

Challenges and Opportunities in the Cloud



Scott Piper

@0xdabbad00

SummitRoute.com

scott@summitroute.com

whoami

- Independent AWS security consultant



Scott Piper

@0xdabbad00

SummitRoute.com

scott@summitroute.com

Salt Lake City, Utah

- Creator of:



flAWS - <http://flaws.cloud/>



CloudMapper - <https://github.com/duo-labs/cloudmapper>

CloudTracker - <https://github.com/duo-labs/cloudtracker>

aws 
CERTIFIED

Solutions Architect
Associate

aws 
CERTIFIED

Developer
Associate

aws 
CERTIFIED

SysOps Administrator
Associate

aws 
CERTIFIED

Solutions Architect
Professional

aws 
CERTIFIED

DevOps Engineer
Professional

aws 
CERTIFIED

Security
Specialty



Public Cloud Market Share



Other
25.0%

IBM

1.9%

Google

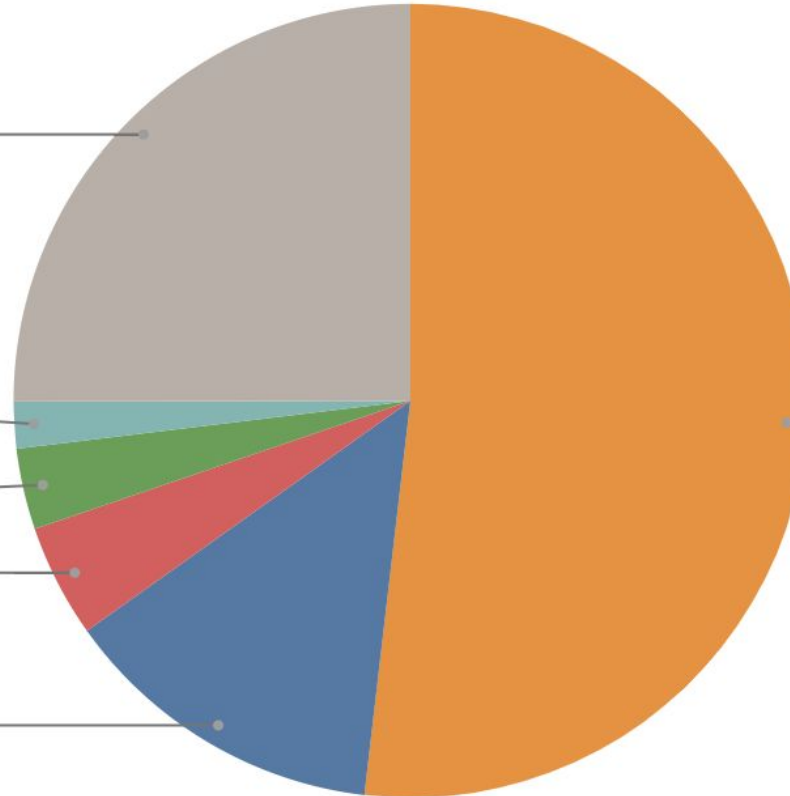
3.3%

Alibaba

4.6%

Microsoft

13.3%



amazon

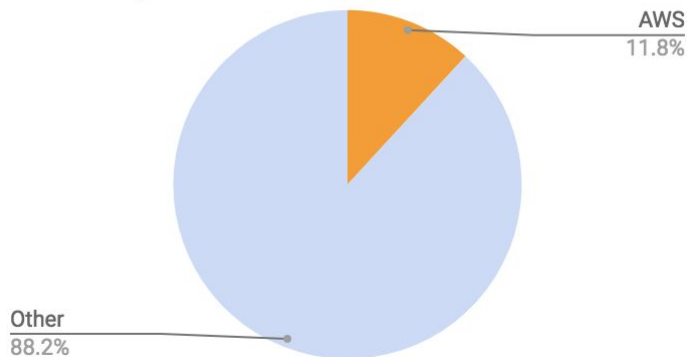
Amazon
51.9%

How big is AWS at Amazon?

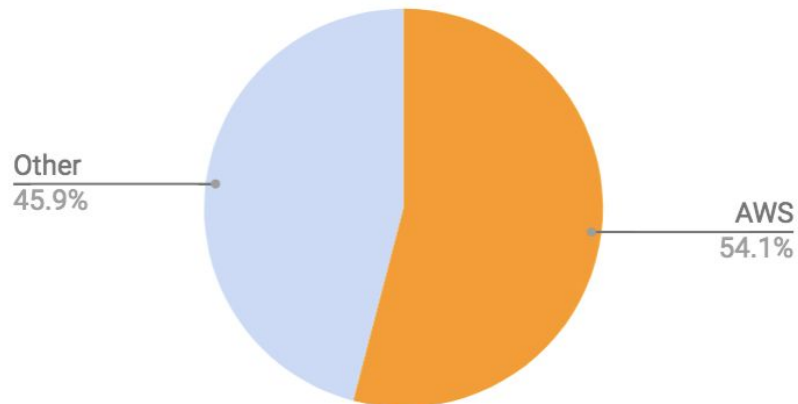
Quarterly results in Billions \$

	Revenue	Operating Income
AWS	6.7	2
Other	49.9	1.7
Total	56.6	3.7

Quarterly Revenue



Quarterly Operating Income



Amazon Sep 30, 2018 - 10-Q

<https://ir.aboutamazon.com/static-files/87c56999-1e07-426d-b388-2997f25c8ec5>

"it's still the Wild West. There aren't enough skilled defenders in the world to protect everybody's on-prem IT, so you can either join the well-guarded townships and follow their rules or enjoy the freedom of your own homestead until the bandits come for you."

Alex Stamos - Former CISO of Facebook

<https://twitter.com/alexstamos/status/993258342230376448>

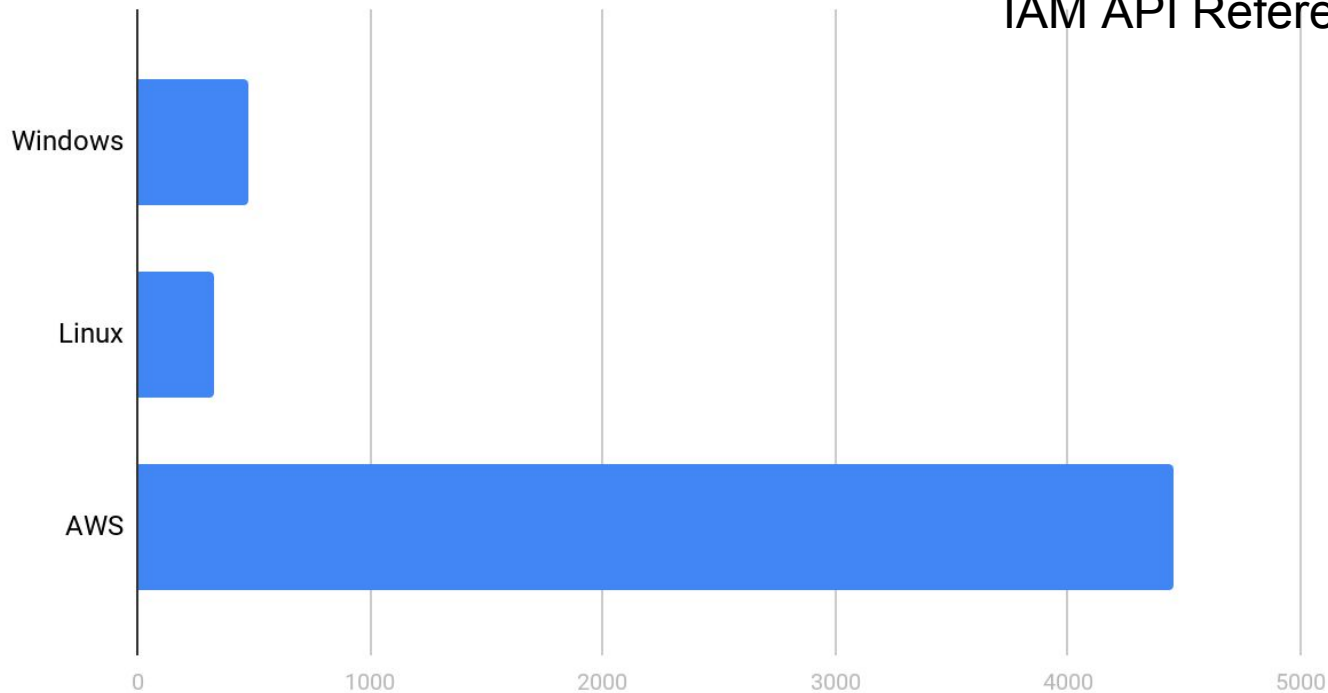
"The number of known attacks against AWS is small, which is at odds with the huge number (and complexity) of services available. It's not a deep insight to argue that the number of classes of cloud specific attacks will rise."

- Marco Slaviero, Thinkst

<http://blog.thinkst.com/2017/09/farseeing-look-at-beyondcorp.html>

The cloud is complex

API functions



IAM User Guide: 1106 pages

IAM API Reference: 442 pages

145 services

4455 API functions

Amazon does security things you don't

Get's advanced notification of vulnerabilities:

- Xen pre-disclosure list

Uses Automated Reasoning

- Firmware verification
- Crypto verification

Buys their datacenters under shell companies.

Has a dedicated DDoS response team, their own threat intel, and more.

But lacks security you might want

Amazon Elasticsearch Service now supports encrypted communication between Elasticsearch nodes

Posted On: Sep 18, 2018



- Account recovery (ie. takeover) only requires access to the root email
 - All communications from AWS go to your root account email
 - Forces you to have many people on a distribution list to receive these
 - There is no way to remove account recovery
 - All accounts have the same level of security
- Can also fax a notarized form to take over an account

What can happen if your AWS account is compromised?

An attacker compromised Code Spaces (a github competitor) in 2014.

Attacker back-doored the account, so when he discovered the employees trying to regain control, he started deleting everything.

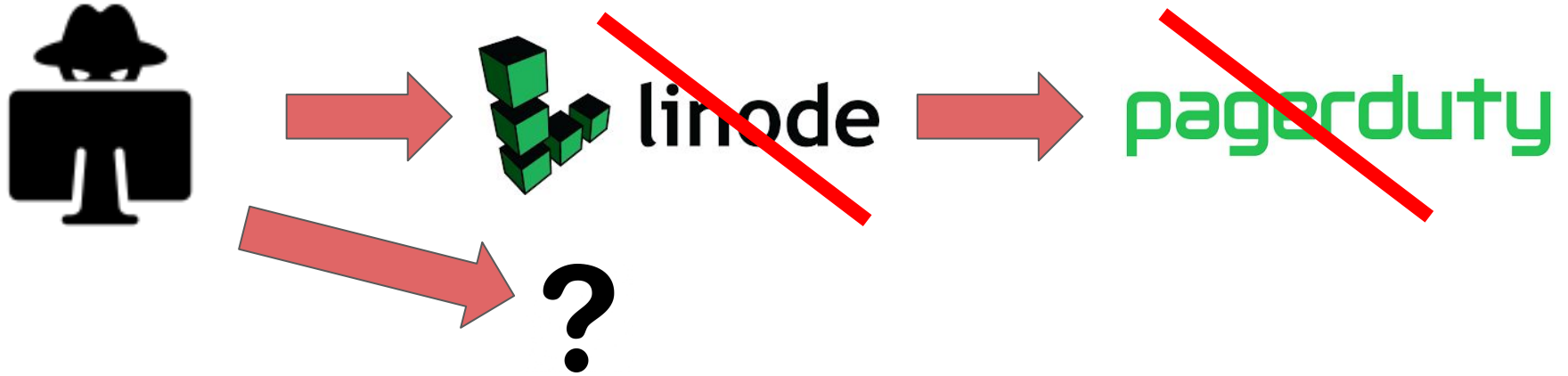
Code Spaces had backups, but they were all in that one account.

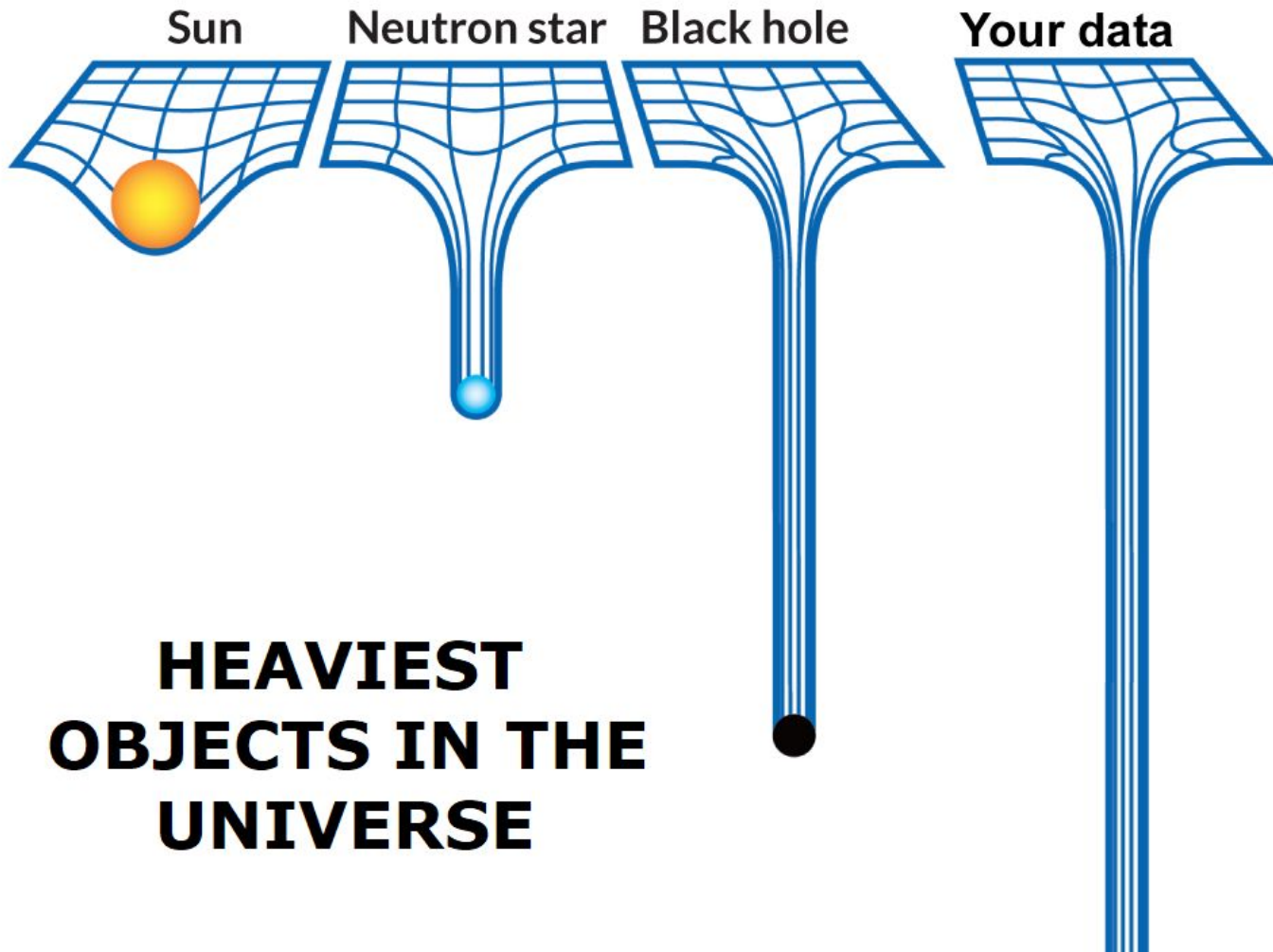
Code Spaces shut down the next day.

Have a solid backup plan!



When your cloud provider is compromised







People often use the lowest common denominator of services when using a multi-cloud strategy.

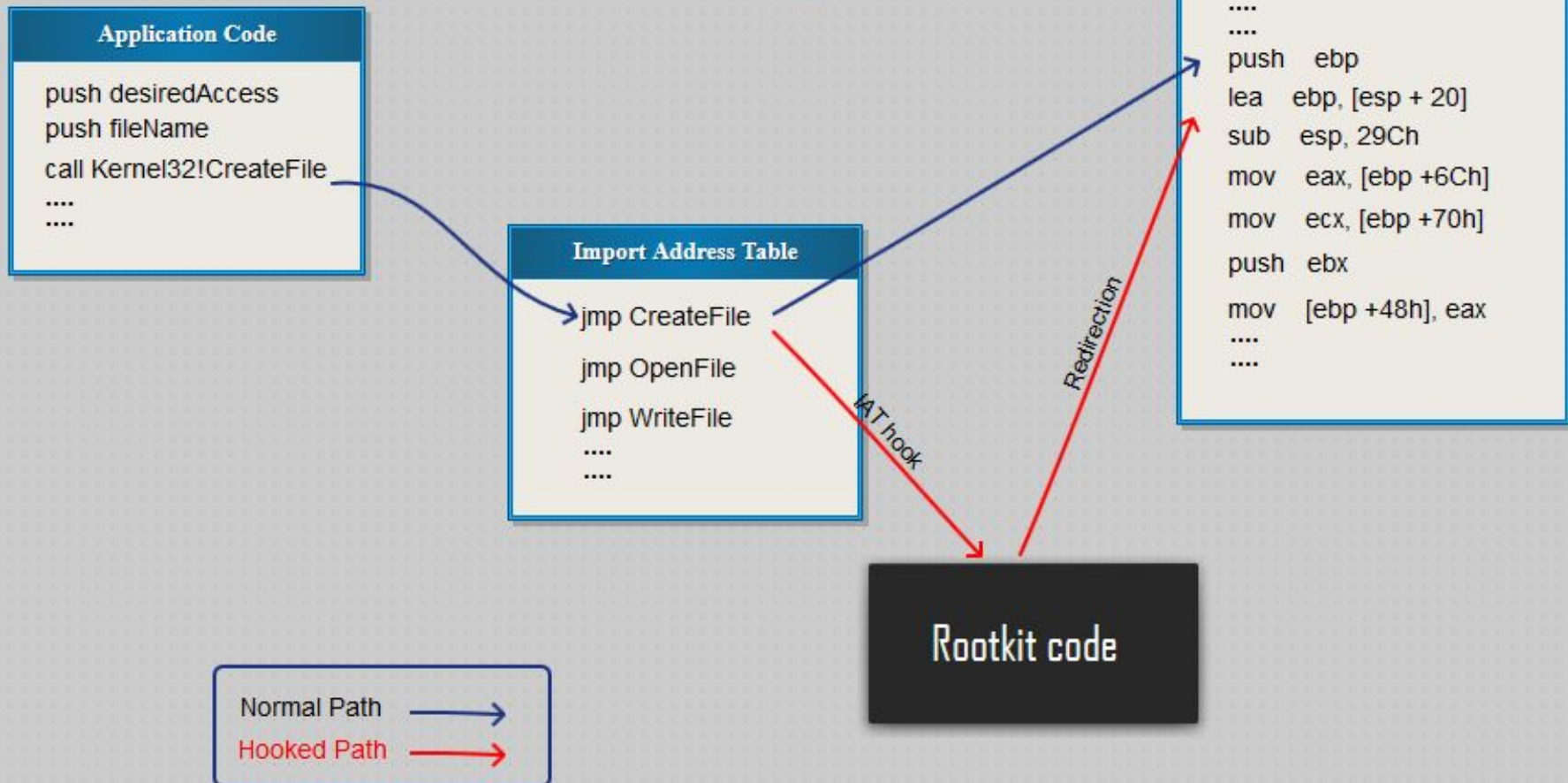
Dangers of the cloud

Your company becomes 100% dependent on a vendor. What if the vendor...

- disappears?
- kicks you off their platform?



IAT Hooking





Permissions

Groups

Security credentials

Access Advisor

Access advisor shows the service permissions granted to this user and when those services were last accessed. You can use this information to revise your policies. [Learn more](#)

Note: Recent activity usually appears within 4 hours. Data is stored for a maximum of 365 days, depending when your region began supporting this feature. [Learn more](#)

Filter: No filter ▾

Showing 2 results

Service Name ▾

Policies Granting Permissi...

Last Accessed ▾

Amazon S3

Level3

Today

Amazon EC2

Level3

Today

Announcing AWS CloudTrail

Posted On: Nov 13, 2013

Service	Launch date	CloudTrail integration	Delta
Route 53	Dec 2010	Feb 2015	4 years
WorkMail	Jan 2016	Dec 2017	2 years
AppStream	Dec 2016	N/A	2 years so far

```
PS C:\> aws appstream describe-fleets
```

```
An error occurred (AccessDeniedException) when calling the DescribeFleets operation:  
User: arn:aws:iam::2[REDACTED]:user/path/TestUser is not authorized to perform: ap  
pstream:DescribeFleets on resource: arn:aws:appstream:us-west-2:2[REDACTED]:fleet/*
```

Mandiant observed that the attacker had granted compromised accounts read access to hundreds of mailboxes with the “Add-MailboxPermission” cmdlet (Fig. 5).

Following the assignment of mailbox permissions, the attacker authenticated to the victim organization’s Outlook Web Access (OWA) portal to access targeted inboxes. By assigning these permissions to a single account, the attacker was able to read, access and steal hundreds of emails in a single view.



The attacker could also blend into normal day-to-day activities of users accessing their email through the OWA portal, and did not need to install any additional malware into the environment. Ultimately, APT35 had used access to hundreds of mailboxes to read email communications and steal data related to Middle East organizations, which later became victims of destructive attacks.


Third-party app is named "Google Docs."



Third-party app uses Google Drive logo.

Google Docs would like to:

 Read, send, delete, and manage your email 

 Manage your contacts 

Third-party app wants full e-mail control.

By clicking Allow, you allow this app and Google to use your information in accordance with their respective [terms of service](#) and [privacy policies](#). You can change this and other [Account Permissions](#) at any time.

Deny

Allow



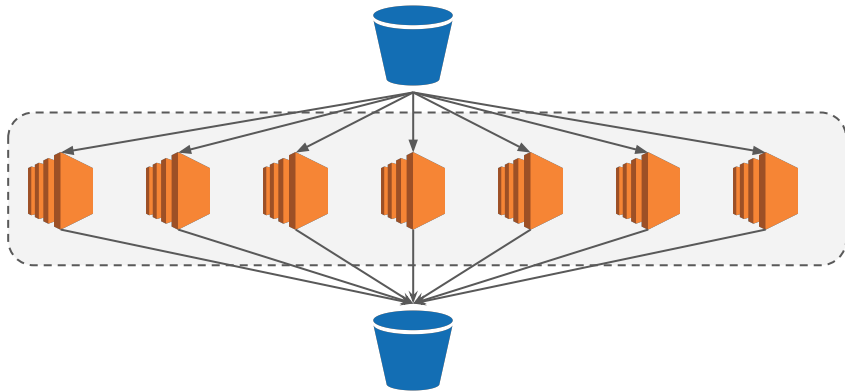
SHAT TERE O



StreamAlert

CloudTracker

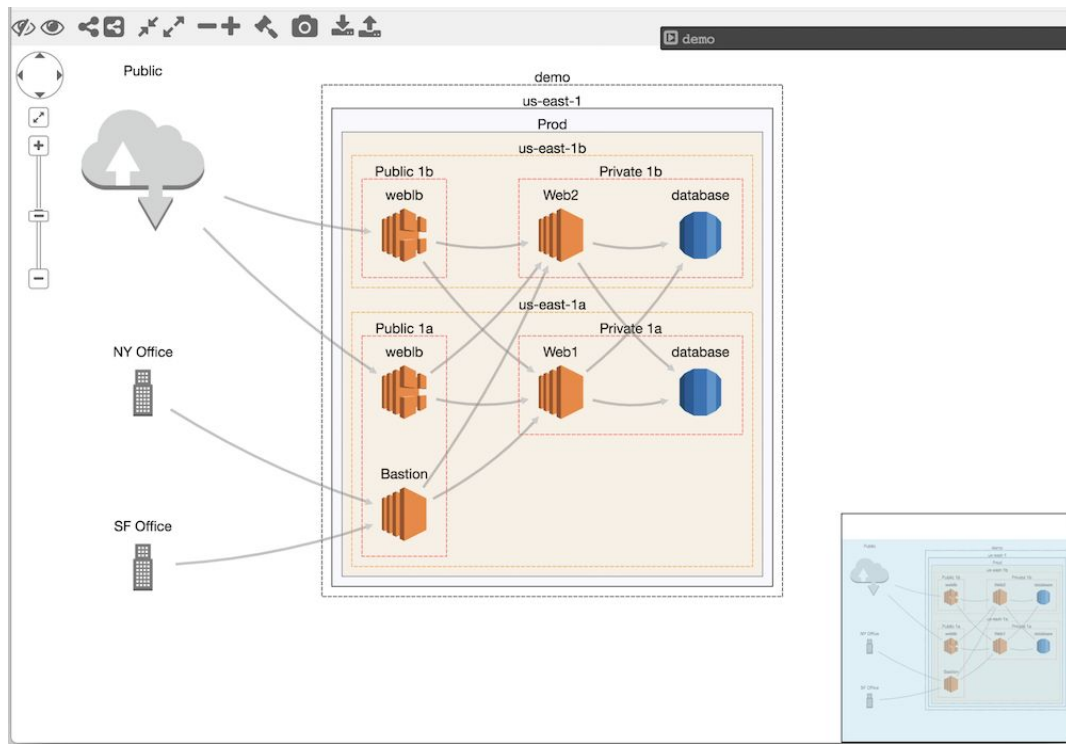
Privileges granted	Privileges used	Recommended privilege adjustment
CreateBucket	CreateBucket	CreateBucket
DeleteBucket		- DeleteBucket



APIs and logs

- Standing up servers is now done through APIs and that is logged
- All firewall configuration changes are logged, and the current rule set is queryable

There is still very little tooling to take advantage of the data available.



APIs and Logs

- Find out every server that is publicly exposed
 - Be able to query its configuration
- Find every API call those users made
 - Restrict their access to exactly those APIs
- Know every resource a user can read or modify
- Know where every application is running
- Visualize the resources and pathways used by every application
- Give auditors only read-only privileges to see only metadata



Google Cloud Platform

GitHub



AWS Partitions

1. AWS Standard
2. AWS China
3. AWS GovCloud
4. AWS Secret Region



Thank you



Scott Piper

@0xdabbad00

SummitRoute.com

scott@summitroute.com