Storage services (S3, EBS, EFS)
- Platform as a Service (PaaS)
 - *All the juice and half the squeeze*
 - Preconfigured platforms, sometimes with no OS/Networks
 - Ex: Database as a Service, Lambda, force.com, Beanstalk, ServiceNow



Cloud 101: The Players

- **Amazon Web Services (AWS)**
 - Trailblazer
 - Developer driven, incredible list of offerings
- **Microsoft Azure**
 - The warm blanket for traditional IT
 - IT driven, underdog with lots of money, catching up quick, all the joys of Microsoft idiosyncrasies
- **Google Cloud Platform**
 - Lower costs, container focused, anarchist to regulators, niche
- **Alibaba/Tencent/Baidu**
 - Sleeping dragon
 - “Borrowers” of intellectual property?

Figure 1 Magic Quadrant for Cloud Infrastructure as a Service, Worldwide



Source: Gartner (May 2018)

A wide-angle photograph of a beach under a massive, dark, and turbulent storm cloud system. The sky is filled with heavy, layered clouds in shades of grey and blue. The beach is sandy and stretches from the foreground into the distance. A few people are visible on the beach, including one person lying down in the foreground. The ocean is dark and calm, meeting the shore with gentle waves. The overall mood is dramatic and atmospheric.

There's a Storm Comin'

My Journey of Enlightenment

There's a Storm Coming

- 2000's
 - Protected "B", Banks, ITSG, ISO, NIST
- 2009
 - I first saw Cloud, niche
 - I can haz American Netflix?
 - Sensitive sectors were still not interested
- 2011 - AWS US GovCloud
- 2014 – Chance of Precipitation (VanCity!)
- 2017 – SSC/TBS are "Cloud Curious"

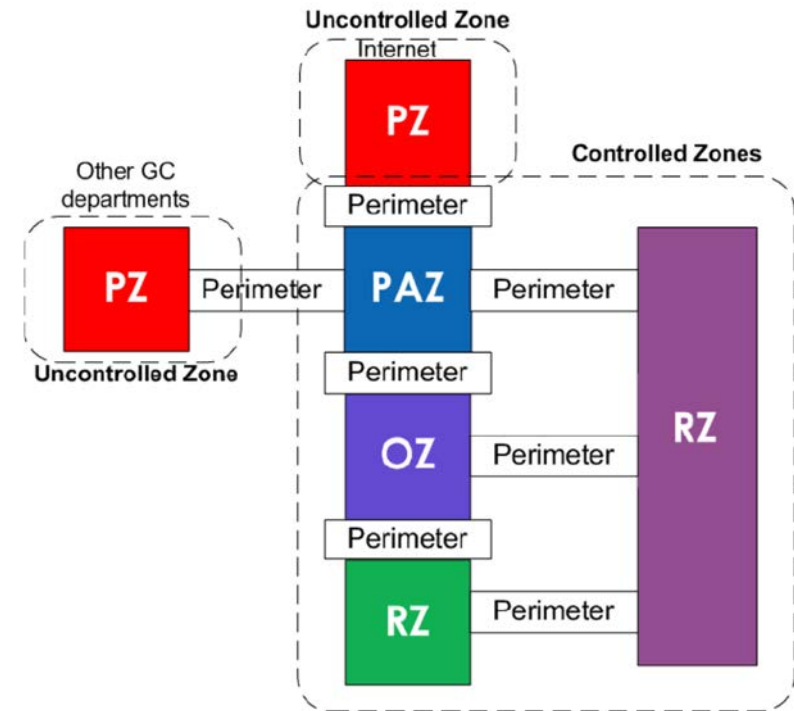


Figure 1: Sample Architecture using ITSG-22 Zones

Cloud Objections: Privacy and Compliance

- Privacy
 - Data sovereignty
 - Storing data on someone else's (shared) infrastructure
 - Loss of control (No throat to choke)
 - Privacy laws
- Compliance
 - Cloud initially didn't offer the security features we needed
 - 1:1 control mapping was futile
- The Concept of Shared Responsibility
 - Hurts our brains especially in the SaaS and PaaS world





Cloud Objections: Blue Team

- Things are Weird
 - No physical access, everything is software defined/manifestations of old technology like networks
- Threat Prevention and Detection
 - Traditional FW are not native
 - No native SPAN/TAP ports
 - Limited cloud specific threat prevention/detection solutions
- Different “Visibility”
 - Collecting/monitoring logs/telemetry has changed
 - Not all things are “hosts” like we know them
 - IP and hostnames are ephemeral
- Dangers of Shared Resources
 - Who watches the watchers?
 - When sharing memory/CPU goes wrong: “Hello from the other side” + Spector/Meltdown

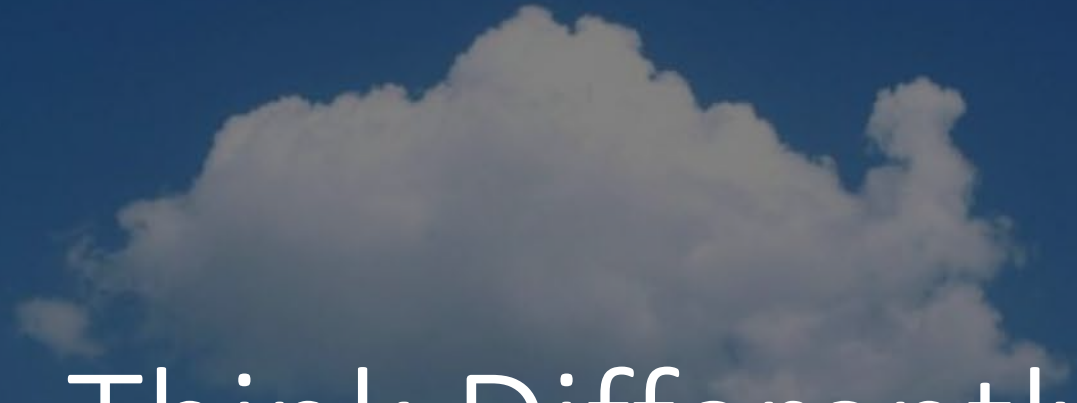


Thunderstorms

	A "Big 4" Consultancy		Code Spaces + VFEmail
<p>Date Late 2016-Nov 2017</p> <p>Dev was using publicly accessible Git repo API Key was hard coded API key was found by attackers AWS account accessed and Data exfiltrated</p> <p>Affected 57 Million PII Records Paid \$100k Hush Money \$148M Fine + 20 years of privacy audits</p> <p>WHY? Poor SDLC/No MFA/No Least Privileged</p>	<p>Date Oct 2016-March 2017</p> <p>Hackers gained access to target's O365 cloud infrastructure via poorly configured O365 administrator account Attacker had ~6 months of unfettered administrative access</p> <p>Affected Email and Customer Data</p> <p>WHY? No MFA/No Monitoring</p>	<p>Date Feb 2019</p> <p>Unprotected MongoDB exposed to Internet Found by researchers, suspected by others</p> <p>Affected 763 Million PII Business ceased to exist Breach Inheritance?</p> <p>WHY? Bad Architecture/Bad Practices/No Monitoring</p>	<p>Date 2014 & 2019</p> <p>Hackers get into infrastructure Encrypt all data, delete backup, lock admins out Demand ransom</p> <p>Affected All data destroyed Both companies ceased to exist</p> <p>WHY? Bad IAM/No segregation of duties/No or bad backups strategies</p>

We've Got 99 Problems, But Cloud Ain't One

- Cultural
 - Cloud works harmoniously, we don't (DevOps vs IT vs IS)
 - Laissez-faire security, but we have a \$securityBox!
 - Security is challenging to enforce and measure
- Technology
 - Complex IT, weak IAM, network segmentation and data classification
 - Tech debt: snowflake IT and tech drift
- Cloud Adoption
 - Risk management traditionally has been left out of the conversation
 - Forklifting bad architectures, host to host comms, owning the stack

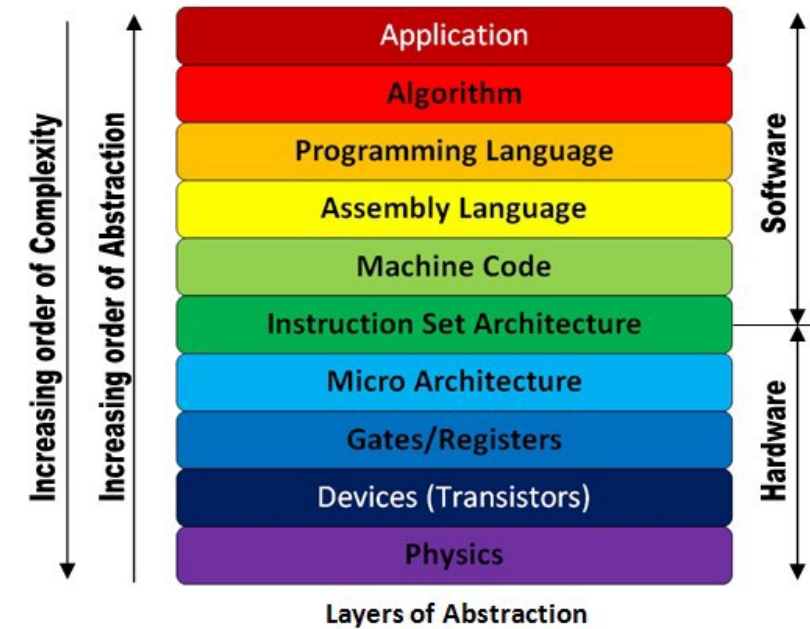


Think Differently

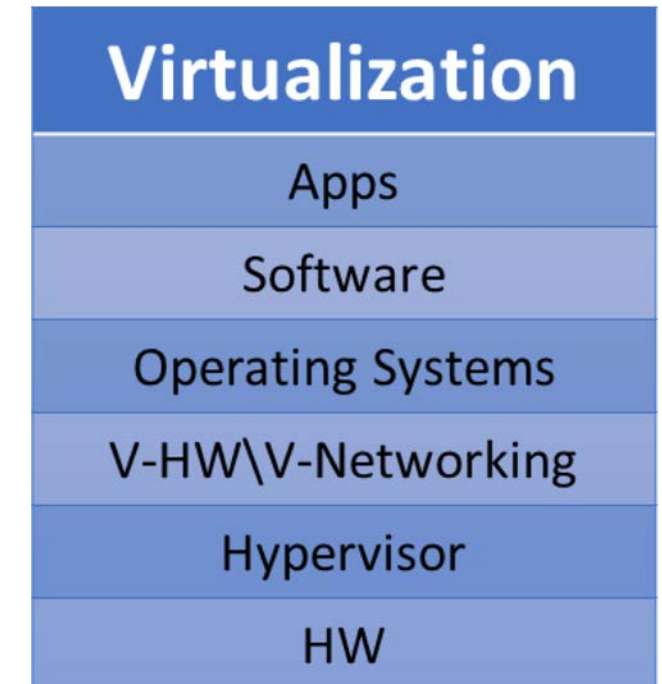
Can Cloud Enable Better Risk Management?

Layers of Abstraction

*“In computing, an abstraction layer or abstraction level is a way of **hiding the working details of a subsystem**, allowing the separation of concerns to facilitate interoperability and platform independence.” -Wikipedia*



- But What Does That Mean For Computing?
 - As we have advanced IT we no longer need to know how upper/lower layers works, just how to interact with it
- Cloud takes this layers of abstraction concept and decouples us from various layers of IT



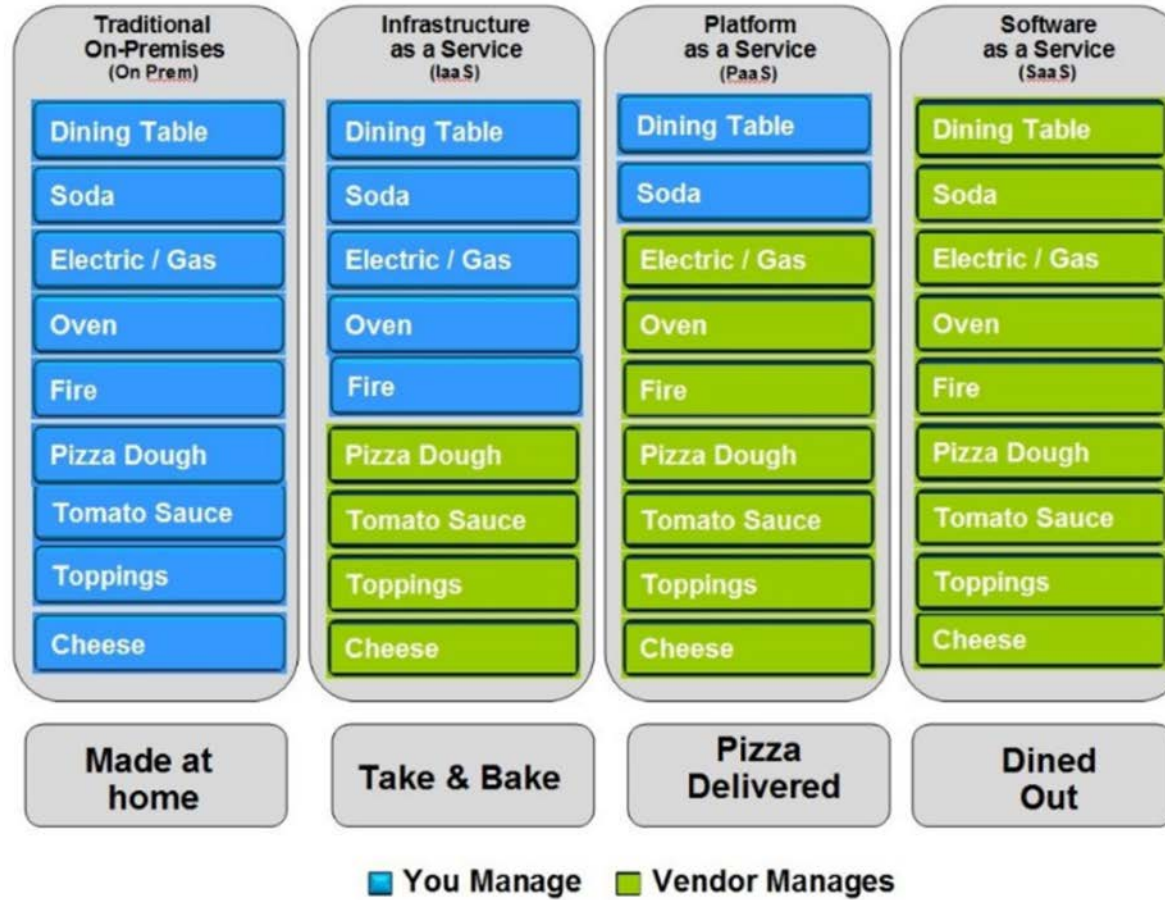
Ascending The Layers of Abstraction

- Imagine the possibilities if you didn't have to be worry about the risk of...
 - Hardware
 - Networking
 - Operating Systems
 - Services
 - Applications
- Risk Treatments
 - Avoid, Reduce, **Transfer**, Accept, Share
- Introducing: The Shared Responsibility Model

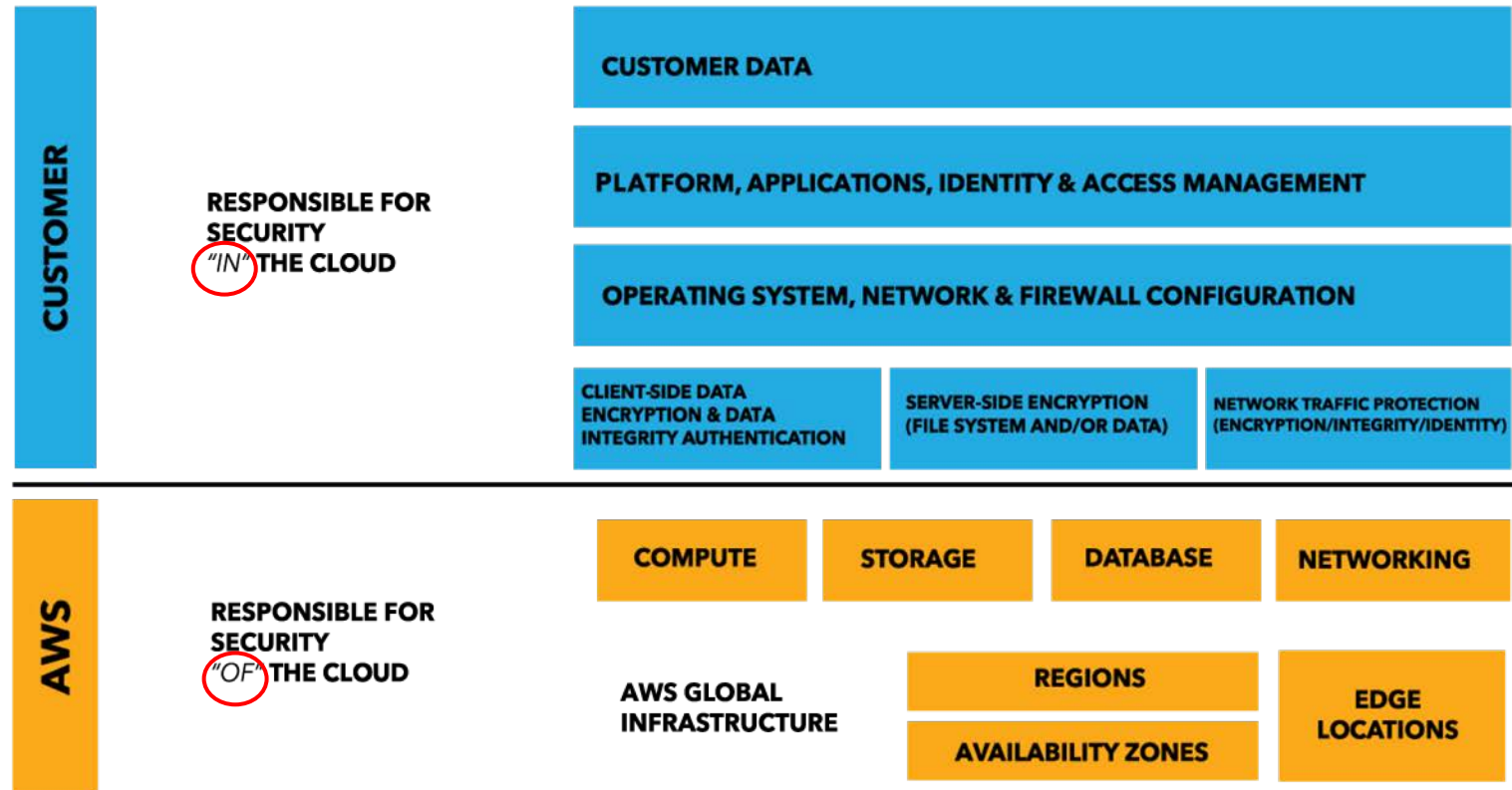


The First Shared Responsibility Model

Pizza as a Service



Shared Responsibility Model



Shared Responsibility Model

Responsibility	SaaS	PaaS	IaaS	On-prem
Data governance & rights management	Customer	Customer	Customer	Customer
Client endpoints	Customer	Customer	Customer	Customer
Account & access management	Customer	Customer	Customer	Customer
Identity & directory infrastructure	Shared	Shared	Customer	Customer
Application	Microsoft	Shared	Customer	Customer
Network controls	Microsoft	Shared	Customer	Customer
Operating system	Microsoft	Microsoft	Customer	Customer
Physical hosts	Microsoft	Microsoft	Microsoft	Customer
Physical network	Microsoft	Microsoft	Microsoft	Customer
Physical datacenter	Microsoft	Microsoft	Microsoft	Customer

■ Microsoft ■ Customer

So Are CSPs Any Good at Security?

- The big ones have a major incentive to do security better than us
- Perpetually Audited
 - GDPR, NIST, HIPAA, FIPS 140-2, PCI-DSS, ISO 27000, SOC plus 26 more!
- But... CSPs will never own ALL the risk
 - Their T & C explicitly say they do not, even for SaaS!
 - Understand the shared responsibility model
- Trust, But Verify
 - Don't assume they are doing the right thing (SaaS!)
 - Read through their reports on compliance
 - Read through their white papers
 - Make informed decisions on adopting and leveraging cloud



You REALLY think you can do security better?


Them: "I'd never put my data in the cloud"

Me: "Do you even threat model, bro?"

State sponsored? – MAYBE go to cloud...

Cyber criminals, Joe from IT and DevOps? – GO TO CLOUD NOW!

Law enforcement? – DO NOT GO TO CLOUD!

A hand is shown squeezing a slice of orange over a tall glass filled with orange juice. The juice is a vibrant yellow-orange color. In the foreground, on a white surface, sits a wedge of an orange. The background is a solid, light blue-grey color. The text is overlaid on the center of the image.

All The Juice, Half the Squeeze?

How Cloud Can Make Security Easier

Cloudification of IT

- AWS has Appified IT
 - Things we weren't great at are now an **app**
 - They are heavily integrated, turn key and work seamless together
- **Some** as a Service
 - Network Segmentation: VPC and Security Groups
 - Keys & Secrets: KMS, parameter store and CloudHSM
 - Compute: EC2, Lightsail, Lambda and Elastic Beanstalk
 - Security: IAM, Guard Duty, Security Hub, CloudTrail and CloudWatch
 - Storage: S3, EBS, EFS and Glacier
 - Databases: RDS, DynamoDB, Aurora and many more options for database!
 - Message Buses: SMS, SQS, Kinesis

Welcome to the Matrix

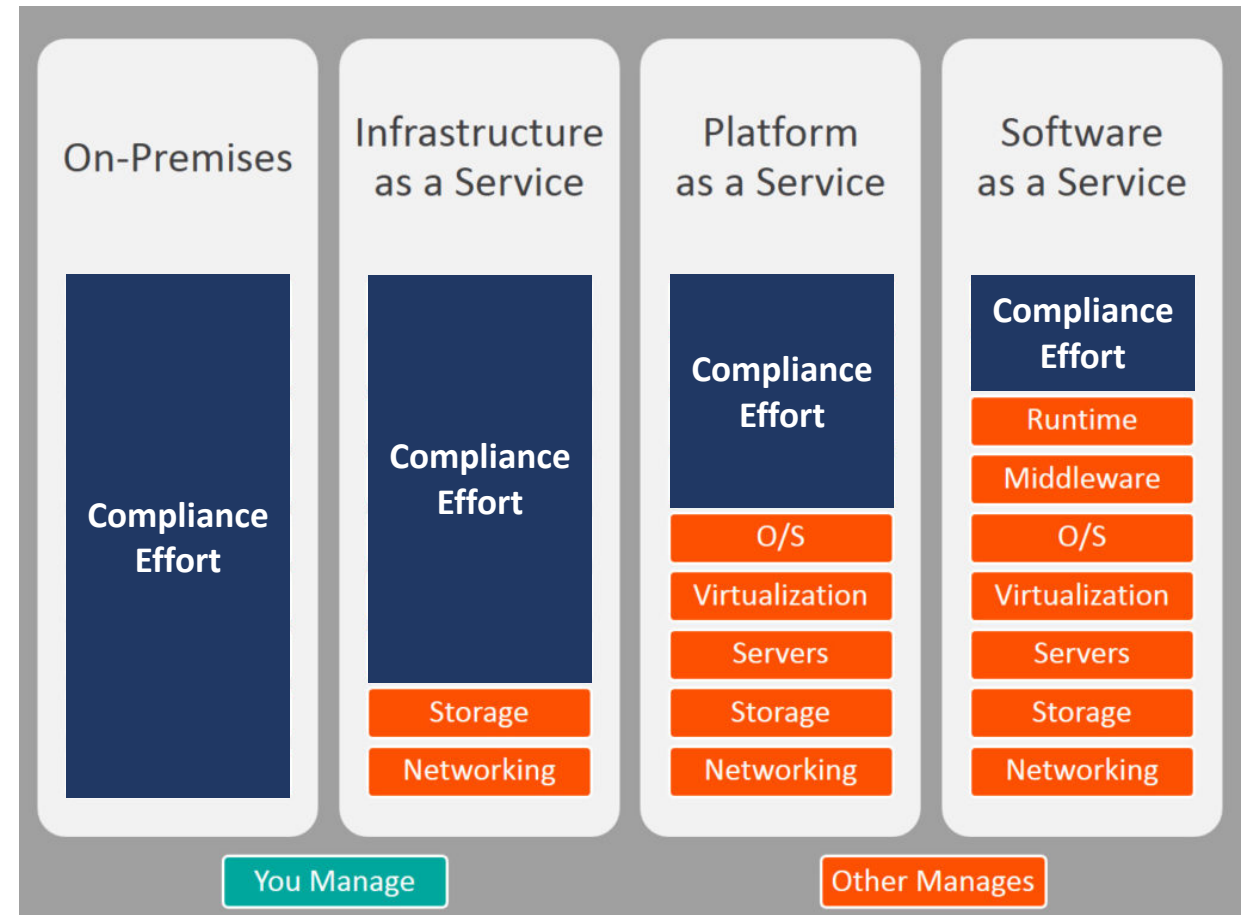
- Software Defined World
 - Manifestation of IT, everything is an object
 - Infrastructure as Code, Security as Code = templates
 - Burstable infrastructure
 - Automation and orchestration without another box
- Management Control Plane
 - Common interconnectivity between cloud resources
 - No direct access to infrastructure, only through the API (AWS CLI or Console)
 - All activities are authenticated, granularly authorized and logged
- Queryable Infrastructure
 - AWS CLI allows total awareness with a couple keystrokes

Blue Team

- Prevention
 - Better architectures and leveraging PaaS = reduced attack surface
 - Microsegmentation (virtual at no extra cost)
 - Implement guardrails through strong Identity and Access Management
 - Baked-in standardized/consistent security for easy/continuous auditing
- Detection
 - Native logging, good tooling such as CloudTrail, CloudWatch, GuardDuty
 - Detect policy violations and threats in real-time
- Response and Recovery
 - Automated response (FaaS) and containment
 - Redeployment orchestration in seconds

Audit and Compliance

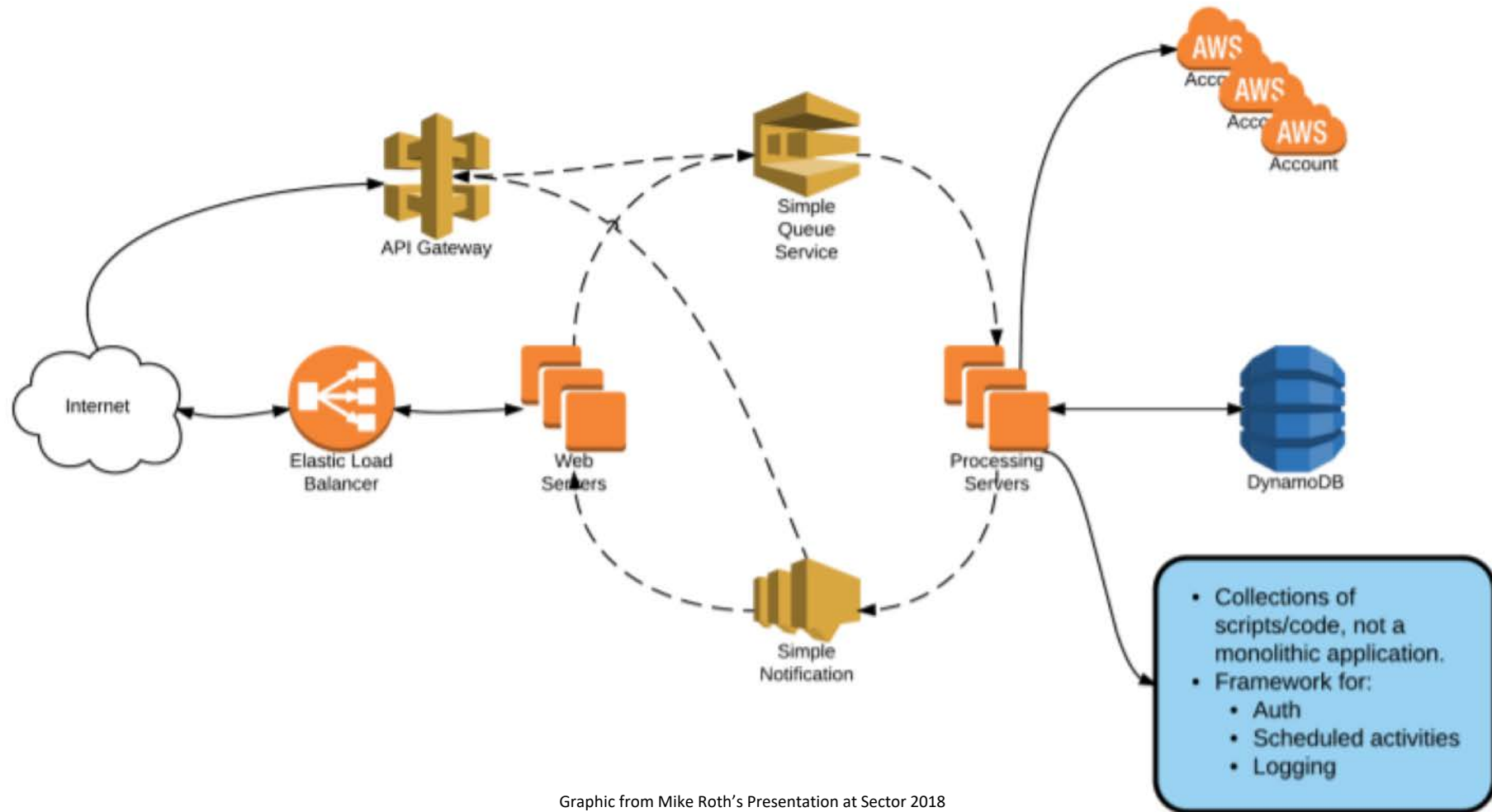
- The Fun Part!
- Leverage your CSP
- Audit as Code = Standards
- Achievable Accuracy
- Continuous Compliance



A misty landscape with a winding road and trees at sunrise or sunset. The scene is bathed in a warm, golden light, with a large tree on the right and a smaller one on the left. The road curves through the mist, and a fence is visible in the background.

Cool Concepts

Reducing the Attack Surface



Graphic from Mike Roth's Presentation at Sector 2018



A New Way of Thinking: Immutable Systems

Pets

- We name them
- Several different kinds
- They get sick, we pay
- Lasts for several years
- You love them
- They die, you are sad

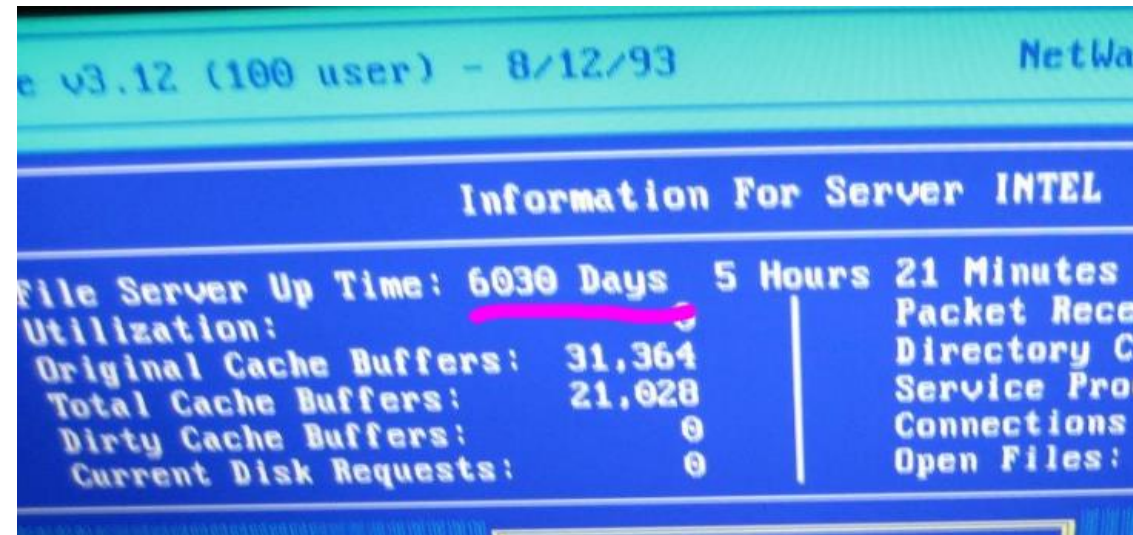
VS

Cattle

- We don't name them
- All the same
- They get sick... they die
- Short life expectancy
- You do not love them
- Steak!

Immutable Systems: Uptime is For Losers!

- Operational Security
 - No more snowflake IT, no golden image drift
 - No troubleshooting in prod
 - Patch in staging, cutover to prod
 - Rapid development
- Increase Costs to the Attacker
 - No SSH, no shells?
 - Constantly having to re-compromise
- Use Case
 - Login/strange activity -> KILL IT



Homogenous IT?

- “Cloud in a Box”
 - Azure Stack & AWS Outpost
 - Addresses latency/connectivity
- Why? We have ESXi!
 - Elasticity + NG Tech + Methods
 - **Common management backplane for all of IT**
- Vendor Lock-in? ☹️





Future Predictions

The Future of Compute

- NOW: IaaS Exists to Help us Luddites “Get” the Cloud
 - IaaS is the most risky cloud service
 - It’s the means that justifies the end
 - OS will be for legacy systems and hobbyists
- SOON: PaaS, CaaS and FaaS are the Future
 - All the juice, half the squeeze
 - Heavy move to “owning less”
 - Serverless examples: Aurora, Lambda
- FUTURE: Compute as a Utility
 - Compute services will be ubiquitous like electricity and water
 - Throw it some code and it will provide results
 - There will be compute brokers



The Future Attack Surface

- If we continue to transcend layers of abstraction, where is the final frontier of information security?
 - ~~Network? OS? Servers?~~
 - The application layer
- DevOps Will Need to Mature
 - Secure SDLC
 - Proper training
 - Continuous Integration/Continuous Deployment Pipelines

Wrap Up

- Cloud is Awesome.
 - Opportunity of a lifetime, greenfield + next gen services
- But...
 - It is only as secure as it is designed and operated
 - We have seen the wrong team driving cloud adoption... In the news
 - **Lift and Shift** = higher interest rates on your tech debt
- So...
 - Data classification is crucial
 - Threat model and design to minimize the attack surface
 - Embrace the new paradigms and avoid Pet laaS
 - Standardization allows for easy and continuous compliance/auditing
 - Cloud native, automation and playbooks

A dramatic landscape featuring rolling hills and mountains under a heavy, cloudy sky. Sunbeams (crepuscular rays) are visible, breaking through the clouds and illuminating the scene. The overall tone is moody and atmospheric.

Thank You!

Q & A

Alex.Dow@MiraiSecurity.com
<https://www.miraisecurity.com>

CSA's Top 12 Cloud Threats

- Data Breaches
 - S3, MongoDBs, poor IAM
- Insufficient Identity, Credentials and Access Management
 - Finding creds->no MFA->IAM pivots
- Insecure Interfaces and APIs
- System Vulnerabilities
- Account Hijacking
 - Ransom, cryptomining
- Malicious Insiders

CSA's Top 12 Cloud Threats

- Advanced Persistent Threats
- Data Loss
 - Poor understanding of encryption, DRP, SLAs
- Insufficient Due Diligence
 - 80% of cloud is not AWS and Azure
- Abuse and Nefarious Use of Cloud Services
 - Distributed computing for fun and profit
- Denial of Service
- Shared Technology Issues
 - VM escapes, Spectre/Meltdown