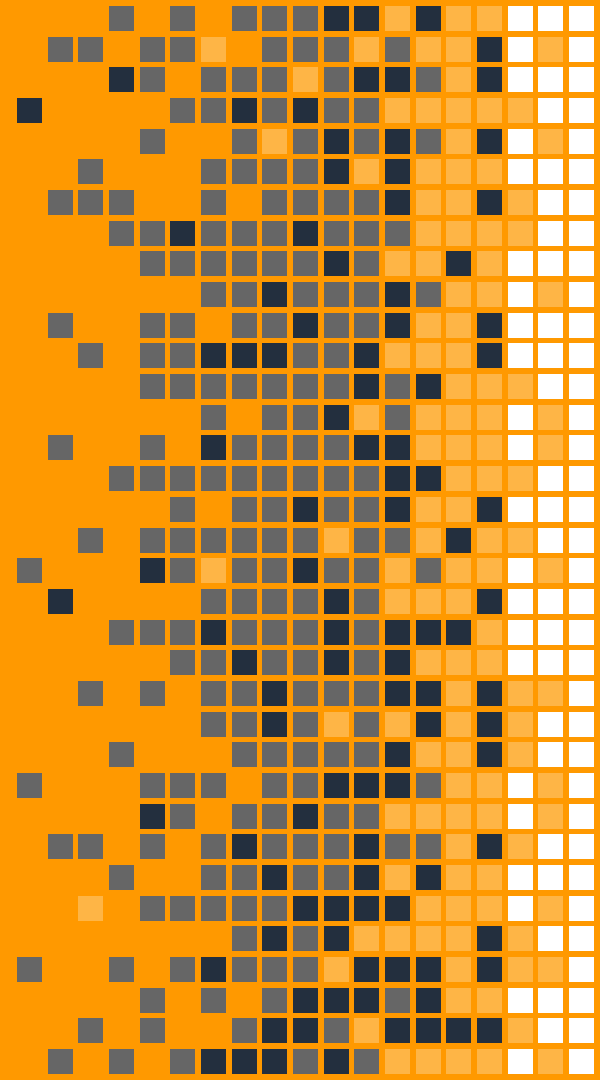


# Cloud Security

## An IAM GAME

Nathaniel Beckstead





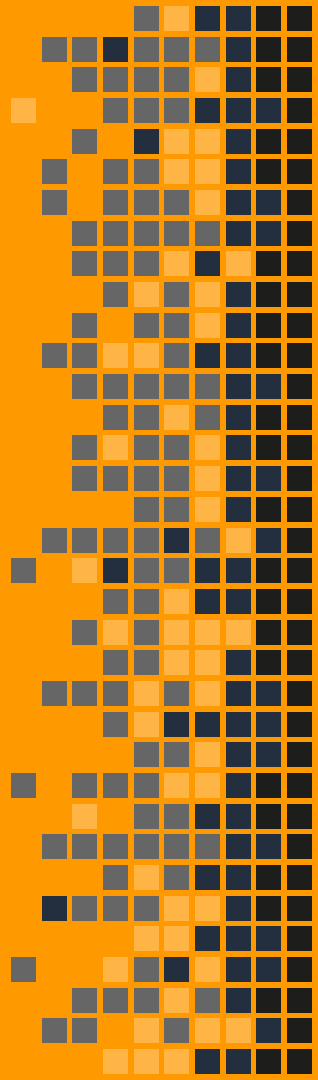
# whoami

I am here because I love to  
give presentations.

@scriptingislife

<https://scriptingis.life>

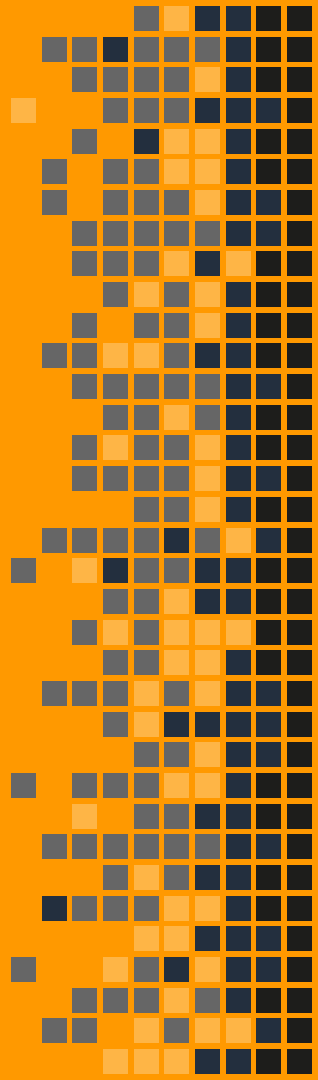
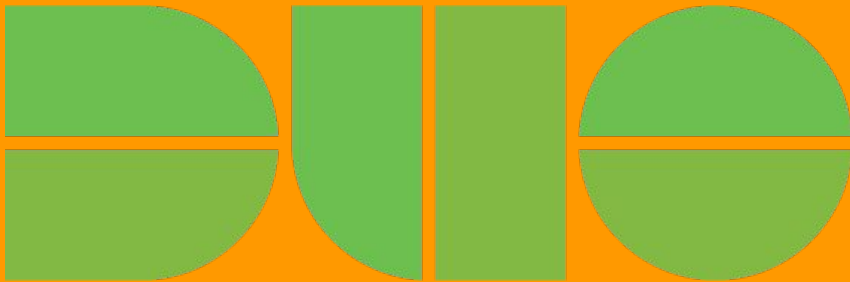
<https://glimpseid.com>



# What is the cloud?



# What is the cloud?



# What is the cloud?

## Bessemer Venture Partners Cloudscape

### END USER APPLICATIONS

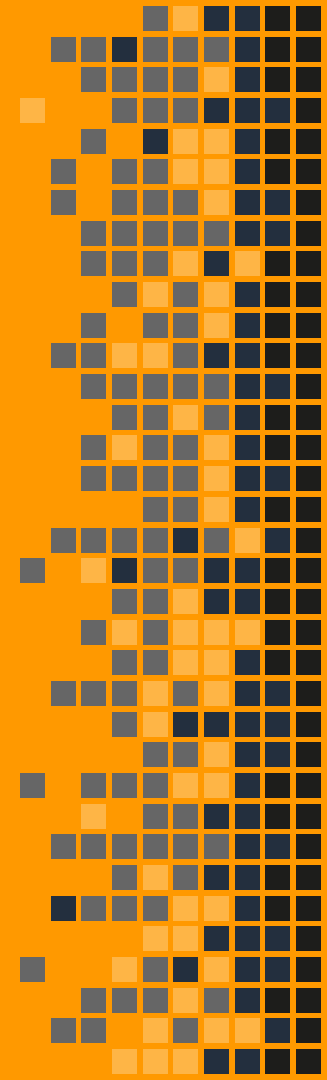
Software-as-a-Service					
CRM	Marketing Demand Generation	Human Resources	Finance & Accounting	Content Management	Vertical
RightNow salesforce.com NETSUITE Assistify satisfaction ORACLE InsideView zendesk MarketTools xactly PARALLEL LIVEPERSON Microsoft	ELOQUA KINSHOOL Avin unbounce iContact CampaignMonitor Bronlo Silverpop WaldLoop VerticalResponse SurveyMonkey Marketo Influencer responsys	Cornerstone LinkedIn workday SuccessFactors HALOGEN saba echosop SAP Taleo vubox tribehr BULLHORN EPICOR	Cincur NETSUITE Intacct workday intuit Expensify RECURLY expensecloud Chargify Freemove Bill.com ZOSOOS Coupa uora Adaptive Planning	box SharePoint Dropbox Watchbox youenoit Drupal Alfresco DocuSign backupify senothisfile ShareFile Scribd bitcasa VIX CloudApp CARBONITE mozy SugarSync Echsign	MINDBODY MEDIANETICS DealerTrack Medifinance REALPAGE navicare VEEVA PointClickCare clo OPPOWER SERVICEMAX superderivatives appolo KINNSER WebPT activeNETWORK
Enterprise Social Media	Marketing Analytics	Retail & E-Commerce	Collaboration	Business Intelligence	Ad Tech
Yammer hootsuite gigya radion jive Zuberance janrain Lithium facebook ELOQUA involver YouTube social BUDYMEDIA twitter vitruve WILDFIRE EVERNOTE	convertro COVARIQ Google Analytics VOCUS GinzaMetrics Keybroker HubSpot BRIGHT EDGE SEOMOZ CLICOTALE WordStream	ERPLY shopify ONESTOP DELIVERYAGENT RSI PowerReviews Magento Bazaarvoice VeriSign WIX BIG Commerce volusion yodle	Altastan skype Google Apps twilio LogMeIn 37signals TeamViewer box clarizen PODIO Teambox RingCentral GFI GoToMeeting DeskAway asana huddle liquid Zimbra COLLABNET	BI On Demand birst ENOECA RPX NIGHTSHADE GoodData EdgeSpring visier mixpanel LATTICE ENGINES OMNITURE kognitio pavotek Datameer Roslyn Analytics SUMIRLU SpatialKey	facebook doubleclick millennialmedia SNAPPENEX critool admob badopt tv OpenX bizo twitter bluekai bluefin

### DEVELOPERS & IT

Platform-as-a-Service					
CLOUD FOUNDRY Cloud9 IDE CLOUDFLARE Parse twilio github Madelogic Expect Labs ELASTRA MarkLogic determina Developer cloudshore	heroku piston cloudPassage dotcloud GIGAS PAGES QrImp Simplified xeround	PERIMETER RALLY keynote BRADSOFT New Relic Authentic8 SUMIRLU	PaaS vauntive catchpoint loglogic splunk cloudlife SOASTA keynote BRADSOFT SCALAXTREM RIGHT SCALE Zerto AppDynamics Acronis	ELASTRA MarkLogic determina Developer cloudshore	heroku piston cloudPassage dotcloud GIGAS PAGES QrImp Simplified xeround
Infrastructure-as-a-Service					
IBM amazon.com rackspace salesforce.com ORACLE EUCALYPTUS	GOGRID Parallels terremark SAVVIS	hp vmware Joyent DynamicOps VERTICA	PERIMETER RALLY keynote BRADSOFT New Relic Authentic8 SUMIRLU	ELASTRA MarkLogic determina Developer cloudshore	heroku piston cloudPassage dotcloud GIGAS PAGES QrImp Simplified xeround

# “Definitions”

- EC2 - Virtual Machine but in the cloud
- S3 - Key-value storage (mostly for files)
- DynamoDB - NoSQL database



## Lion Air Data Breach! Another Misconfigured S3 Bucket

Security Boulevard · Last month



## Amazon's cloud was at the heart of the big Capital One hack, even though it doesn't seem to be at fault

Business Insider · Jul 30



## Lyft plans to spend \$300 million on Amazon Web Services through 2021

CNBC · Mar 1



## Contractor's server exposes data from Fortune 100 companies: Ford, Netflix, TD Bank

ZDNet · Jun 28



# Why is it so hard to secure?

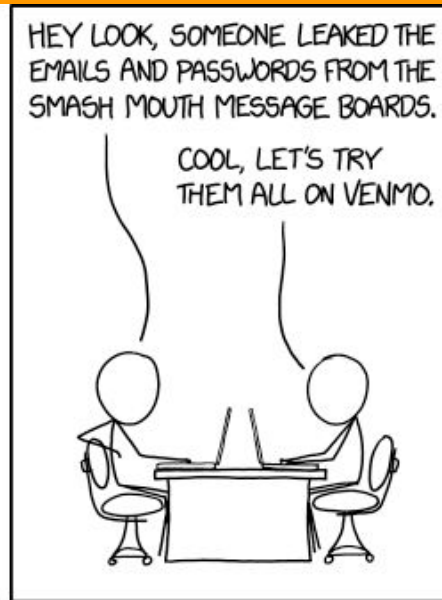
- It's not







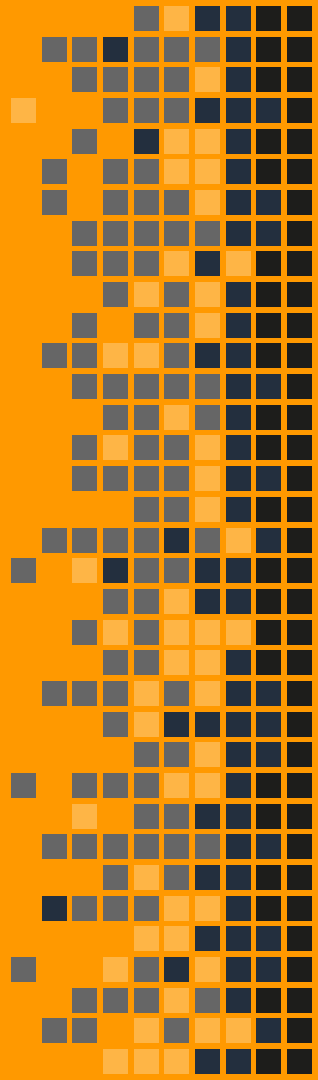
HOW PEOPLE THINK HACKING WORKS



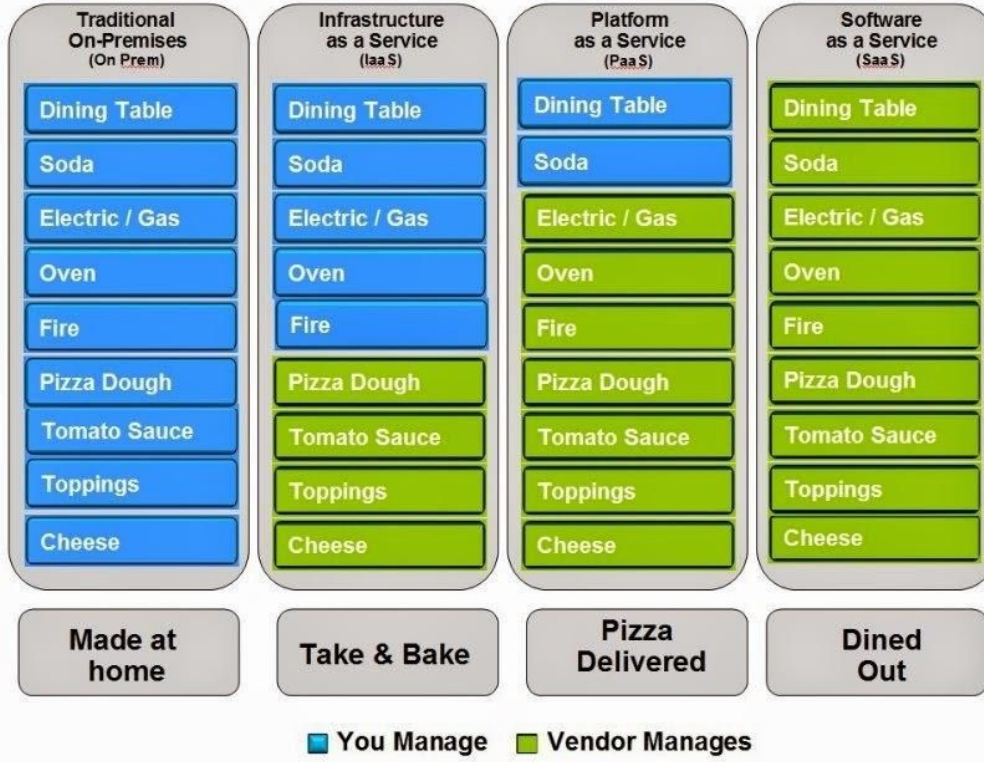
HOW IT ACTUALLY WORKS

# What's different about the cloud?

- Speed
- IaaS, PaaS, SaaS
- No rules!



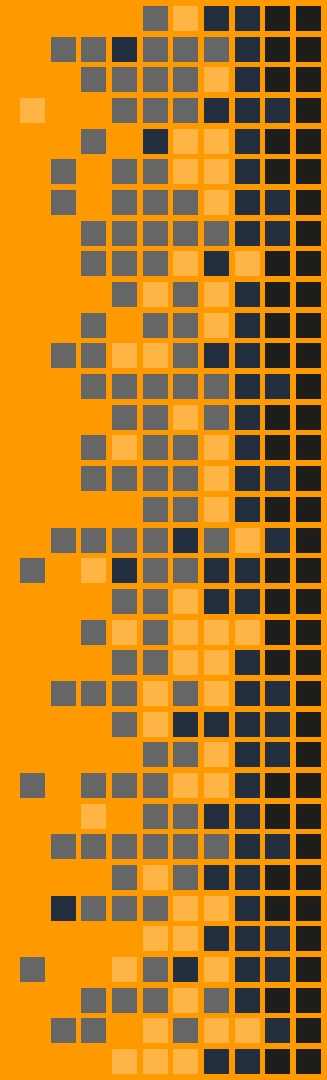
# Pizza as a Service



<https://www.episerver.com/learn/resources/blog/fred-bals/pizza-as-a-service/>

# What is IAM?

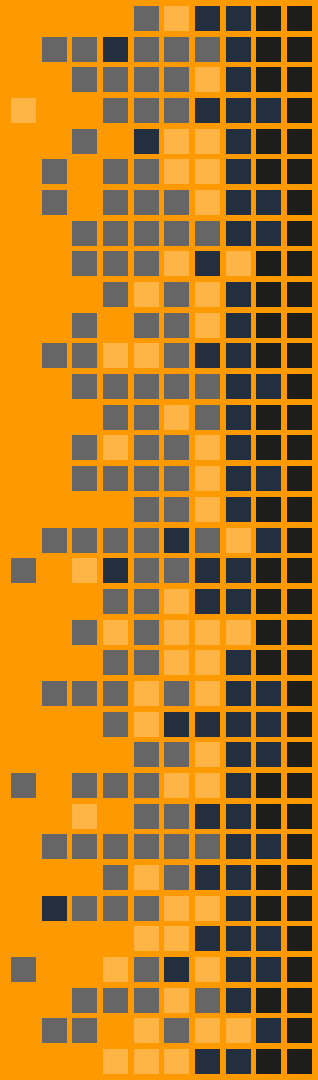
- Identity and Access Management
- Users, API Keys, Roles, Policies
- Omnipresent in the cloud



# Roles

- Like a user, but can be assumed by anyone who needs it.

[https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_roles.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html)



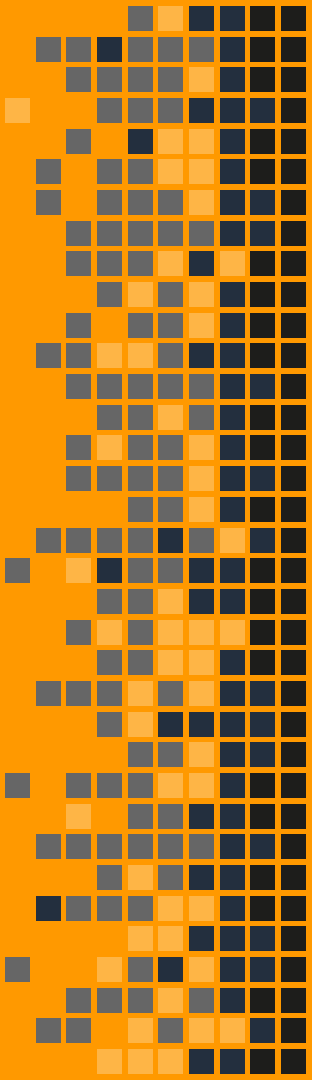
# Roles



# Policies



- Defines permissions for an action.

[https://docs.aws.amazon.com/IAM/latest/UserGuide/access\\_policies.html#targetText=Policies%20and%20Permissions%20or%20resource%2C%20defines%20their%20permissions.](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html#targetText=Policies%20and%20Permissions%20or%20resource%2C%20defines%20their%20permissions.)



# Access Keys

- Used for programmatic access

<input type="checkbox"/>	<a href="#">glimpse-cli</a>	Glimpse	 188 days	None	<a href="#">162 days</a>	Not enabled
<input type="checkbox"/>	<a href="#">molecule</a>	CLI-Permissions	None	None	<a href="#">327 days</a>	Not enabled
<input type="checkbox"/>	<a href="#">nathaniel</a>	Administrators	 38 days	671 days	<a href="#">Today</a>	Not enabled



**Code Spaces**  
Source Code Hosting

Home Features Pricing Contact Us Blog **Sign Up** Login

- ✓ Subversion Hosting
- ✓ Git Hosting
- ✓ Project Management
- ✓ Fast, Reliable & Secure

**Start your free 45-day trial now!**

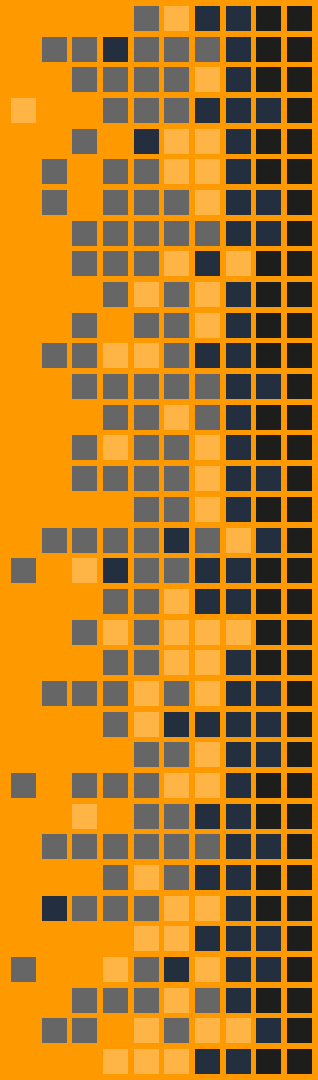
For over 5 years, we've helped ISVs, open source communities, and enterprise development teams manage their code repositories and get their projects launched.

ORACLE ★ macy's Trend Micro RICOH BOSCH TIBCO

<https://blog.trendmicro.com/the-code-spaces-nightmare/>

# Why is IAM so hard?

- It's complicated.



# Why is IAM so hard?

Block public access

Access Control List

Bucket Policy

CORS configuration

## Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, or both. In order to ensure that you turn on Block *all* public access, but before applying any of these settings, ensure that your applications will work correctly for your specific storage use cases. [Learn more](#)

### Block *all* public access

Off

Block public access to buckets and objects granted through *new* access control lists (ACLs)

Off

Block public access to buckets and objects granted through *any* access control lists (ACLs)

Off

Block public access to buckets and objects granted through *new* public bucket policies

Off

Block public and cross-account access to buckets and objects through *any* public bucket policies

Off

# Why is IAM so hard?

Block public access | **Access Control List** | Bucket Policy | CORS configuration

Access for bucket owner

Canonical ID ⓘ	List objects ⓘ	Write objects ⓘ	Read bucket permissions ⓘ	Write bucket permissions ⓘ
<input type="radio"/> [Redacted] (Your AWS account)	Yes	Yes	Yes	Yes

Access for other AWS accounts

[+ Add account](#) [Delete](#)

Canonical ID ⓘ	List objects ⓘ	Write objects ⓘ	Read bucket permissions ⓘ	Write bucket permissions ⓘ
----------------	----------------	-----------------	---------------------------	----------------------------

Public access

Group ⓘ	List objects ⓘ	Write objects ⓘ	Read bucket permissions ⓘ	Write bucket permissions ⓘ
<input type="radio"/> Everyone	-	-	-	-

S3 log delivery group

Group ⓘ	List objects ⓘ	Write objects ⓘ	Read bucket permissions ⓘ	Write bucket permissions ⓘ
<input type="radio"/> Log Delivery	-	-	-	-

# Why is IAM so hard?

Read

<input type="checkbox"/> DescribeJob ?	<input type="checkbox"/> GetBucketRequestPayment ?	<input type="checkbox"/> GetObjectVersion ?
<input type="checkbox"/> GetAccelerateConfiguration ?	<input type="checkbox"/> GetBucketTagging ?	<input type="checkbox"/> GetObjectVersionAcl ?
<input type="checkbox"/> GetAccountPublicAccessBlock ?	<input type="checkbox"/> GetBucketVersioning ?	<input type="checkbox"/> GetObjectVersionForReplication ?
<input type="checkbox"/> GetAnalyticsConfiguration ?	<input type="checkbox"/> GetBucketWebsite ?	<input type="checkbox"/> GetObjectVersionTagging ?
<input type="checkbox"/> GetBucketAcl ?	<input type="checkbox"/> GetEncryptionConfiguration ?	<input type="checkbox"/> GetObjectVersionTorrent ?
<input type="checkbox"/> GetBucketCORS ?	<input type="checkbox"/> GetInventoryConfiguration ?	<input type="checkbox"/> GetReplicationConfiguration ?
<input type="checkbox"/> GetBucketLocation ?	<input type="checkbox"/> GetLifecycleConfiguration ?	<input type="checkbox"/> ListBucketByTags ?
<input type="checkbox"/> GetBucketLogging ?	<input type="checkbox"/> GetMetricsConfiguration ?	<input type="checkbox"/> ListBucketMultipartUploads ?
<input type="checkbox"/> GetBucketNotification ?	<input type="checkbox"/> GetObject ?	<input type="checkbox"/> ListBucketVersions ?
<input type="checkbox"/> GetBucketPolicy ?	<input type="checkbox"/> GetObjectAcl ?	<input type="checkbox"/> ListJobs ?
<input type="checkbox"/> GetBucketPolicyStatus ?	<input type="checkbox"/> GetObjectTagging ?	<input type="checkbox"/> ListMultipartUploadParts ?
<input type="checkbox"/> GetBucketPublicAccessBlock ?	<input type="checkbox"/> GetObjectTorrent ?	

# Why is IAM so hard?

Read

<input type="checkbox"/> DescribeJob ?	<input type="checkbox"/> GetBucketRequestPayment ?	<input type="checkbox"/> GetObjectVersion ?
<input type="checkbox"/> GetAccelerateConfiguration ?	<input type="checkbox"/> GetBucketTagging ?	<input type="checkbox"/> GetObjectVersionAcl ?
<input type="checkbox"/> GetAccountPublicAccessBlock ?	<input type="checkbox"/> GetBucketVersioning ?	<input type="checkbox"/> GetObjectVersionForReplication ?
<input type="checkbox"/> GetAnalyticsConfiguration ?	<input type="checkbox"/> GetBucketWebsite ?	<input type="checkbox"/> GetObjectVersionTagging ?
<input type="checkbox"/> GetBucketAcl ?	<input type="checkbox"/> GetEncryptionConfiguration ?	<input type="checkbox"/> GetObjectVersionTorrent ?
<input type="checkbox"/> GetBucketCORS ?	<input type="checkbox"/> GetInventoryConfiguration ?	<input type="checkbox"/> GetReplicationConfiguration ?
<input type="checkbox"/> GetBucketLocation ?	<input type="checkbox"/> GetLifecycleConfiguration ?	<input type="checkbox"/> ListBucketByTags ?
<input type="checkbox"/> GetBucketLogging ?	<input type="checkbox"/> GetMetricsConfiguration ?	<input type="checkbox"/> ListBucketMultipartUploads ?
<input type="checkbox"/> GetBucketNotification ?	<input type="checkbox"/> <b>GetObject ?</b>	<input type="checkbox"/> ListBucketVersions ?
<input type="checkbox"/> GetBucketPolicy ?	<input type="checkbox"/> GetObjectAcl ?	<input type="checkbox"/> ListJobs ?
<input type="checkbox"/> GetBucketPolicyStatus ?	<input type="checkbox"/> GetObjectTagging ?	<input type="checkbox"/> ListMultipartUploadParts ?
<input type="checkbox"/> GetBucketPublicAccessBlock ?	<input type="checkbox"/> GetObjectTorrent ?	

# Why is IAM so hard?

## ▼ Write

- |   |   |  |
|---|---|--|
| <input type="checkbox"/> AbortMultipartUpload ?             | <input type="checkbox"/> PutAnalyticsConfiguration ?        | <input type="checkbox"/> PutMetricsConfiguration ?     |
| <input type="checkbox"/> CreateBucket ?                     | <input type="checkbox"/> PutBucketCORS ?                    | <input type="checkbox"/> PutObject ?                   |
| <input type="checkbox"/> CreateJob ?                        | <input type="checkbox"/> PutBucketLogging ?                 | <input type="checkbox"/> PutObjectLegalHold ?          |
| <input type="checkbox"/> DeleteBucket ?                     | <input type="checkbox"/> PutBucketNotification ?            | <input type="checkbox"/> PutObjectRetention ?          |
| <input type="checkbox"/> DeleteBucketWebsite ?              | <input type="checkbox"/> PutBucketObjectLockConfiguration ? | <input type="checkbox"/> PutReplicationConfiguration ? |
| <input type="checkbox"/> DeleteObject ?                     | <input type="checkbox"/> PutBucketRequestPayment ?          | <input type="checkbox"/> ReplicateDelete ?             |
| <input type="checkbox"/> DeleteObjectVersion ?              | <input type="checkbox"/> PutBucketVersioning ?              | <input type="checkbox"/> ReplicateObject ?             |
| <input type="checkbox"/> GetBucketObjectLockConfiguration ? | <input type="checkbox"/> PutBucketWebsite ?                 | <input type="checkbox"/> RestoreObject ?               |
| <input type="checkbox"/> GetObjectLegalHold ?               | <input type="checkbox"/> PutEncryptionConfiguration ?       | <input type="checkbox"/> UpdateJobPriority ?           |
| <input type="checkbox"/> GetObjectRetention ?               | <input type="checkbox"/> PutInventoryConfiguration ?        | <input type="checkbox"/> UpdateJobStatus ?             |
| <input type="checkbox"/> PutAccelerateConfiguration ?       | <input type="checkbox"/> PutLifecycleConfiguration ?        |  |

# Why is IAM so hard?

▼  Write

<input type="checkbox"/> AbortMultipartUpload ?	<input type="checkbox"/> PutAnalyticsConfiguration ?	<input type="checkbox"/> PutMetricsConfiguration ?
<input type="checkbox"/> CreateBucket ?	<input type="checkbox"/> PutBucketCORS ?	<input type="checkbox"/> PutObject ?
<input type="checkbox"/> CreateJob ?	<input type="checkbox"/> PutBucketLogging ?	<input type="checkbox"/> PutObjectLegalHold ?
<input type="checkbox"/> DeleteBucket ?	<input type="checkbox"/> PutBucketNotification ?	<input type="checkbox"/> PutObjectRetention ?
<input type="checkbox"/> DeleteBucketWebsite ?	<input type="checkbox"/> PutBucketObjectLockConfiguration ?	<input type="checkbox"/> PutReplicationConfiguration ?
<input type="checkbox"/> DeleteObject ?	<input type="checkbox"/> PutBucketRequestPayment ?	<input type="checkbox"/> ReplicateDelete ?
<input type="checkbox"/> DeleteObjectVersion ?	<input type="checkbox"/> PutBucketVersioning ?	<input type="checkbox"/> ReplicateObject ?
<input type="checkbox"/> GetBucketObjectLockConfiguration ?	<input type="checkbox"/> PutBucketWebsite ?	<input type="checkbox"/> RestoreObject ?
<input type="checkbox"/> GetObjectLegalHold ?	<input type="checkbox"/> PutEncryptionConfiguration ?	<input type="checkbox"/> UpdateJobPriority ?
<input type="checkbox"/> GetObjectRetention ?	<input type="checkbox"/> PutInventoryConfiguration ?	<input type="checkbox"/> UpdateJobStatus ?
<input type="checkbox"/> PutAccelerateConfiguration ?	<input type="checkbox"/> PutLifecycleConfiguration ?	



# Why is IAM so hard?

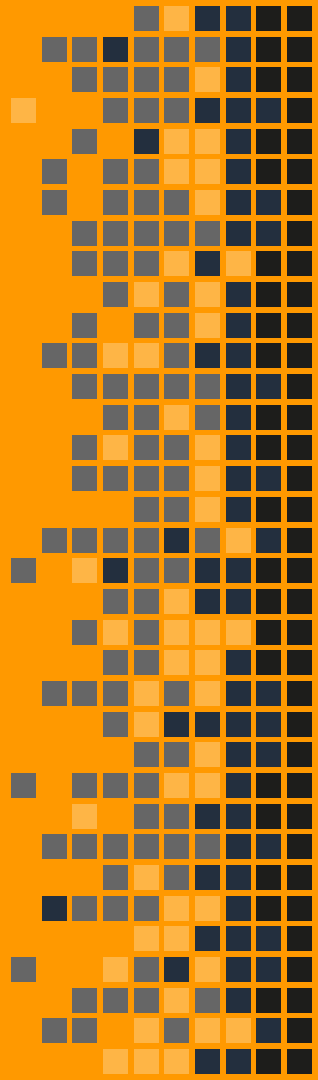
- It's preventive.



*Every developer using the cloud. (Circa 2019)*

# AWS Metadata Service

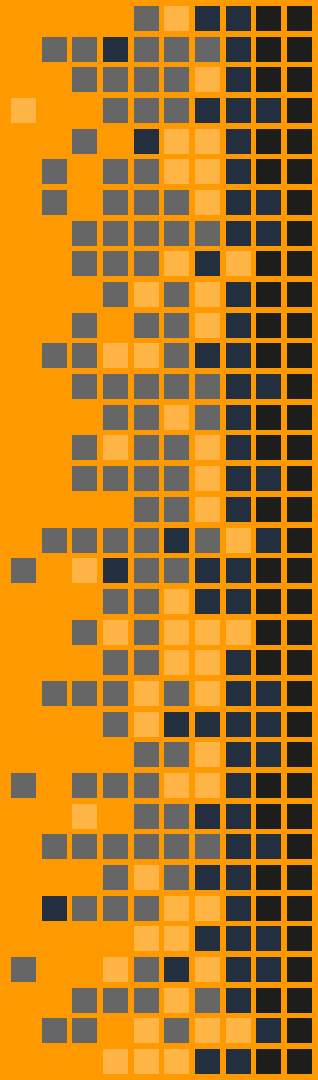
```
ubuntu@ip-172-31-11-136:~$ curl http://169.254.169.254/2018-09-24/meta-data/  
ami-id  
ami-launch-index  
ami-manifest-path  
block-device-mapping/  
events/  
hostname  
iam/  
identity-credentials/  
instance-action  
instance-id  
instance-type  
local-hostname  
local-ipv4  
mac  
metrics/  
network/  
placement/  
profile  
public-hostname  
public-ipv4  
public-keys/  
reservation-id  
security-groups  
services/ubuntu@ip-172-31-11-136:~$ █
```





# Capital One

- Some application was vulnerable to SSRF
- WAF let SSRF through
- Role had read access to all S3 buckets



# What is the solution?

- Cloud is special
- Least privilege is best privilege
- Monitor API key usage
- Automate, automate, automate




# Least Privilege in AWS

## AWS Access Advisor

Filter: No filter ▾

Service Name ↕	Policies Granting Permissions	Last Accessed ▾
AWS Security Token Service	<a href="#">AdministratorAccess</a>	169 days ago
Amazon EC2	<a href="#">AdministratorAccess</a>	169 days ago
Alexa for Business	<a href="#">AdministratorAccess</a>	Not accessed in the tracking period
AWS Accounts	<a href="#">AdministratorAccess</a>	Not accessed in the tracking period
AWS Certificate Manager	<a href="#">AdministratorAccess</a>	Not accessed in the tracking period

 duo-labs / cloudtracker

 Netflix / repokid



# Resources



<https://expel.io/blog/>



<https://flaws.cloud>

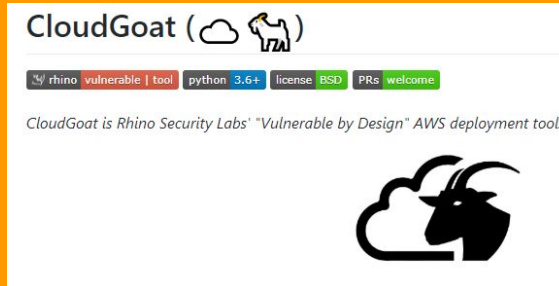
<https://flaws2.cloud>



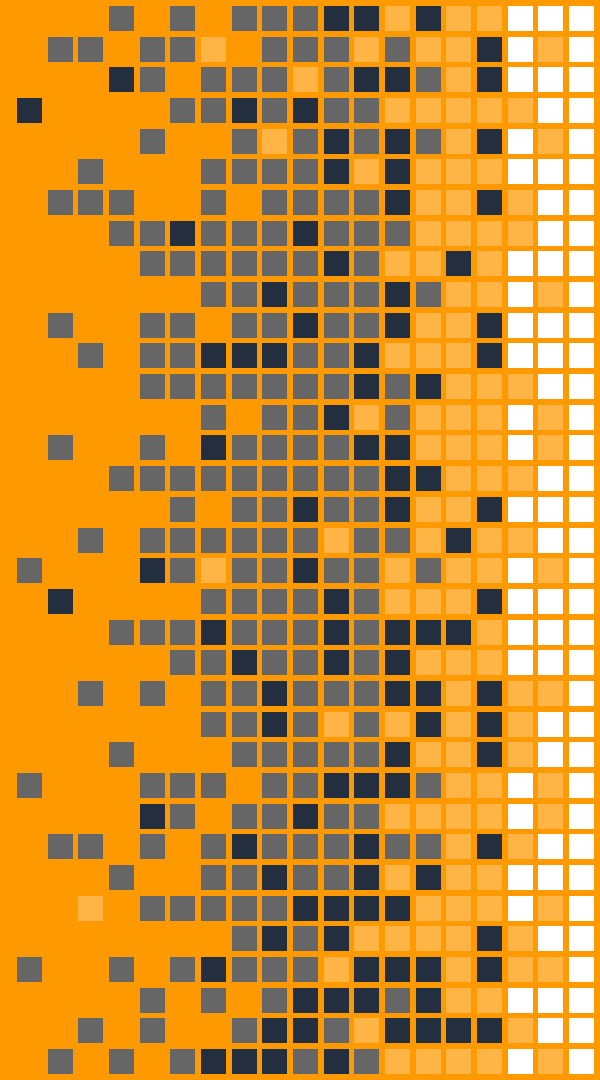
A screenshot of a Twitter profile for Corey Quinn. The header image shows a man with a surprised expression in front of a whiteboard with the text 'BILLED ON aws' and various technical diagrams. The profile name is 'Corey Quinn at Monktoberfest' with the handle '@QuinnyPig'. The bio identifies him as a 'Cloud Economist at the Duckbill Group' and lists his website and podcast. Location is 'San Francisco, CA' and he joined in December 2009.



A screenshot of a Twitter profile for Rhino Security Labs. The header image shows the company logo and a stylized rhino head. The profile name is 'Rhino Security Labs' with the handle '@RhinoSecurity'. The bio describes the firm as a 'top penetration testing and security assessment firm with a focus on cloud (AWS, GCP, Azure), network, and web application pentesting'. Location is 'Seattle, WA' and they joined in February 2013.



A screenshot of the CloudGoat project page. The title is 'CloudGoat' with a cloud and a goat icon. Below the title are tags: 'rhino', 'vulnerable', 'tool', 'python', '3.6+', 'license', 'BSD', 'PRs', and 'welcome'. The description states: 'CloudGoat is Rhino Security Labs' "Vulnerable by Design" AWS deployment tool.' A large logo of a goat's head inside a cloud shape is at the bottom right.



# Questions?

