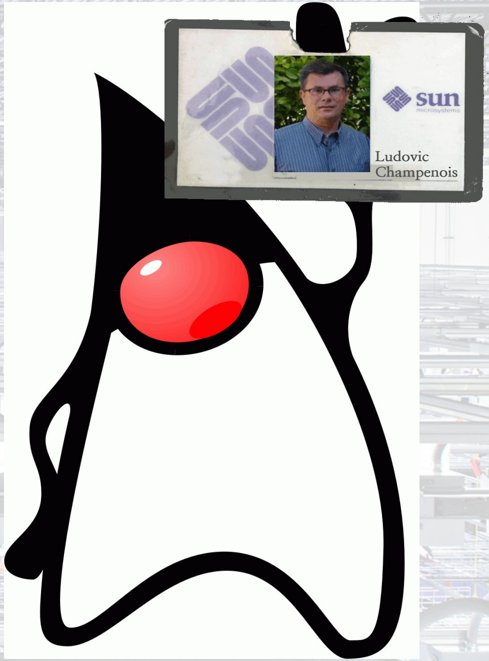
Jfokus 2019

Evolution of a Platform as a Service from the inside



Ludovic Champenois, TL Java runtimes
@ludoch
Google San Francisco

Google Cloud

Agenda

Act 1, 2008 : The Genesis

Act 2, 2009 : Java, Restricted

Act 3, 2017 : The Next Generation

Act 4, 2019 : Java 11, Unrestricted

Act 1, 2008

The Genesis

Act 1: Public Announcement

guido@ Nov 2008: *“Unlike other cloud offerings, App Engine does not offer you a virtual machine, but a scalable container in which your application runs...”*

Original Slides at
http://web.stanford.edu/class/ee380/Abstracts/081105-slides.pdf

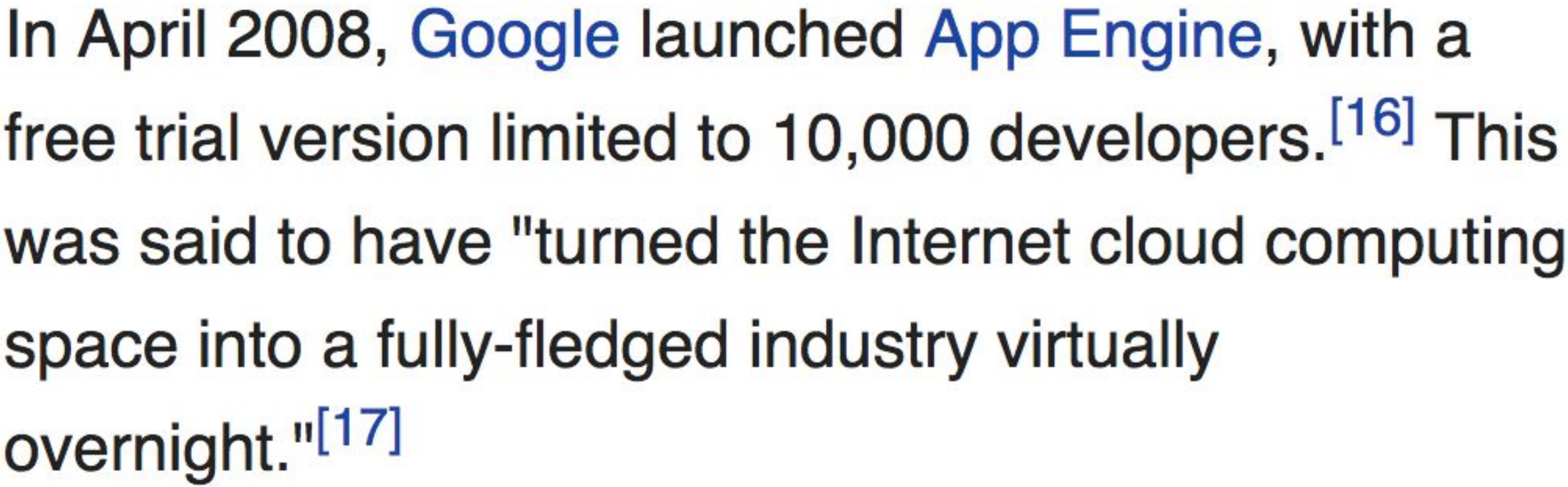
Source: https://en.wikipedia.org/wiki/Platform_as_a_service

Act 1: Public Announcement

11 years ago...

07. Launch Day April 2008 Google Campfire One.

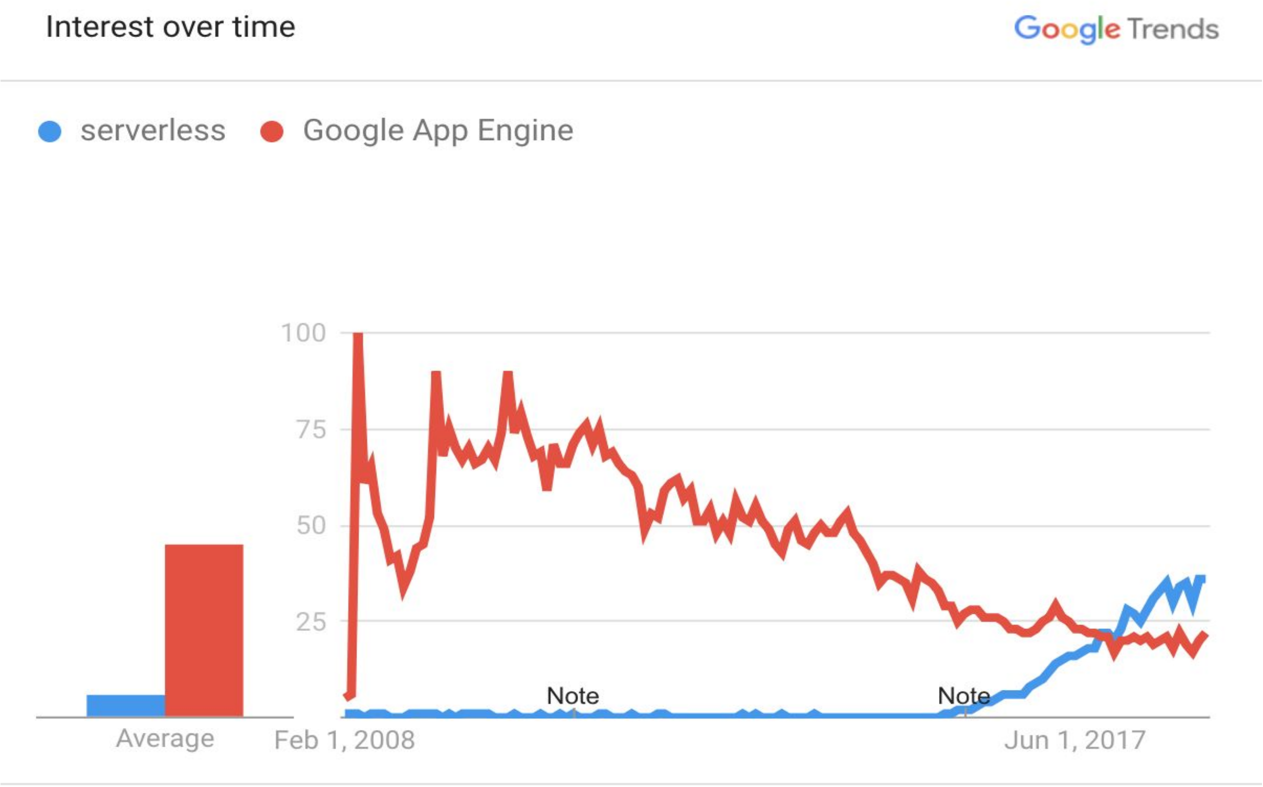
Act 1: Public Announcement

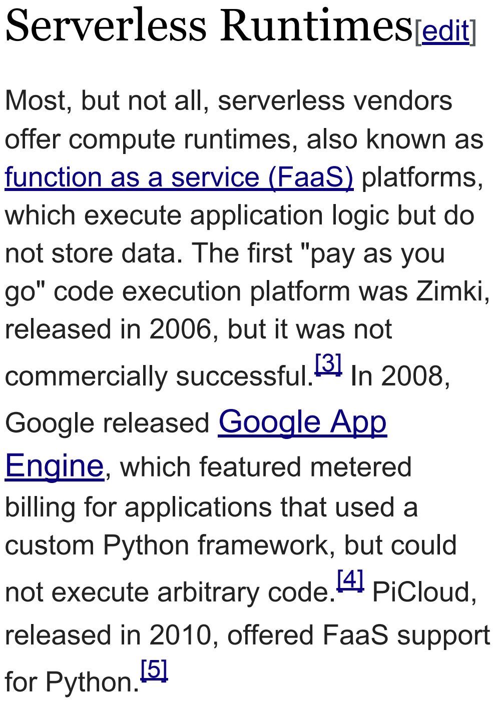


In April 2008, Google launched App Engine, with a free trial version limited to 10,000 developers.[16] This was said to have "turned the Internet cloud computing space into a fully-fledged industry virtually overnight."[17]

Source: https://en.wikipedia.org/wiki/Platform_as_a_service

Act 1: Serverless Before Serverless Was a Thing





Serverless Runtimes[edit]

Most, but not all, serverless vendors offer compute runtimes, also known as function as a service (FaaS) platforms, which execute application logic but do not store data. The first "pay as you go" code execution platform was Zimki, released in 2006, but it was not commercially successful.[3] In 2008, Google released Google App Engine, which featured metered billing for applications that used a custom Python framework, but could not execute arbitrary code.[4] PiCloud, released in 2010, offered FaaS support for Python.[5]

https://en.wikipedia.org/wiki/Serverless_computing

How Successful?

App Engine

Now serving

>300 Billion

requests per day

Wikipedia serves per day and it’s “only” 300+ million per day...

Act 1: With Sandboxing Restrictions

guido@ circa 2008: *“Unlike other cloud offerings, App Engine does not offer you a virtual machine, but a scalable container in which your application runs…”* **securely**…

Advantages

- Sandboxing a process, not an OS
- No network programming involved
- Low configuration overhead for instances
- Low memory overhead per instance

Which lead to…

- Fast startup times => 0/1/0 scaling
- High instance creation rates (xxK/sec)
- Extreme multi-tenancy (xxM daily active)
- Low memory pressure (infrequent eviction => fewer cold starts)

Drawbacks

- Security requirements imposing restrictions.
- Non-standard request and API protocol
- No standard application packaging format, no runtime definition or contract.

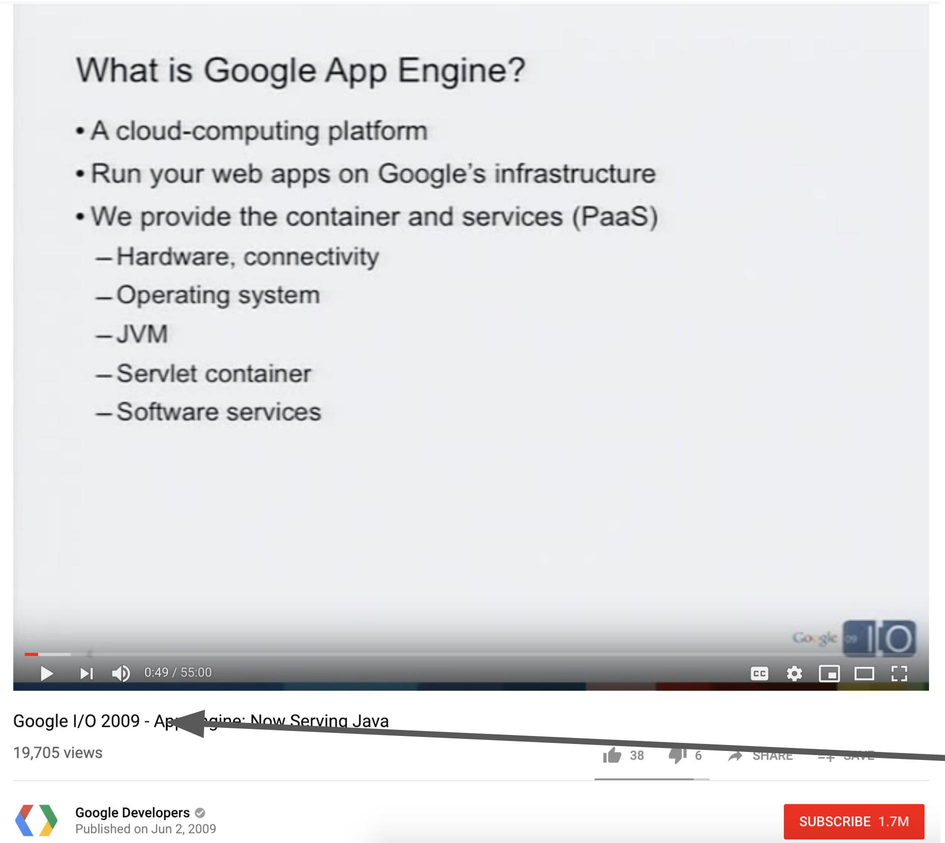
Which lead to…

- Stagnation: Java 7 to Java 8 lag…

Act 2, 2009

Java, restricted

Act 2: Announcing App Engine Java



What is Google App Engine?

- A cloud-computing platform
- Run your web apps on Google's infrastructure
- We provide the container and services (PaaS)
  - Hardware, connectivity
  - Operating system
  - JVM
  - Servlet container
  - Software services

Google I/O 2009 - App Engine: Now Serving Java

19,705 views

Google Developers

Published on Jun 2, 2009

Cloud Computing

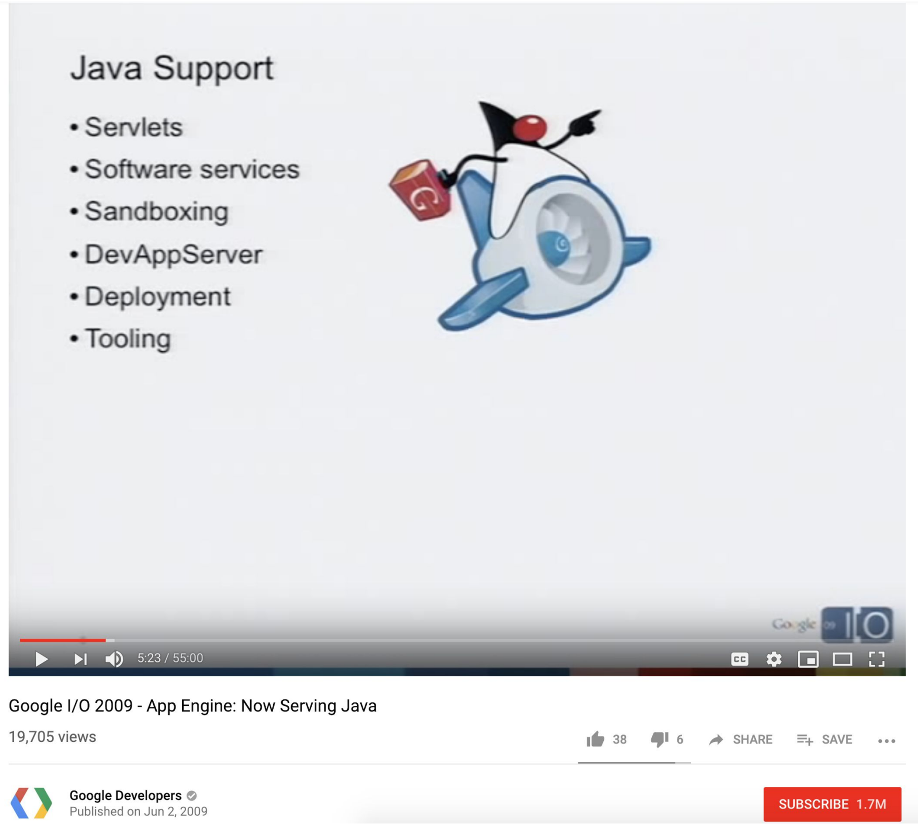
Infrastructure

Container

In 2009...

Source: https://www.youtube.com/watch?v=ofn8QYEVyhA

Act 2: Java Sandboxing



Java Support

- Servlets
- Software services
- Sandboxing
- DevAppServer
- Deployment
- Tooling

Google I/O 2009 - App Engine: Now Serving Java

19,705 views

Google Developers

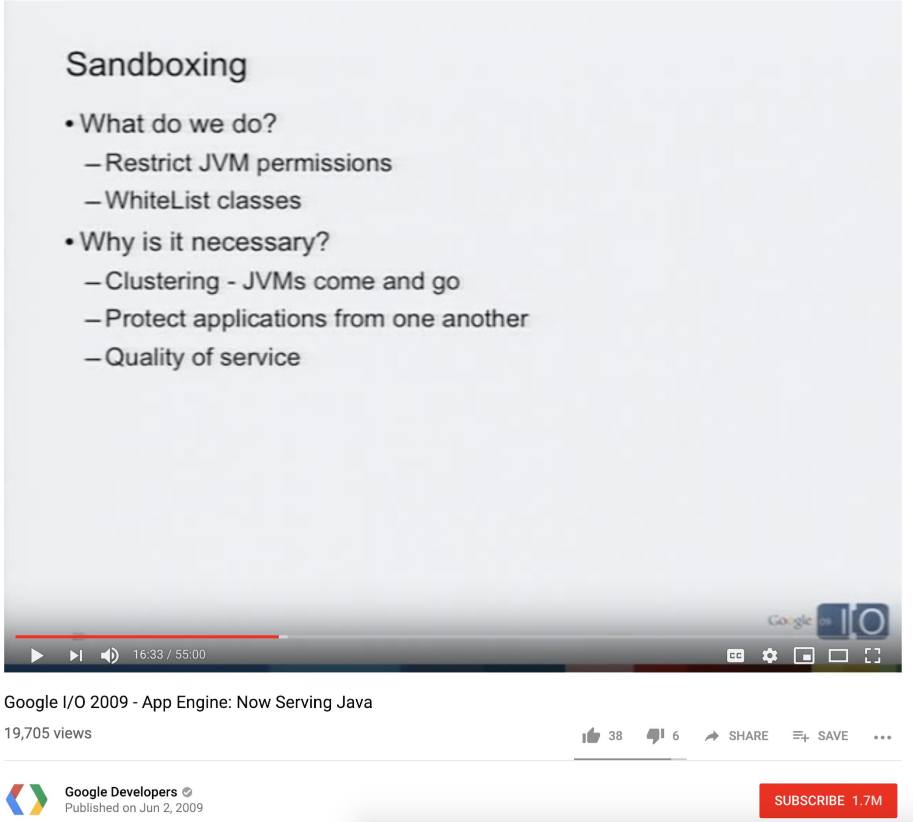
Published on Jun 2, 2009

Sandboxing
(in Java 6, 7)

07. Java Sandboxing in 2009

Source: https://www.youtube.com/watch?v=ofn8QYEVyhA

Act 2: Java Sandboxing Restrictions



Sandboxing

- What do we do?
  - Restrict JVM permissions
  - WhiteList classes
- Why is it necessary?
  - Clustering - JVMs come and go
  - Protect applications from one another
  - Quality of service

Google I/O 2009 - App Engine: Now Serving Java

19,705 views

Google Developers

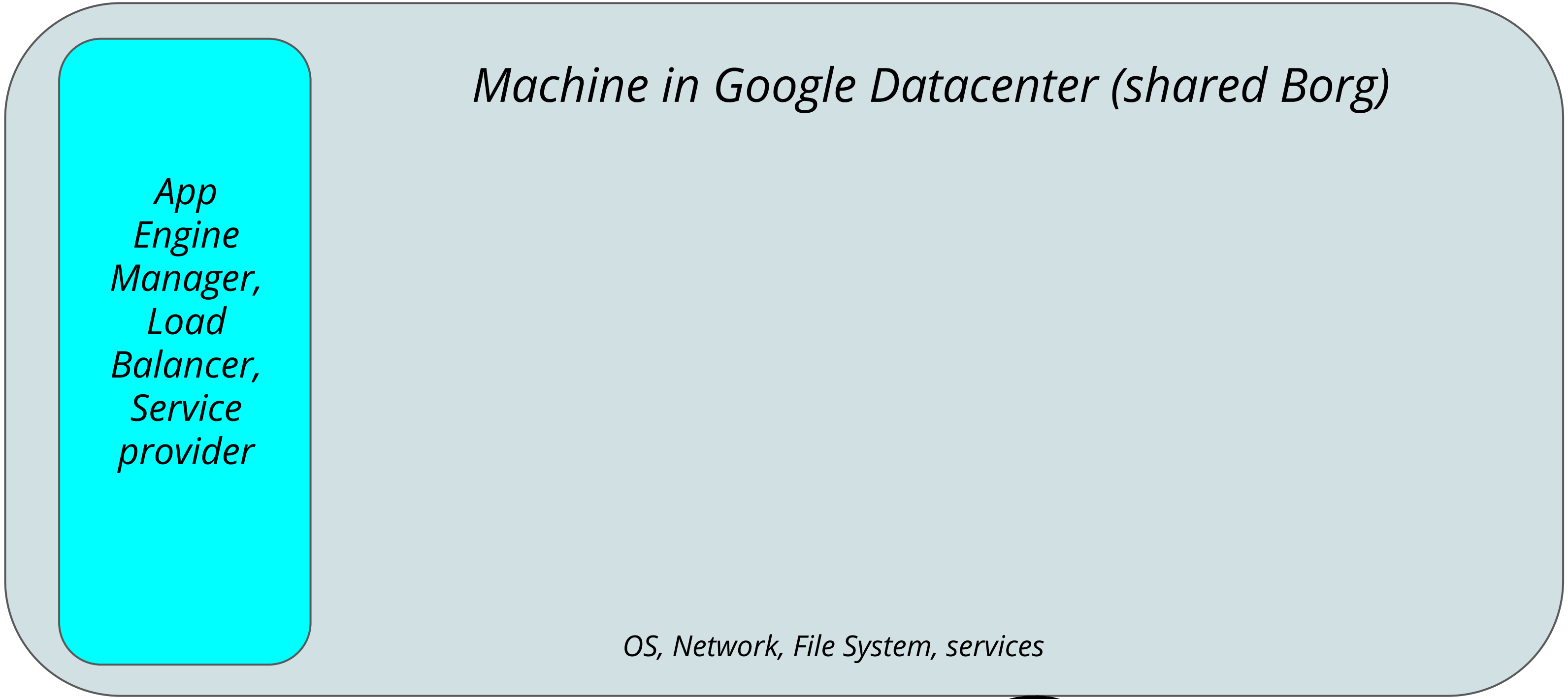
Published on Jun 2, 2009

Sandboxing (in Java 6, 7)

07. Java Sandboxing in 2009

Source: https://www.youtube.com/watch?v=ofn8QYEVyhA

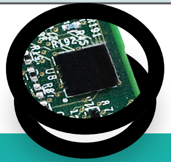
App Engine Security Sandbox



Machine in Google Datacenter (shared Borg)

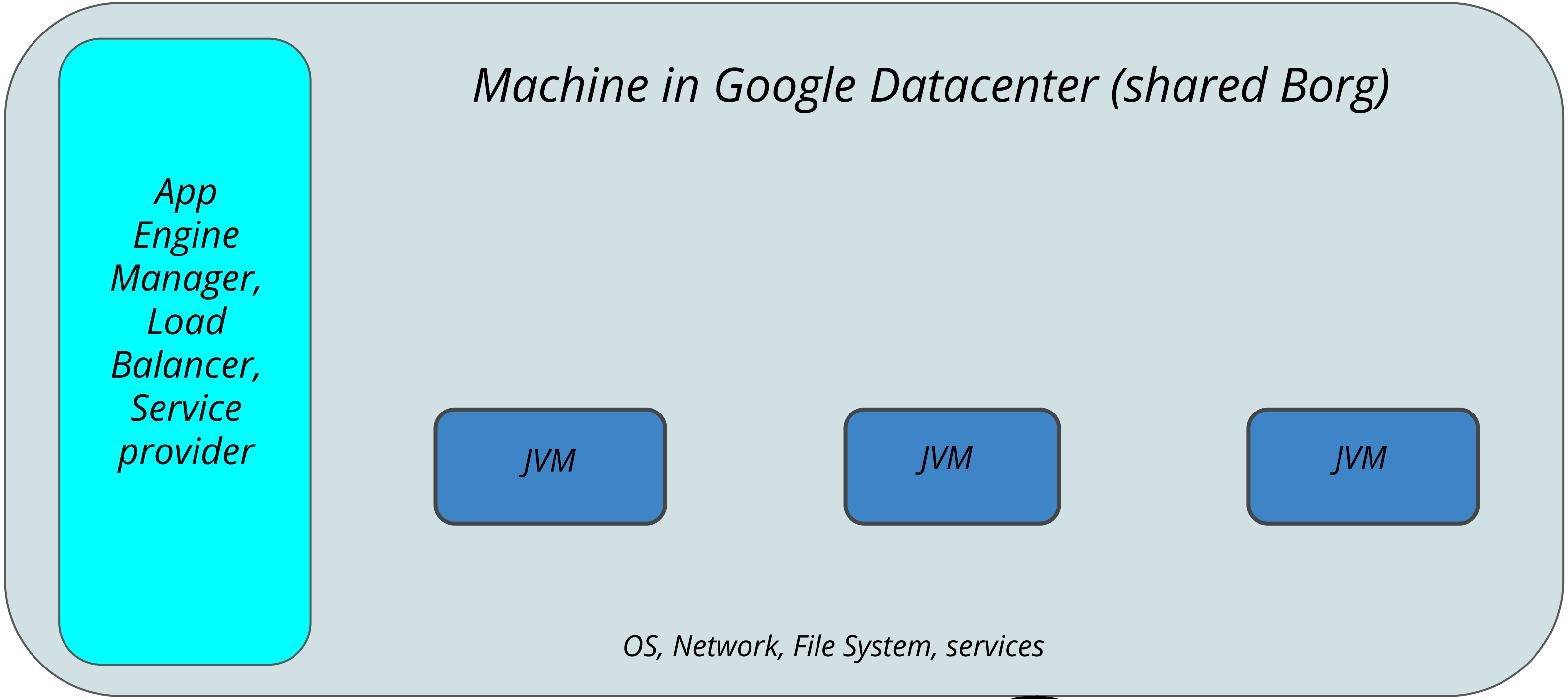
App Engine Manager, Load Balancer, Service provider

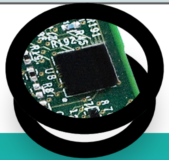
OS, Network, File System, services



Google's purpose-built chip to establish **hardware root of trust**

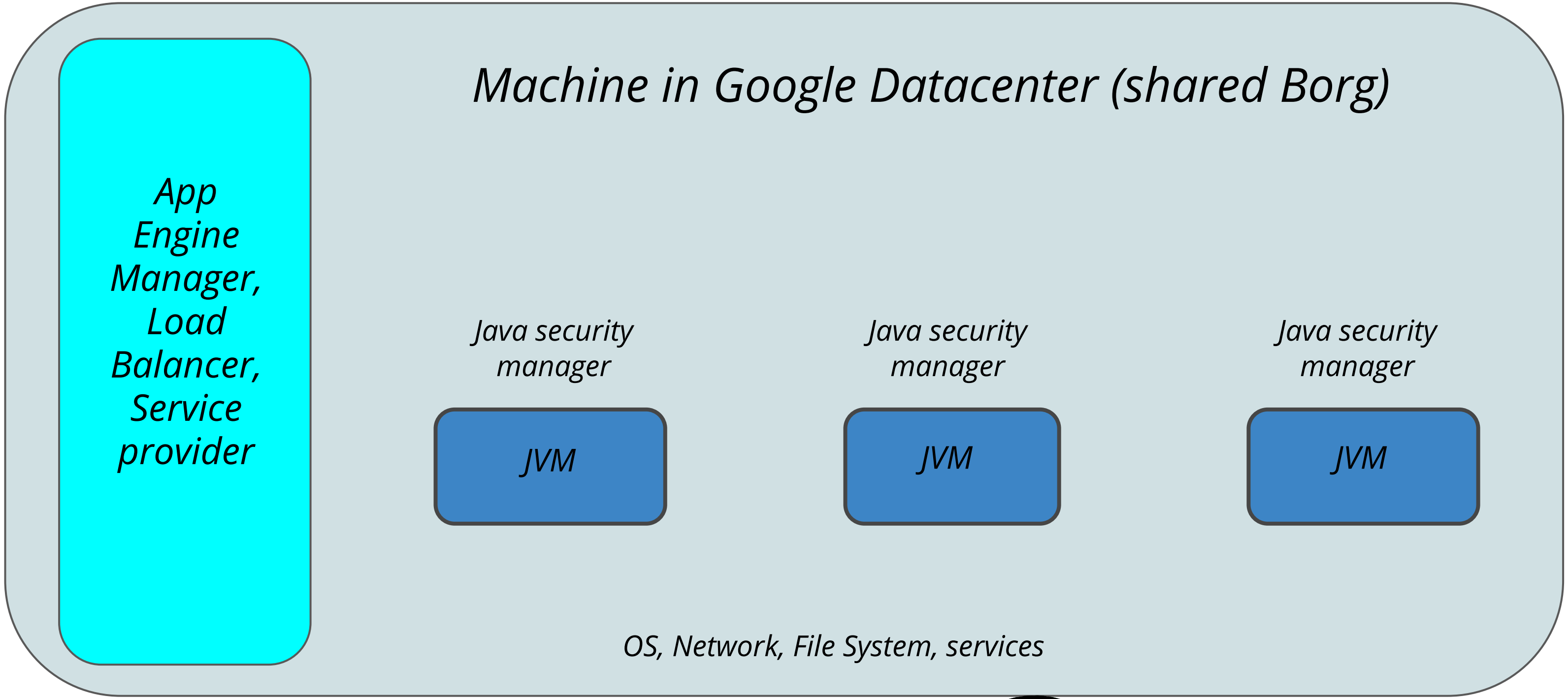
App Engine Security Sandbox


Machine in Google Datacenter (shared Borg)
App Engine Manager, Load Balancer, Service provider
JVM
JVM
JVM
OS, Network, File System, services



Google's purpose-built chip to establish **hardware root of trust**

App Engine Security Sandbox



Machine in Google Datacenter (shared Borg)

App Engine Manager, Load Balancer, Service provider

Java security manager

JVM

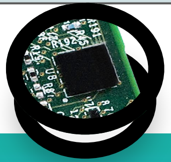
Java security manager

JVM

Java security manager

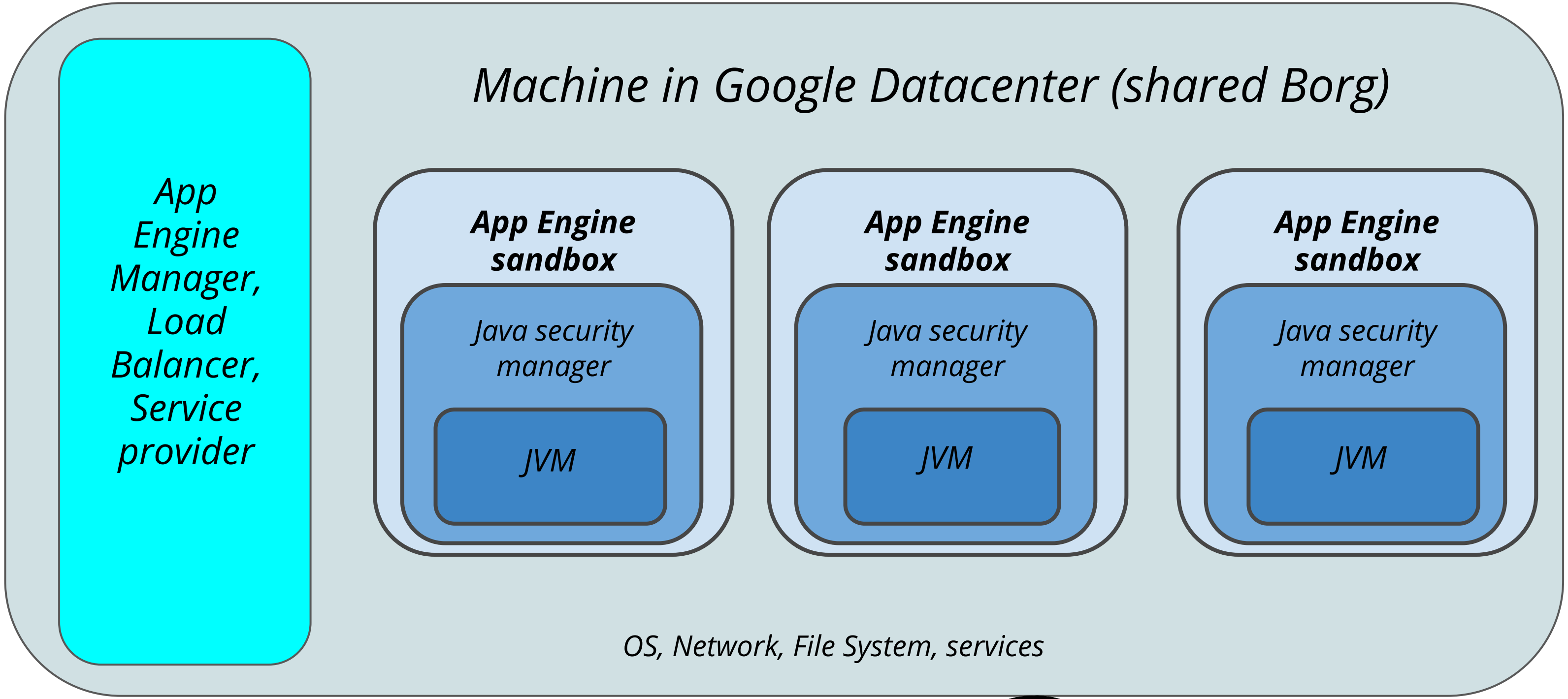
JVM

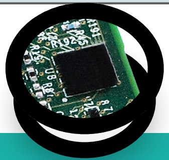
OS, Network, File System, services



Google's purpose-built chip to establish **hardware root of trust**

App Engine Security Sandbox


Machine in Google Datacenter (shared Borg)
App Engine Manager, Load Balancer, Service provider
App Engine sandbox
Java security manager
JVM
App Engine sandbox
Java security manager
JVM
App Engine sandbox
Java security manager
JVM
OS, Network, File System, services



Google's purpose-built chip to establish **hardware root of trust**

Act 2: The Original App Engine Security Sandbox

- Google Security mandates more than 1 security layer
  - For Java 6, Java 7:
    - Java Security Manager, Java Permissions
    - Class whitelist, no native code, limited threads,...
    - User Code introspection to detect vectors of attacks
    - pTrace
- Java 8 exposed more ways to be attacked...

- We could not use anymore this type of andboxing with Java 8...

Act 2: App Engine Security Attacks: (Public Ones)

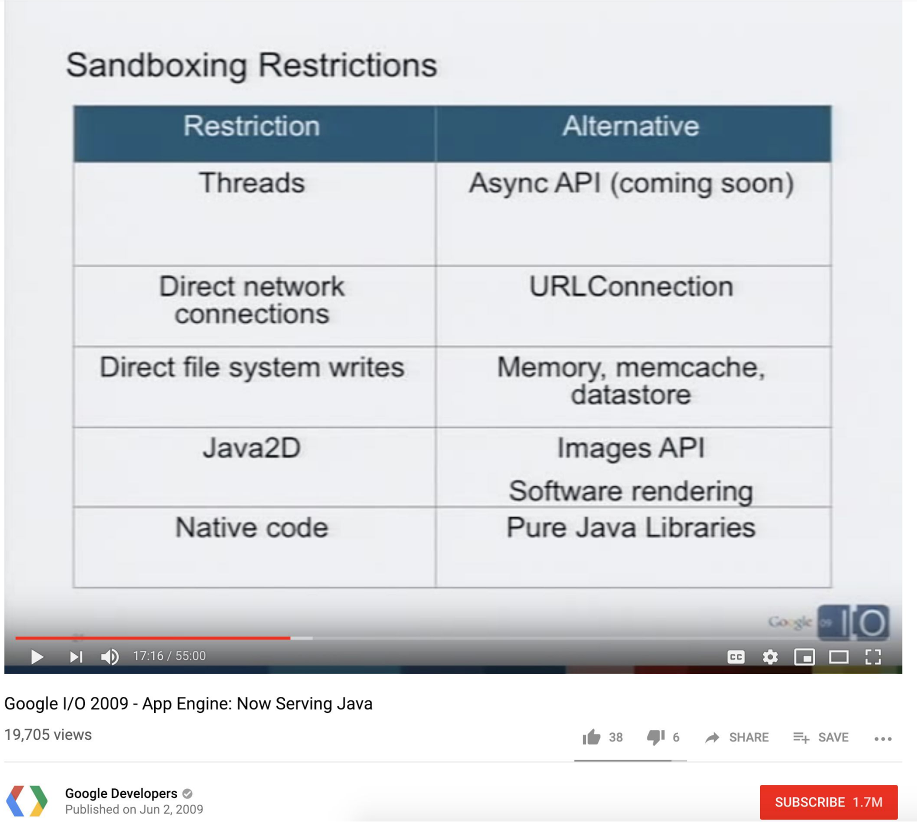
https://www.computerworld.com/article/2857007/more-than-30-vulnerabilities-found-in-google-app-engine.html Dec 2014

http://www.zdnet.com/article/details-of-unpatched-vulnerabilities-in-google-app-engine-revealed/ May 2015

http://www.zdnet.com/article/google-awards-student-10k-for-discovery-of-app-engine-flaw August 2017

https://security.googleblog.com/2018/01/todays-cpu-vulnerability-what-you-need.html 2018 (Google Project Zero, Intel CPUs)

Act 2: Initial Java 6,7 Sandboxing Restrictions



Sandboxing Restrictions

Restriction	Alternative
Threads	Async API (coming soon)
Direct network connections	URLConnection
Direct file system writes	Memory, memcache, datastore
Java2D	Images API Software rendering
Native code	Pure Java Libraries

Google I/O 2009 - App Engine: Now Serving Java

19,705 views

Google Developers
Published on Jun 2, 2009

2017 Java8:
All limitations **gone**
with the
new Sandboxing

07. Sandboxing Restrictions in 2009

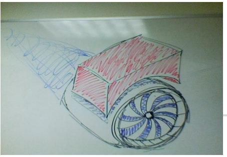
Source: https://www.youtube.com/watch?v=ofn8QYEVyhA

Act 3, 2017

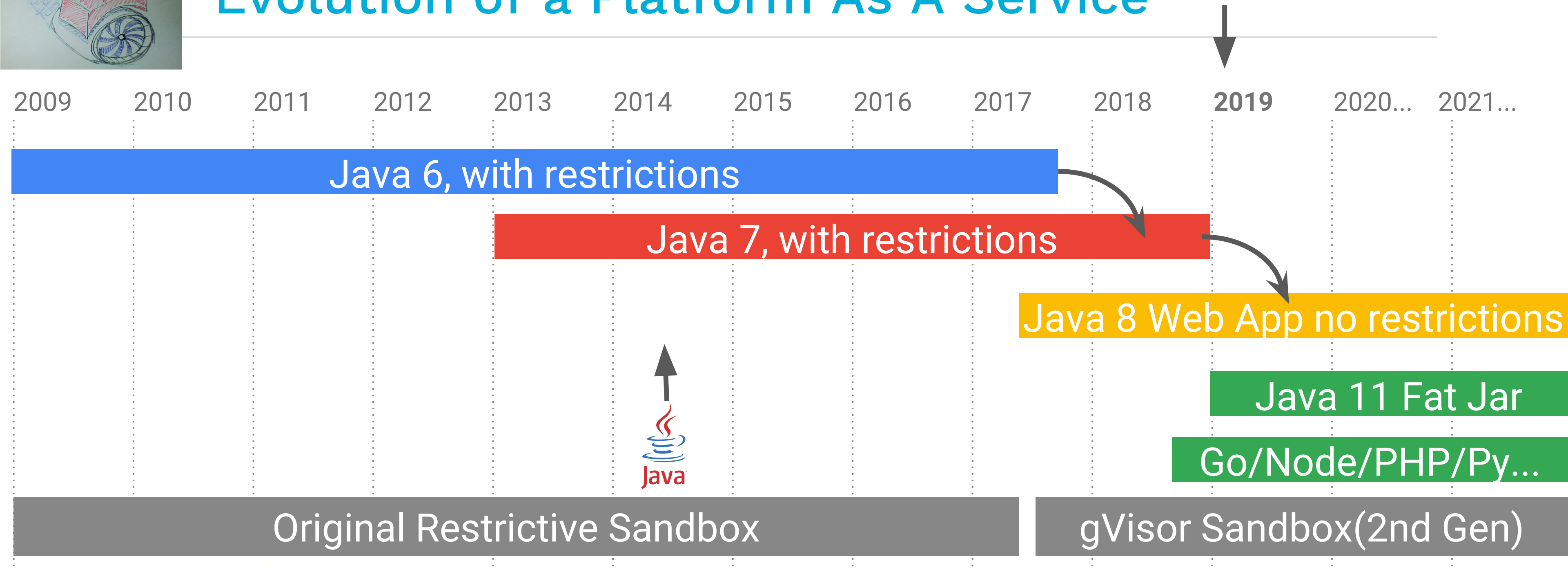
The Next Generation

Act 3: The Next Generation

Enter: gVisor (2017)



Evolution of a Platform As A Service



2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 **2019** 2020... 2021...

Java 6, with restrictions

Java 7, with restrictions

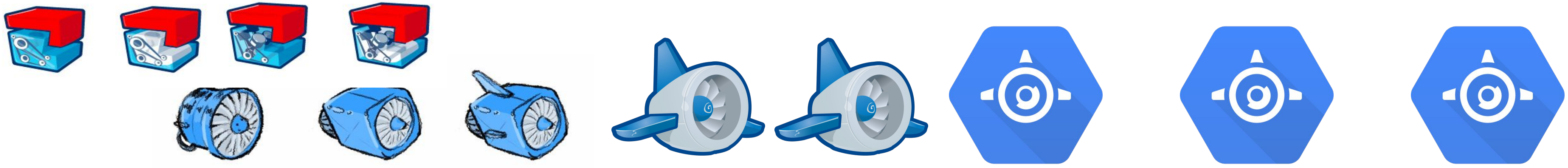
Java 8 Web App no restrictions

Java 11 Fat Jar

Go/Node/PHP/Py...

Original Restrictive Sandbox

gVisor Sandbox(2nd Gen)



Quiz: Which logo do you prefer?

https://cloudplatform.googleblog.com/2013/12/an-ode-to-sharkon.html

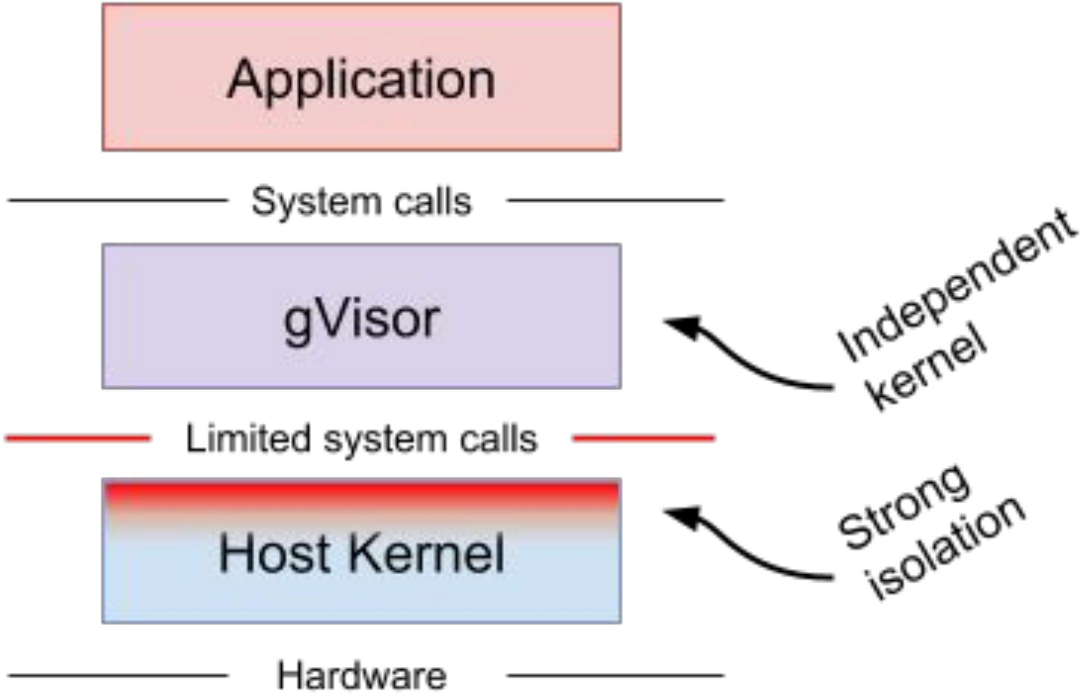
Act 3: The Next Generation

gVisor is a user-space kernel, written in Go, that implements a substantial portion of the Linux system surface.

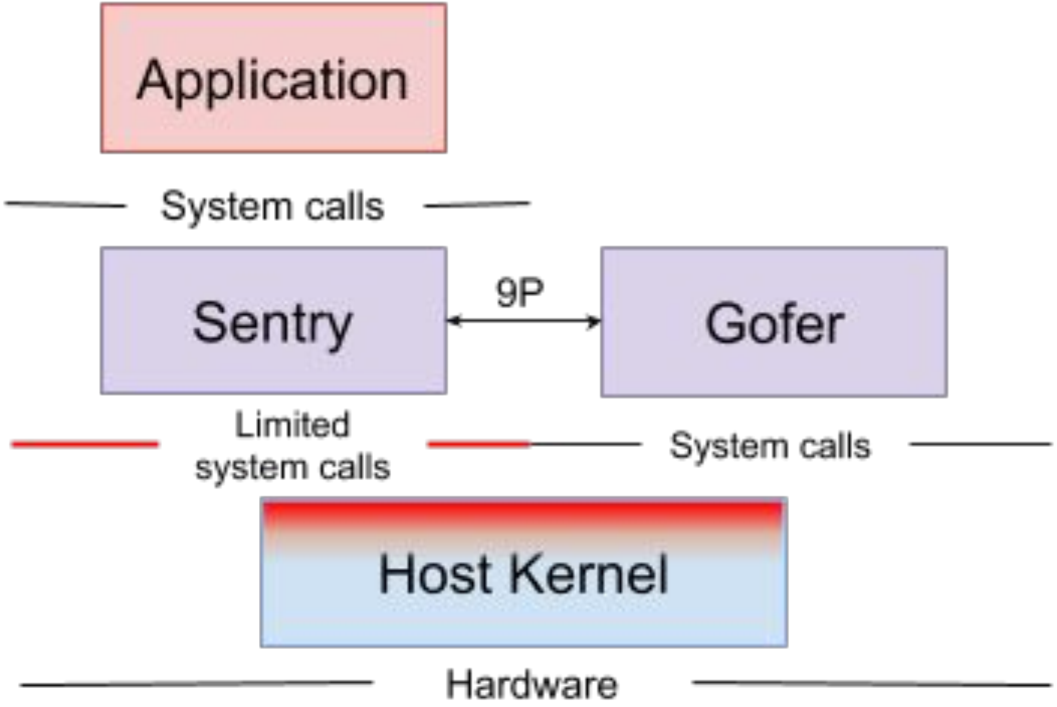
gVisor intercepts application system calls and acts as the guest kernel.

github.com/google/gvisor

Act 3: The Next Generation



Act 3: The Next Generation



Act 3: The Next Generation

- A virtualization based sandbox.
- Providing strong isolation and security guarantees by adopting an application OS approach.
- It's **not** a virtual machine.
- It allows most Linux syscalls (250+ and growing).
- It's lightweight and fast.
- It doesn't require **any** changes to the Java JVM/Libraries.

  - gVisor can now run in Docker as well (runsc)...

Act 3: Java 8 First gVisor Based Runtime

- Launched **GA** Sept 26th 2017
- Very Strict backward compatibility for Millions of Apps
- **Without** the previous limitations
- Allowing **both** the Standard GAE APIs and the Cloud APIs
- Already serving **Millions** of Queries Per Second (QPS)
- Open JDK 8 and Jetty 9 (Servlet 3.1 based)

Act 4, 2019

Java 11 Unrestricted

Act 4: Java 11 Unrestricted

- Send us a fat jar, a collection of jars, including a Web Server
- Listen to port 8080
- Optionally the entrypoint command
- Use Google Cloud APIs
- Seamlessly shift from App Engine to Kubernetes or VMs (even with a competitor) as needed

Act 4: Java 11: Simple Configuration File

app.yaml:

```
  runtime : java11
  entrypoint : java -jar myjar.jar
  // Optional
  instance_class: F4 // Optional
  // Scalability settings Optional
```

Java11 A single line configuration file

Act 4: App Engine Containers with gVisor

You give us your jar(s) once...

- We maintain a Ubuntu 18.0.4 base image (LTS)

- We maintain an Open JDK 11 (LTS)

- Your App deployed in 2019 (now) will inherit automatic updates from the base layers

- If you are aware of another platform doing this, let me know...

Deploy once, stay up to date without doing anything

Act 4: Java 11 The Next Generation

Try it today:

goo.gl/b8N7L2 (Form to apply)

https://github.com/ludoch/samples/tree/master/java11

10. Java11 Alpha get it from goo.gl/b8N7L2

Act 5, 2019

Java 11 Demos

Act 5: Java 11 Demos

Simple Java 11 app ever
SpringBoot
Micronaut
Spark Java
Jetty 9.4 Web Apps (embedded)
Your App?...

Java11 samples: https://github.com/ludoch/samples/tree/master/java11

Thanks!

Ludovic Champenois
Google
ludo@google.com
github.com/ludoch
twitter: @ludoch