I got 10 trillion problems, but logging ain't one

John Graham-Cumming

CLOUDFLARE


London
Seattle
Chicago
Toronto
Newark
San Jose
Ashburn
Los Angeles
Dallas
Atlanta
Miami
Singapore

CLOUDFLARE


Seattle
San Jose
Los Angeles
Chicago
Dallas
Toronto
Newark
Ashburn
Atlanta
Miami
Düsseldorf
London
Amsterdam
Paris
Frankfurt
Madrid
Milan
Stockholm
Warsaw
Prague
Vienna
Singapore

CLOUDFLARE


Seattle
San Jose
Los Angeles
Chicago
Dallas
Toronto
Newark
Ashburn
Atlanta
Miami
Düsseldorf
London
Amsterdam
Paris
Frankfurt
Madrid
Stockholm
Warsaw
Prague
Vienna
Milan
Seoul
Tokyo
Hong Kong
Singapore

CLOUDFLARE


Düsseldorf
London
Amsterdam
Paris
Frankfurt
Madrid
Stockholm
Warsaw
Prague
Vienna
Milan
Seattle
San Jose
Los Angeles
Chicago
Dallas
Toronto
Newark
Ashburn
Atlanta
Miami
Medellín
Lima
Valparaíso
São Paulo
Buenos Aires
Johannesburg
Seoul
Tokyo
Hong Kong
Singapore
Sydney
Melbourne
Auckland

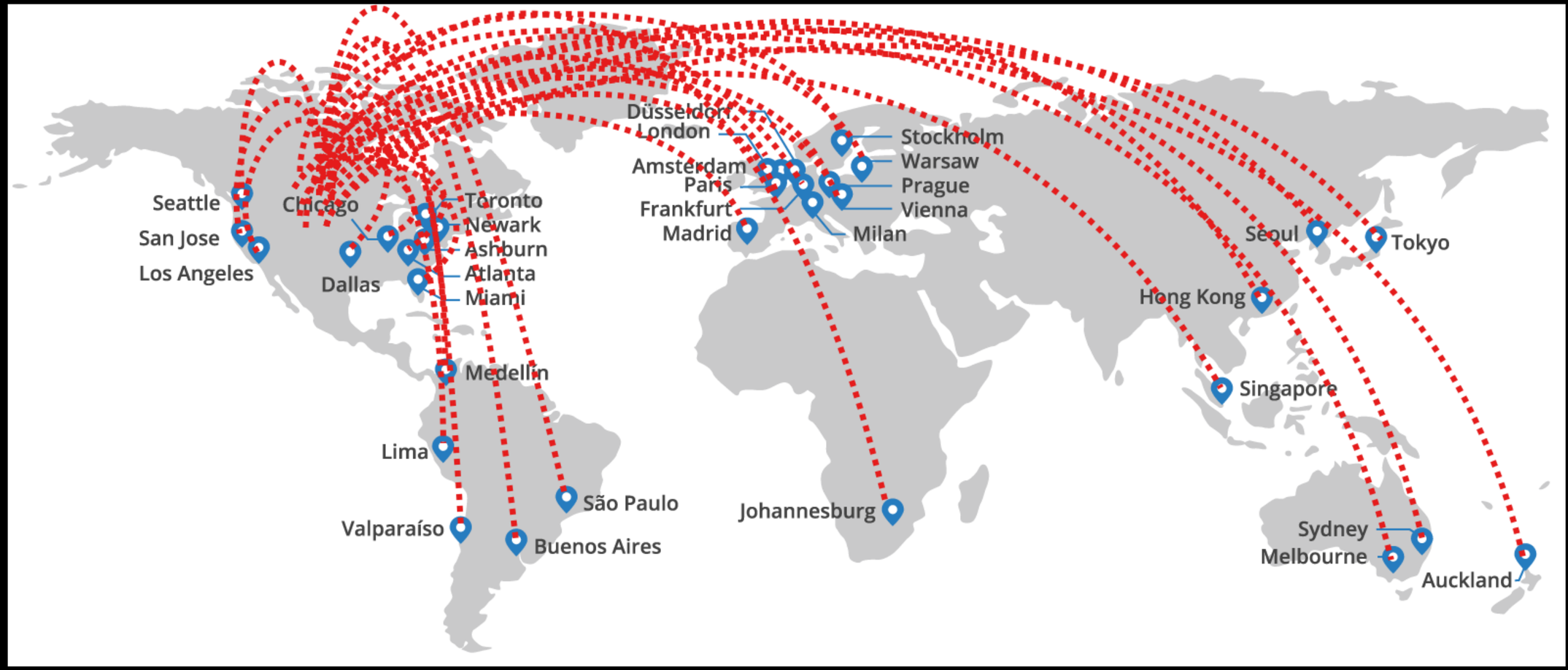
CLOUDFLARE


Düsseldorf
London
Amsterdam
Paris
Frankfurt
Madrid
Stockholm
Warsaw
Prague
Vienna
Milan
Seattle
San Jose
Los Angeles
Chicago
Dallas
Toronto
Newark
Ashburn
Atlanta
Miami
Medellín
Lima
Valparaíso
São Paulo
Buenos Aires
Johannesburg
Seoul
Tokyo
Hong Kong
Singapore
Sydney
Melbourne
Auckland

CLOUDFLARE


Düsseldorf
London
Amsterdam
Paris
Frankfurt
Madrid
Stockholm
Warsaw
Prague
Vienna
Milan
Seattle
Chicago
San Jose
Los Angeles
Dallas
Toronto
Newark
Ashburn
Atlanta
Miami
Medellín
Lima
São Paulo
Valparaíso
Buenos Aires
Johannesburg
Seoul
Tokyo
Hong Kong
Singapore
Sydney
Melbourne
Auckland

CLOUDFLARE


Seattle
San Jose
Los Angeles
Chicago
Dallas
Toronto
Newark
Ashburn
Atlanta
Miami
Medellín
Lima
Valparaíso
São Paulo
Buenos Aires
Johannesburg
Düsseldorf
London
Amsterdam
Paris
Frankfurt
Madrid
Stockholm
Warsaw
Prague
Vienna
Milan
Seoul
Tokyo
Hong Kong
Singapore
Sydney
Melbourne
Auckland

CLOUDFLARE


BRACE YOURSELVES
THE LOG LINES ARE COMING
memegenerator.net

CLOUDFLARE

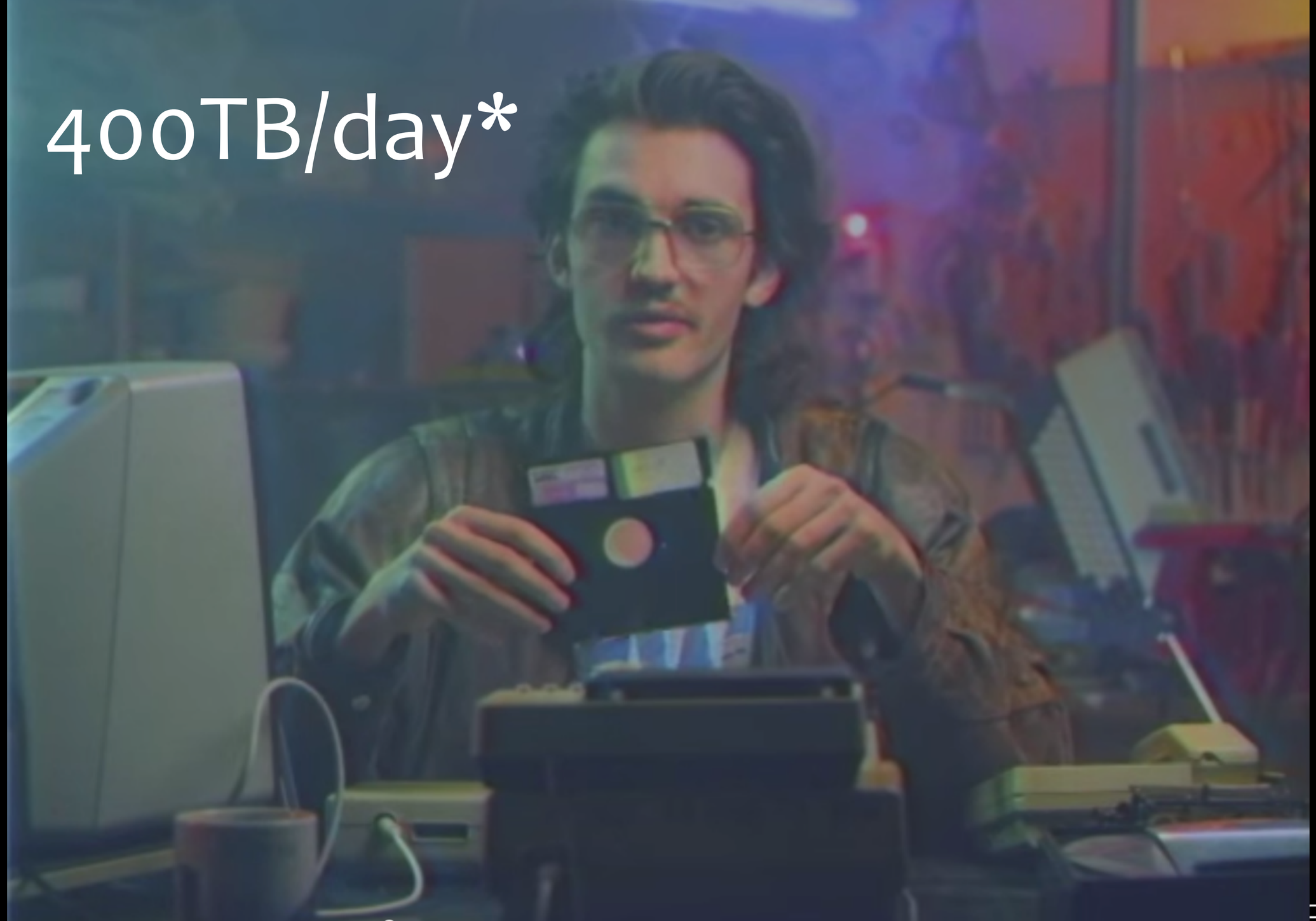
10 trillion HTTP requests
per month

4Mhz log lines

A log processing* company
that also runs a CDN and
web security service

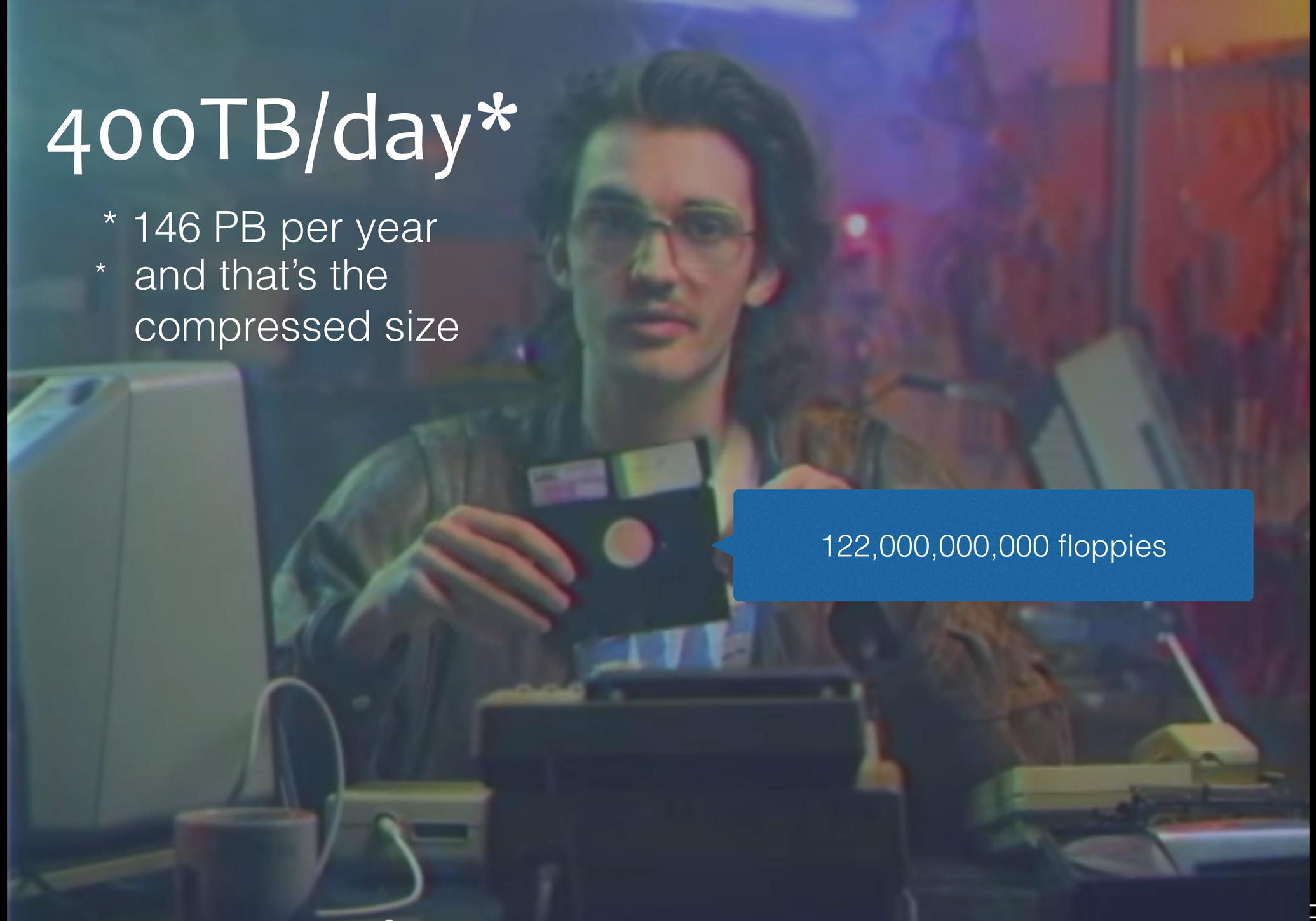
A log processing* company
that also runs a CDN and
web security service

*not storage


400TB/day*


400TB/day*
* 146 PB per year


400TB/day*
* 146 PB per year
* and that's the compressed size


400TB/day*
* 146 PB per year
* and that's the compressed size
122,000,000,000 floppies
CLOUDFLARE

Privacy

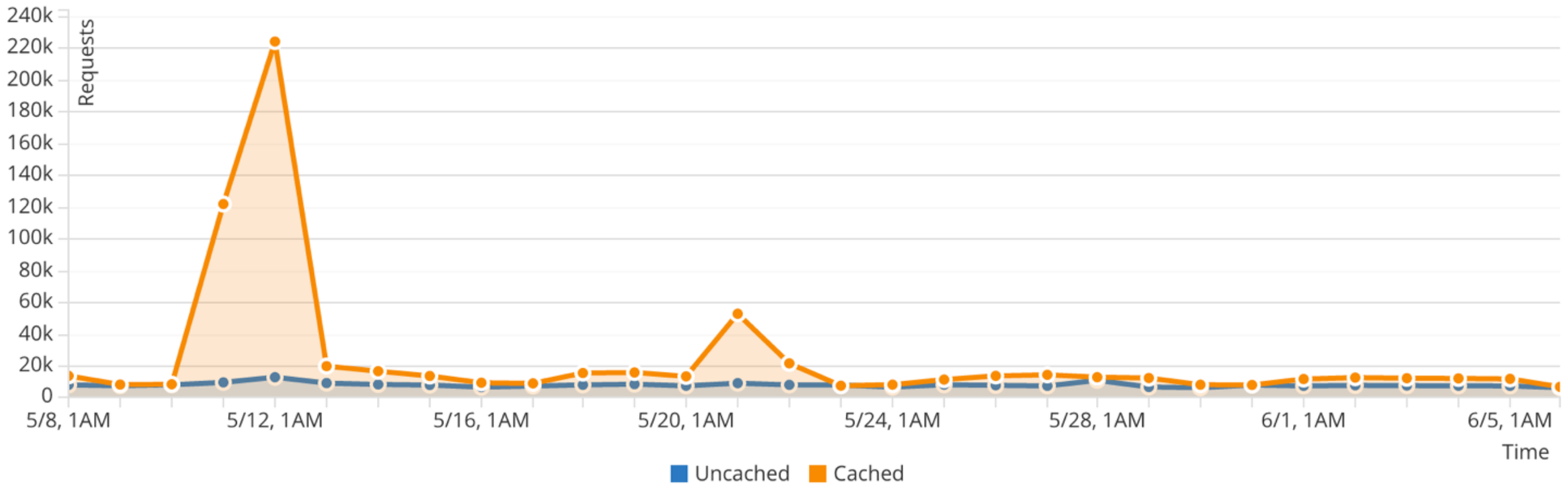
Three Things

- Provide charts for our customers
- Give customers data about attacks
- Automatically spot attacks in real-time

Requests Through CloudFlare

Requests • Bandwidth • Unique Visitors • Threats

Total Requests	Cached Requests	Uncached Requests
Last Month	Last Month	Last Month
950,299	719,254	231,045



CLOUDFLARE

100030	Challenge	1[redacted]6	US	jgc.org	3 minutes ago	Details

100030

Date: 06/08/2015

Time: 09:14:20 +02:00

Data Center: SJC

Action: challenge

IP Address: 1[redacted]6 Filter On This | Block | Challenge | Whitelist

Details

Location: US Block | Challenge | Whitelist

User Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/43.0.2357.81 Safari/537.36

Host: jgc.org

URI: /?try_to_be_bad=%3Cscript%3Ealert(%22pwned!%22);%3C/script%3E

CLOUDFLARE

Things we ❤️

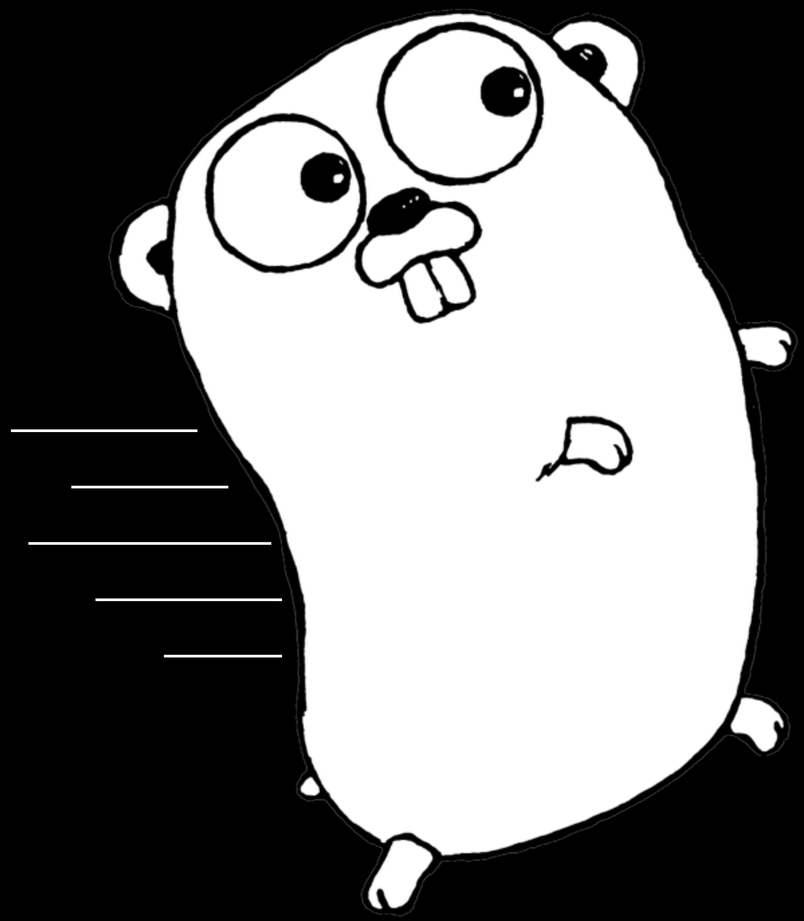
- NGINX + LuaJIT
- Cap’n Proto
- Apache Kafka
- Redis
- Go
- Postgres and CitusDB
- Streaming Algorithms

Things we ❤️

- NGINX + LuaJIT
- Cap’n Proto
- Apache Kafka
- Redis
- Go
- Postgres and CitusDB
- Streaming Algorithms

Things we ❤️

- NGINX + LuaJIT
- Cap’n Proto
- Apache Kafka
- Redis
- Go
- Postgres and CitusDB
- Streaming Algorithms



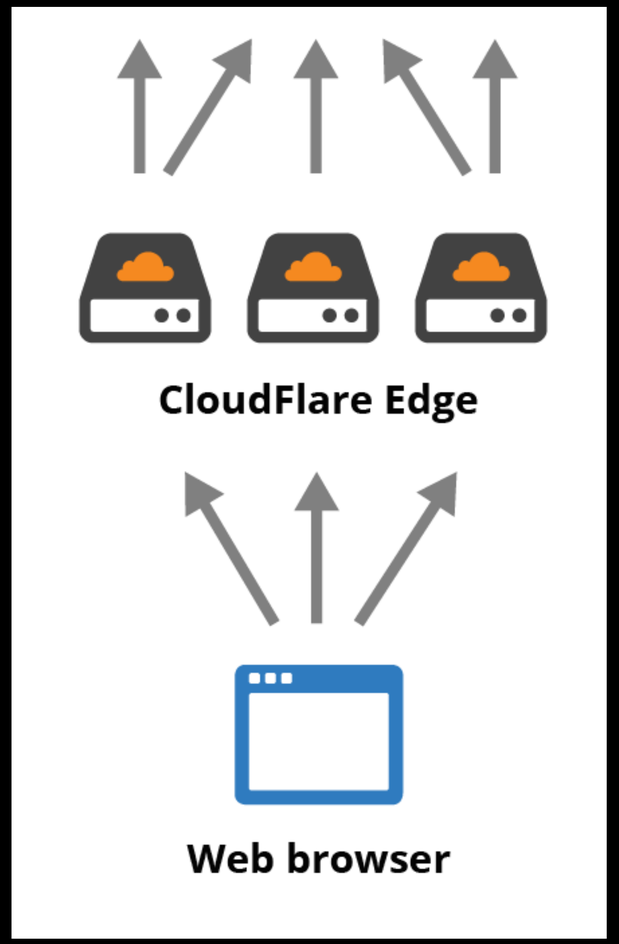
https://blog.cloudflare.com/tag/go/

CLOUDFLARE

NGINX + LuaJIT

- Every request executes Lua code… lots
- LuaJIT is very fast
- Mixture of human-written Lua and generated code

- http://wiki.nginx.org/HttpLuaModule



CLOUDFLARE

Lua for WAF

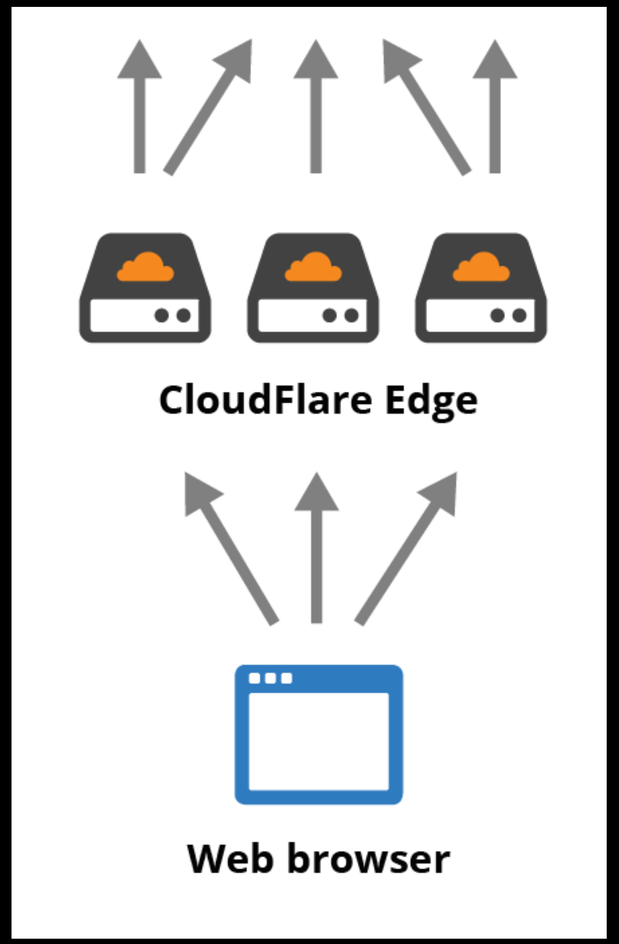
```
location / {
    set $backend_waf        "WAF_CORE";
    default_type            'text/plain';

    access_by_lua '
        local waf = require "waf"
        waf.execute("")
    ';

    log_by_lua_file "lua/metrics/waf_metrics_main.lua";

    content_by_lua 'ngx.say("")';
    error_page 500 =200 @error;
}
```

Generated Code

```
local waf_vars = waf.vars
local waf_streq = waf.streq
local waf_setvar = waf.setvar
local waf_msg = waf.msg
local waf_drop = waf.drop
local waf_disabled_ids = waf.disabled_ids
local waf_deny = waf.deny
local waf_activate = waf.activate
local t1_1 = {}
if not waf_disabled_ids['00001'] and waf_streq(waf, v2_5, '2_5', t1_1, '1_1', 'b783efc191a7c066c1d87068f63a84a39f9830bb', false) then
  waf_vars['RULE']['ID'] = '00001'
  waf_activate(waf, rulefile)
  waf_msg(waf, 'CloudFlare Test Rule (drop) activated')
  waf_setvar(waf, {{'TX:ANOMALY_SCORE', '+100'},{'TX:%{RULE:ID}', 'CloudFlare unique hash test rule (drop)'}})
  waf_drop(waf, rulefile)
end
if not waf_disabled_ids['00002'] and waf_streq(waf, v2_5, '2_5', t1_1, '1_1', '4709edce126971876b547523778fa7b942ec14b5', false) then
  waf_vars['RULE']['ID'] = '00002'
  waf_activate(waf, rulefile)
  waf_msg(waf, 'CloudFlare Test Rule (deny) activated')
  waf_setvar(waf, {{'TX:ANOMALY_SCORE', '+100'},{'TX:%{RULE:ID}', 'CloudFlare unique hash test rule (deny)'}})
  waf_deny(waf, rulefile)
end
```

NGINX + LuaJIT

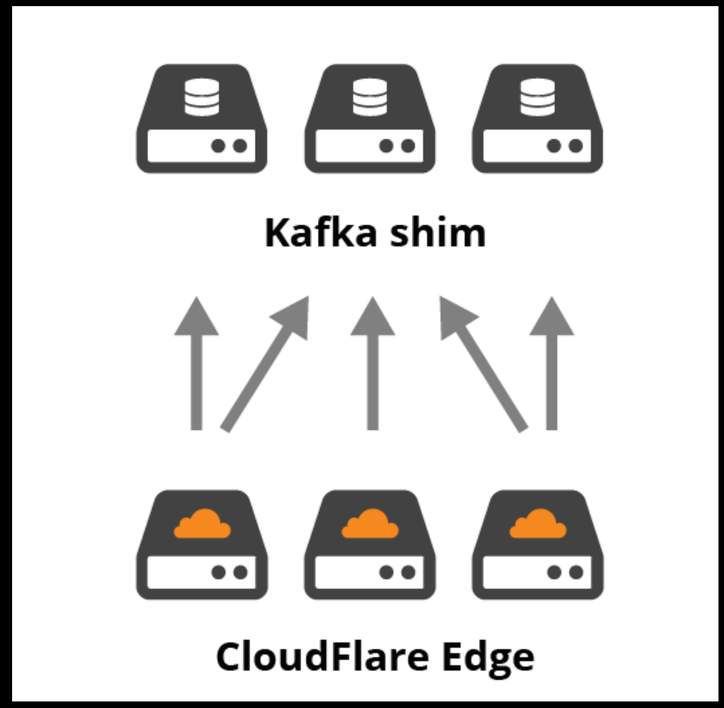
- Go program receives log events from NGINX in Cap'n Proto format
- Batches events
- Compresses using LZ4
- Sends via TLS to Data



CLOUDFLARE

Cap'n Proto

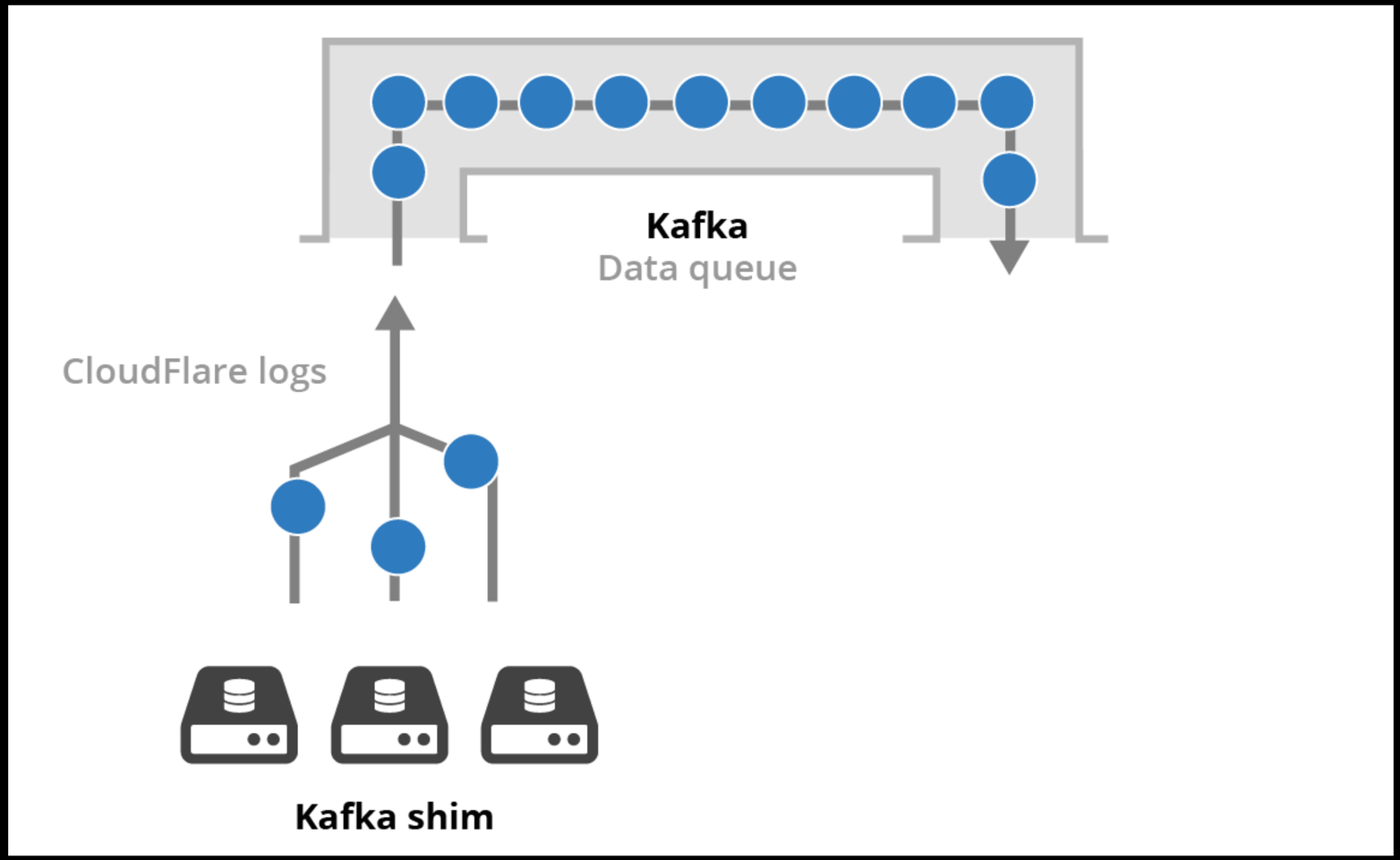
- Insanely fast
  - Saw 20x speedup over cjson
- It's a wire format and an in memory representation
- Extend with no penalty
- https://capnproto.org/
- Our interface from Lua https://blog.cloudflare.com/introducing-lua-capnproto-better-serialization-in-lua/



CLOUDFLARE

Apache Kafka

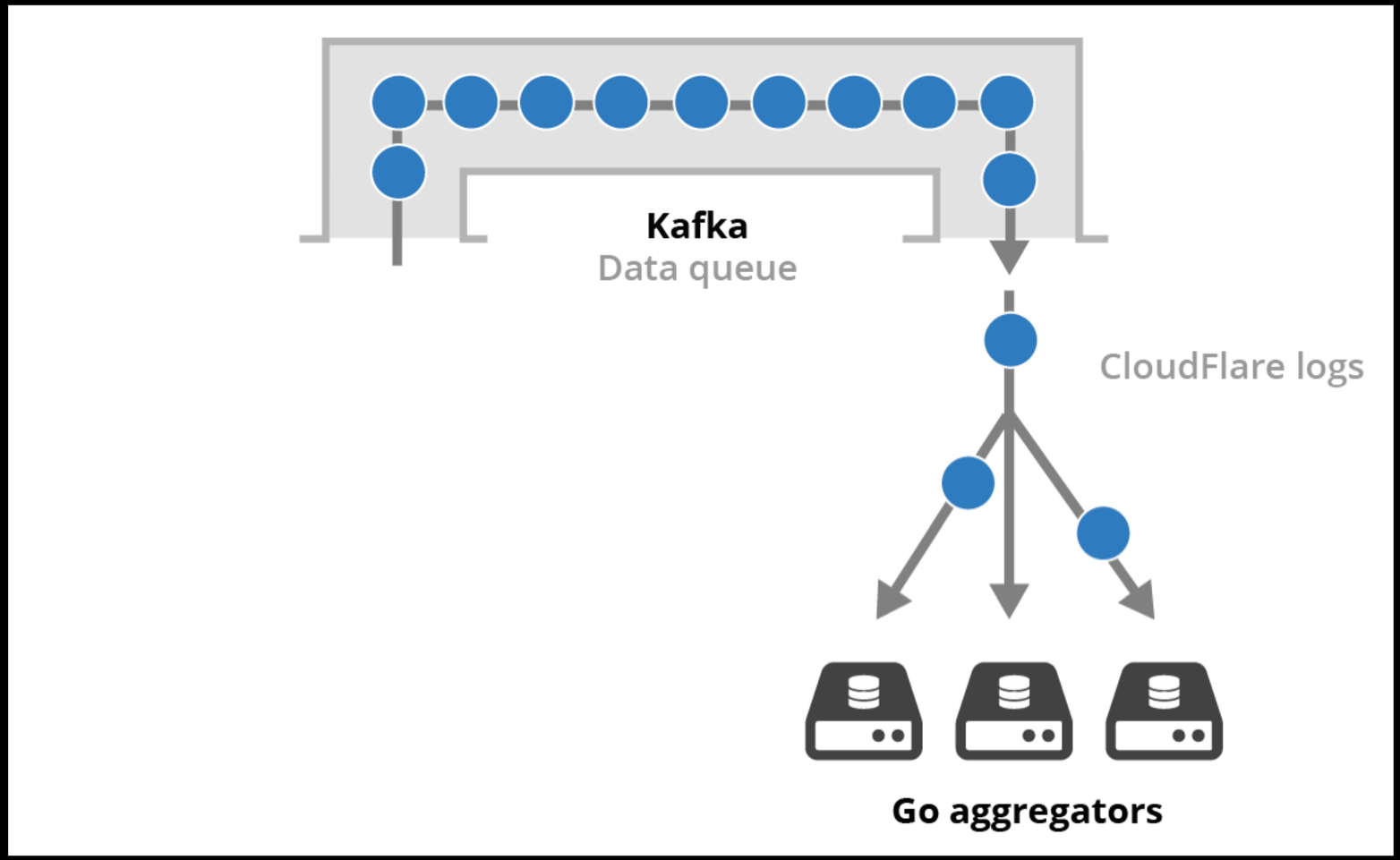
- Fast, scalable, resilient queue
- Queue on a cluster not a single machine
- Allows clusters of readers to process queue messages
- https://kafka.apache.org/



CLOUDFLARE

Apache Kafka

- Cluster of Go programs process log messages
- Generate detailed attack logs for customers
- Feed aggregates to Postgres

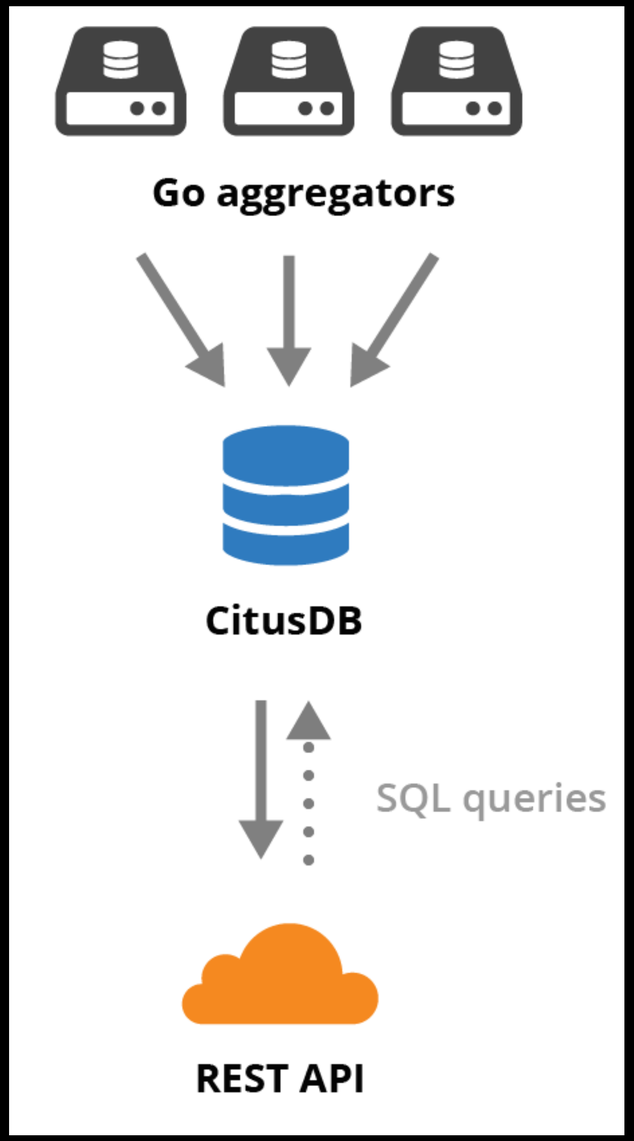


CLOUDFLARE

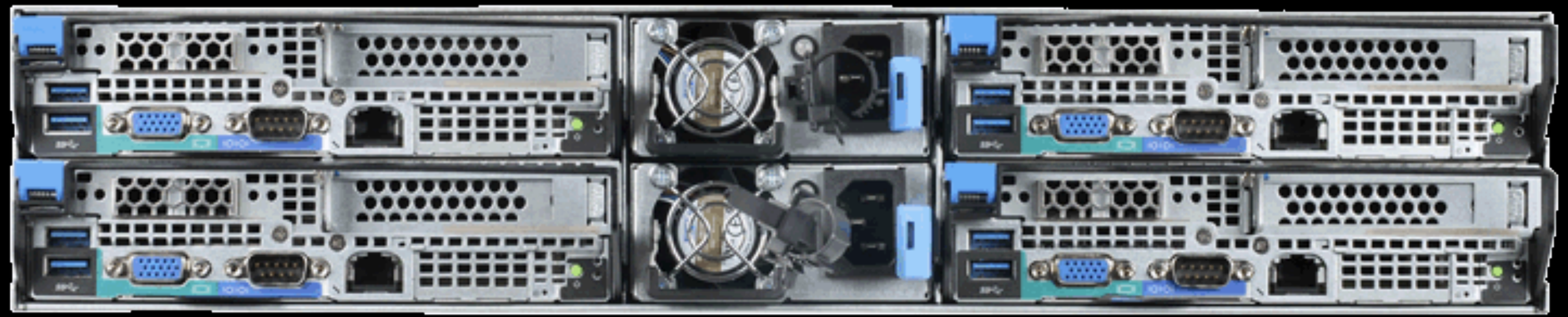
```
{
  "_index": "waf-2015.06.08",
  "_type": "waf",
  "_id": "1[redacted]9",
  "_score": null,
  "_source": {
    "type": "waf",
    "rayid": "1[redacted]9",
    "zone_id": [redacted],
    "timestamp": "2015-06-08T07:14:20.94Z",
    "client_ip": "1[redacted]6",
    "host": "jgc.org",
    "http_method": "GET",
    "protocol": "HTTP/1.1",
    "uri": "/?try_to_be_bad=%3Cscript%3Ealert(%22pwned!%22);%3C/script%3E",
    "country": "us",
    "action": "challenge allow",
    "rule_id": "100030",
    "colo": 4,
    "edge_dur": 3000064,
    "user_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/43.0.2357.81 Safari/53
7.36",
    "rule_group": "cloudflare_specials",
    "activated_rules": [
      "100030"
    ],
    "exit_code": 403
  },
  "sort": [
    1433747660940,
    1433747660940
  ]
}
```


Postgres and CitusDB

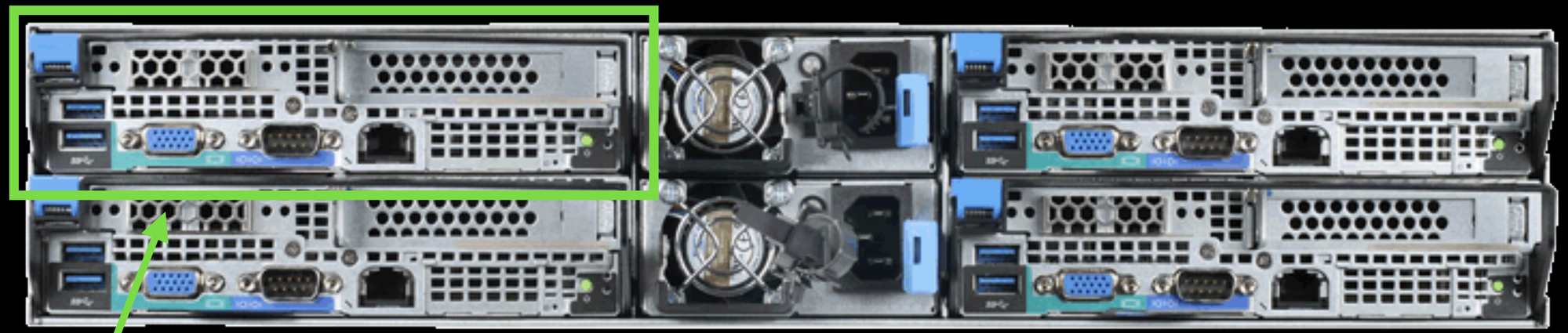
- Go processes produce 1 minute roll ups of customer analytics an insert into CitusDB
- Later 1 hour, 1 day etc. roll ups created
- CitusDB is a sharded, replicated Postgres implementation for very fast queries
- https://blog.cloudflare.com/scaling-out-postgresql-for-cloudflare-analytics-using-citusdb/
- https://www.citusdata.com/



CLOUDFLARE

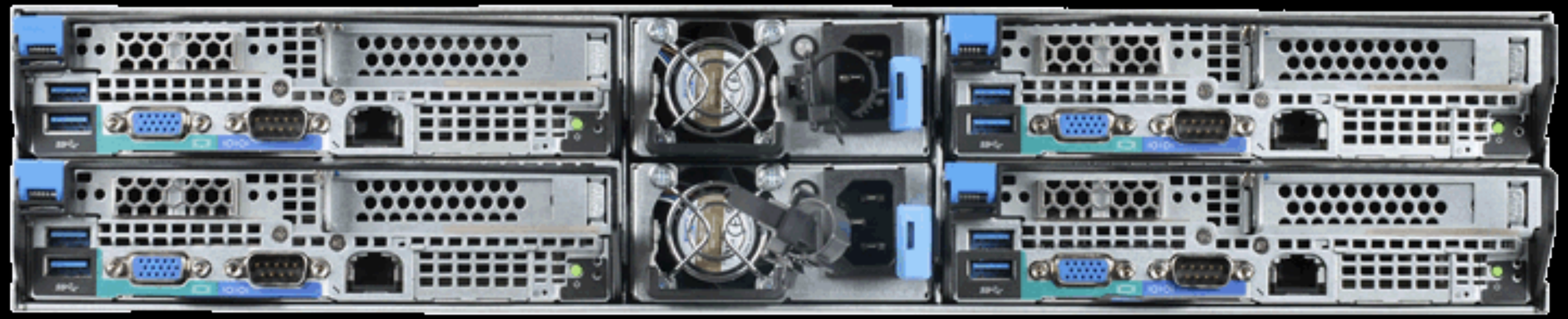


CLOUDFLARE



- 128GB RAM
  2x Intel® Xeon® Processor E5-2630 v3 (16 cores)
  10G Ethernet
  Disks vary
- Custom made for us by Quanta

CLOUDFLARE



- 40 machines for Kafka
  400TB of compressed, replicated 500-byte log lines
  Ingest at ~15Gbps
  ~50TB of spinning rust per node
- 5 machines for CitusDB
  Analytics for 2 million customers
  ~12TB of SSD per node
- > 100 machines for consumers written in Go
  The analytics roll up processes
  Attack detection
  Botnet analysis

CLOUDFLARE

Streaming Algorithms

- Space Saving Algorithm
  Efficient Computation of Frequent and Top-k Elements in Data Streams
  https://icmi.cs.ucsb.edu/research/tech_reports/reports/2005-23.pdf

  Hasn't worked well for 'long tail data'

- HyperLogLog
  Counting distinct elements
  https://github.com/aggregateknowledge/postgresql-hll

CLOUDFLARE

CLOUDFLARE

CloudFlare Open Source.

JavaScript Go Nginx and Lua Postgres Other

Recently updated View all on github »

cfssl · Sat Jun 06 2015 · 571 stargazers · 50 forks
cf-tls · Sat Jun 06 2015 · 6 stargazers · 2 forks
collapsify · Mon Jun 01 2015 · 15 stargazers · 3 forks

Learn More

CloudFlare
Careers
Blog

https://cloudflare.github.io/

CLOUDFLARE