

# Security oriented OpenShift within regulated environments

Dawid Szymański - IT Architect, BZWBK

Tomasz Cholewa - Lead Cloud Architect (RHCA), Mindbox

Jarosław Stakun - Lead Solutions Architect, Red Hat

9th May 2018

# Why?

A photograph of a two-lane asphalt road with yellow double lines, curving through a dry, sparsely vegetated desert landscape. The road leads towards a range of mountains in the background, which are composed of distinct, layered rock formations in shades of brown, tan, and reddish-brown. The sky is clear and blue.

# Road to OpenShift

Before  
Containers

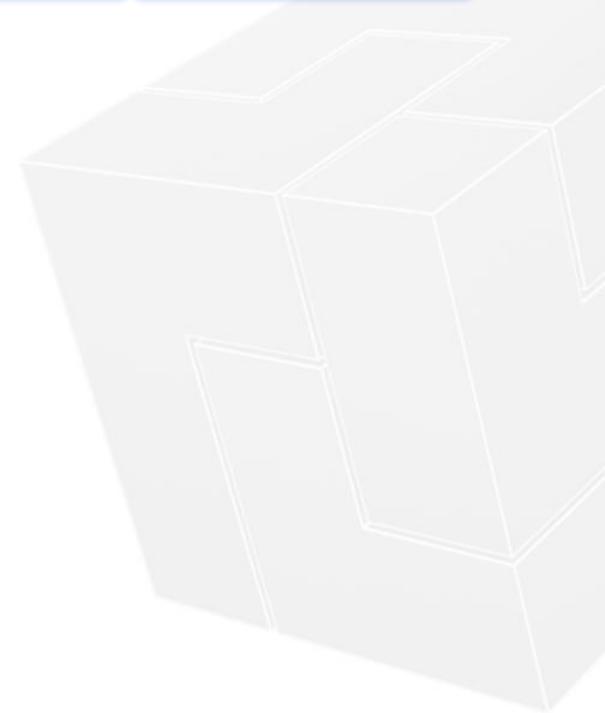
World of  
Containers

OpenShift  
Infra Design

OpenShift  
Pipeline

OpenShift  
App Devel

X86 VM



Before  
Containers

World of  
Containers

OpenShift  
Infra Design

OpenShift  
Pipeline

OpenShift  
App Devel

X86 VM

IBM LPAR

Before  
Containers

World of  
Containers

OpenShift  
Infra Design

OpenShift  
Pipeline

OpenShift  
App Devel

X86 VM

IBM LPAR

Technology  
obsolescence

Before  
Containers

World of  
Containers

OpenShift  
Infra Design

OpenShift  
Pipeline

OpenShift  
App Devel

X86 VM

IBM LPAR

Technology  
obsolescence

A lot of manual  
work

Before  
Containers

World of  
Containers

OpenShift  
Infra Design

OpenShift  
Pipeline

OpenShift  
App Devel

X86 VM

IBM LPAR

Technology  
obsolescence

A lot of manual  
work

Almost no control  
over development  
components

## Before Containers

## World of Containers

## OpenShift Infra Design

## OpenShift Pipeline

## OpenShift App Devel

X86 VM

IBM LPAR

Technology  
obsolescence

A lot of manual  
work

Almost no control  
over development  
components

A lot of different  
versions of  
platforms

## Before Containers

## World of Containers

## OpenShift Infra Design

## OpenShift Pipeline

## OpenShift App Devel

X86 VM

IBM LPAR

Technology  
obsolescence

A lot of manual  
work

Almost no control  
over development  
components

A lot of different  
versions of  
platforms

Compliance and  
security are pain in  
the ...

## Before Containers

## World of Containers

## OpenShift Infra Design

## OpenShift Pipeline

## OpenShift App Devel

X86 VM

IBM LPAR

Technology  
obsolescence

A lot of manual  
work

Almost no control  
over development  
components

A lot of different  
versions of  
platforms

Compliance and  
security are pain in  
the ...

Changes are  
required in many  
places

Before  
Containers

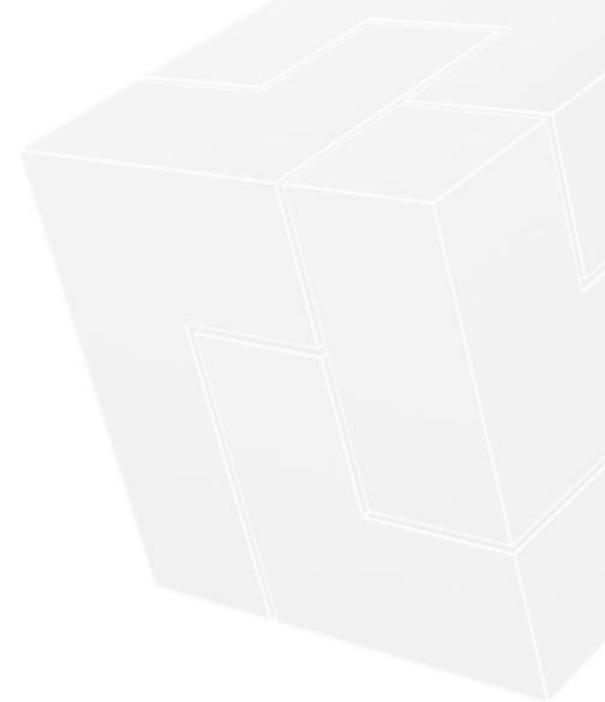
World of  
Containers

OpenShift  
Infra Design

OpenShift  
Pipeline

OpenShift  
App Devel

Docker Swarm  
Architecture PoC



Before  
Containers

World of  
Containers

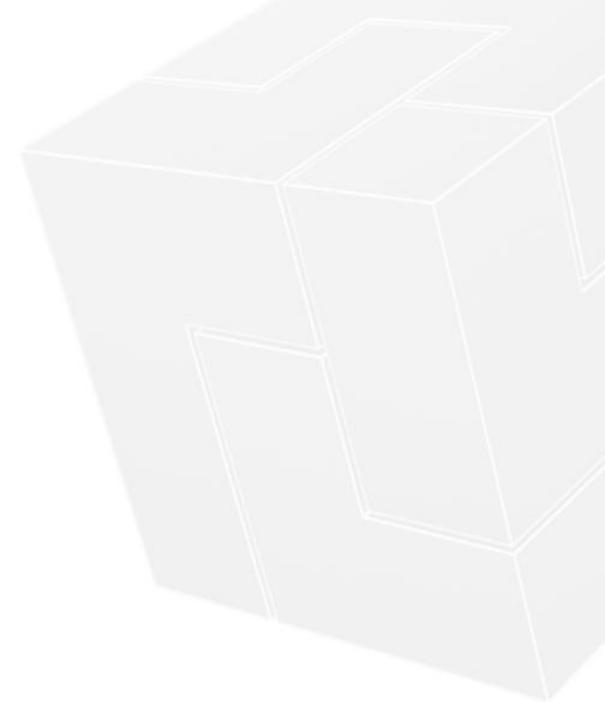
OpenShift  
Infra Design

OpenShift  
Pipeline

OpenShift  
App Devel

Docker Swarm  
Architecture PoC

FE 2.0 Project



Before  
Containers

World of  
Containers

OpenShift  
Infra Design

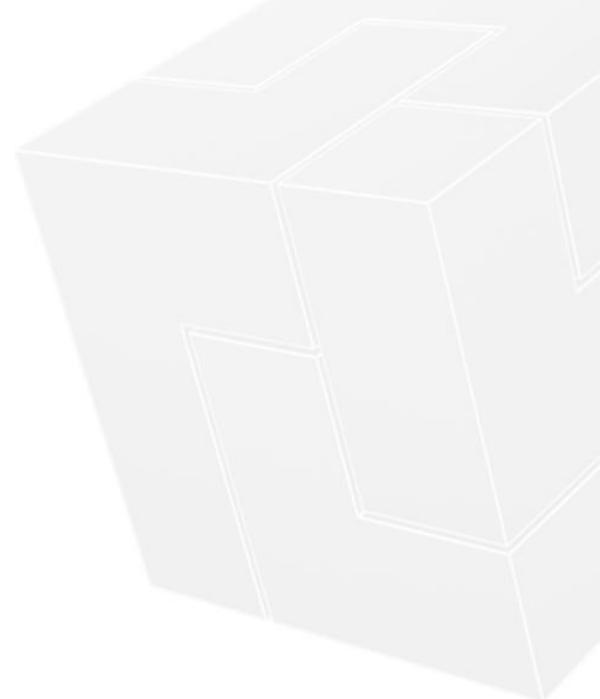
OpenShift  
Pipeline

OpenShift  
App Devel

Docker Swarm  
Architecture PoC

FE 2.0 Project

Docker Swarm  
Infra PoC



Before  
Containers

World of  
Containers

OpenShift  
Infra Design

OpenShift  
Pipeline

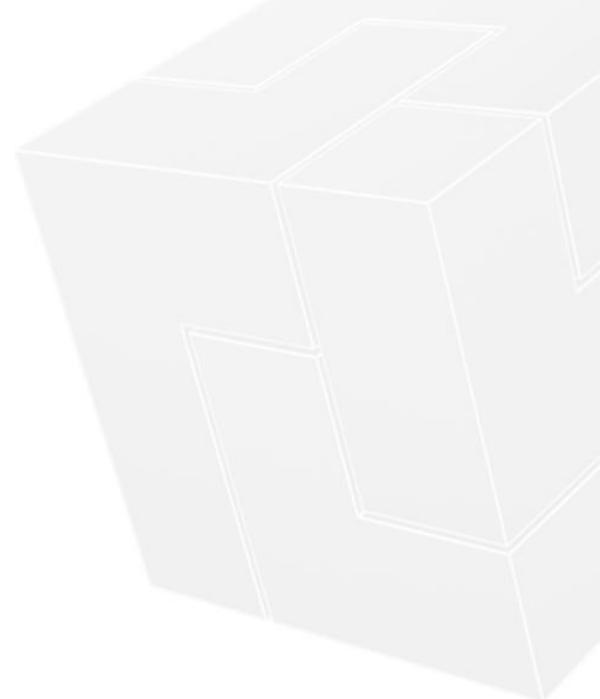
OpenShift  
App Devel

Docker Swarm  
Architecture PoC

FE 2.0 Project

Docker Swarm  
Infra PoC

BZWBK24  
Docker in  
Production



Before  
Containers

World of  
Containers

OpenShift  
Infra Design

OpenShift  
Pipeline

OpenShift  
App Devel

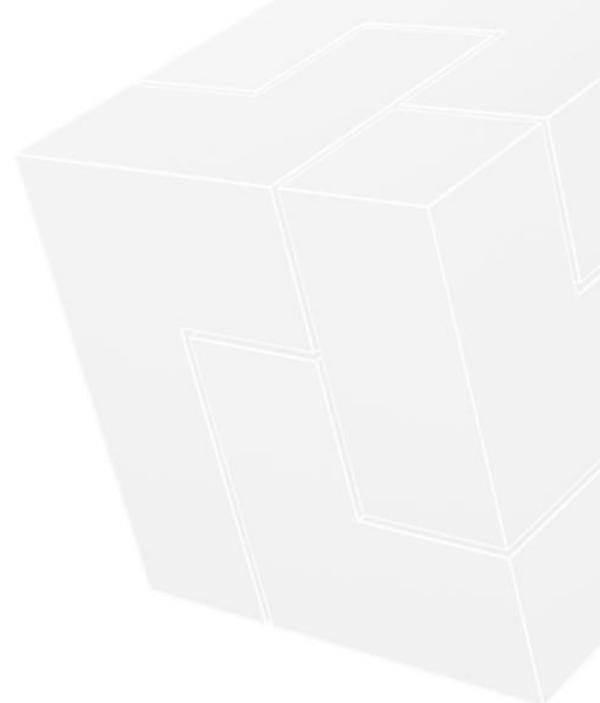
Docker Swarm  
Architecture PoC

FE 2.0 Project

Docker Swarm  
Infra PoC

BZWBK24  
Docker in  
Production

We all go together!



Before  
Containers

World of  
Containers

OpenShift  
Infra Design

OpenShift  
Pipeline

OpenShift  
App Devel

Docker Swarm  
Architecture PoC

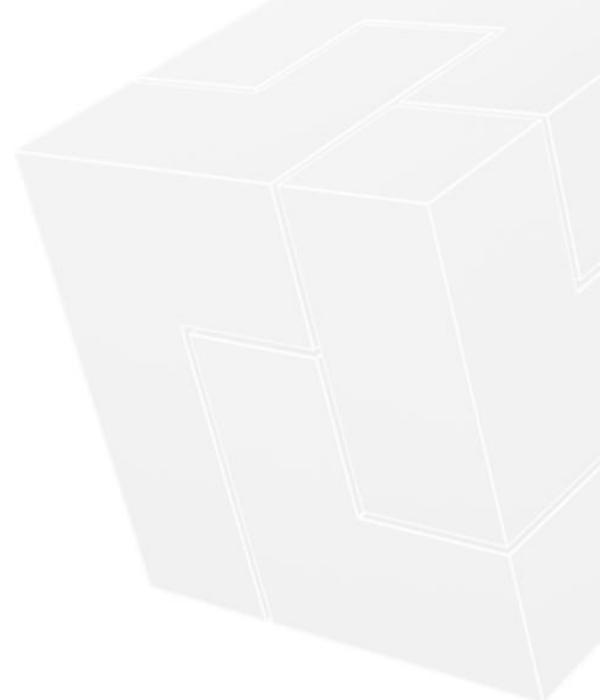
FE 2.0 Project

Docker Swarm  
Infra PoC

BZWBK24  
Docker in  
Production

We all go together!

Docker Swarm  
issues



Before  
Containers

World of  
Containers

OpenShift  
Infra Design

OpenShift  
Pipeline

OpenShift  
App Devel

Docker Swarm  
Architecture PoC

FE 2.0 Project

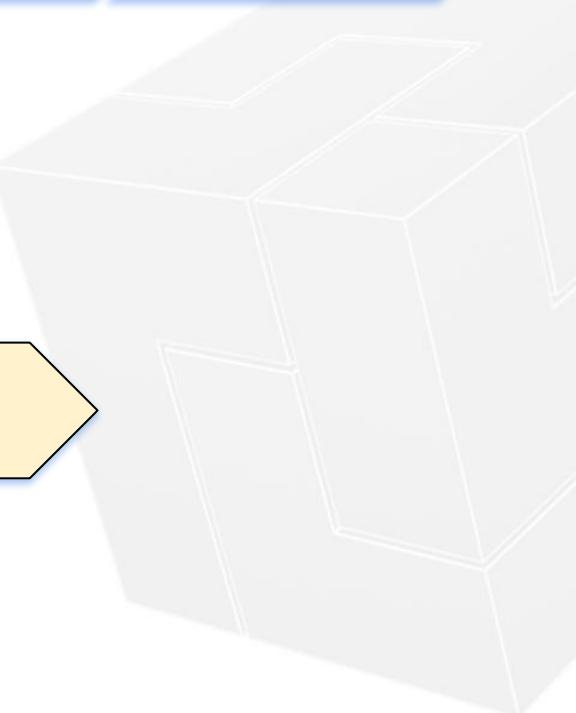
Docker Swarm  
Infra PoC

BZWBK24  
Docker in  
Production

We all go together!

Docker Swarm  
issues

RFI  
RFP



Before  
Containers

World of  
Containers

OpenShift  
Infra Design

OpenShift  
Pipeline

OpenShift  
App Devel

Docker Swarm  
Architecture PoC

FE 2.0 Project

Docker Swarm  
Infra PoC

BZWBK24  
Docker in  
Production

We all go together!

Docker Swarm  
issues

RFI  
RFP

OpenShift!

Bank central 🚨  
I Use internal  
ii registry and  
ii external if needed!

Service Serving  
Certificate Secrets!

4 Clusters  
3 Clusters  
2 Clusters  
2 Clusters  
1 Prod / 1 Test

# Adjusting deployments to new cloud native reality

Before  
Containers

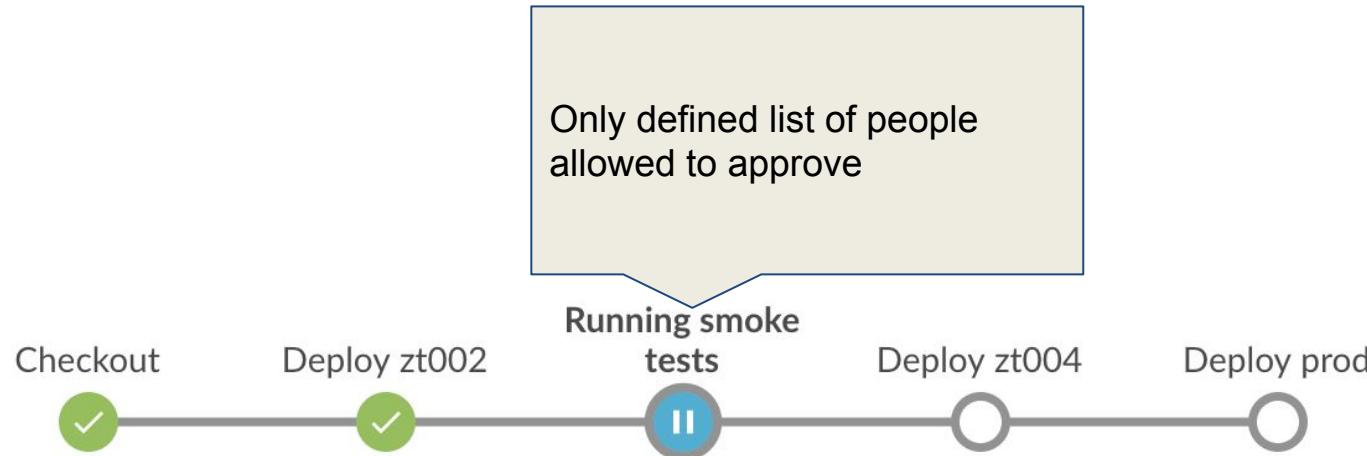
World of  
Containers

OpenShift  
Infra Design

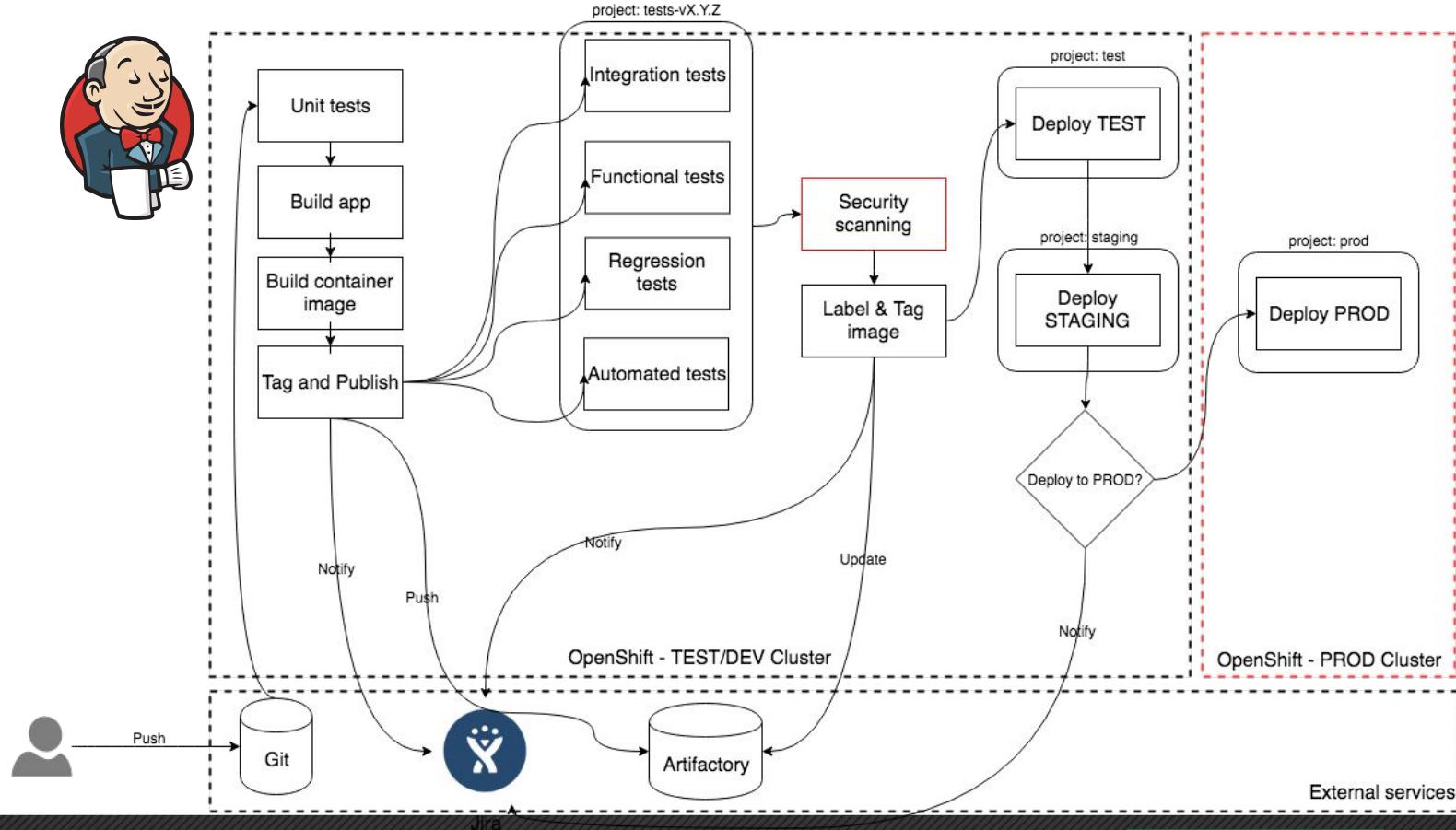
OpenShift  
Pipeline

OpenShift  
App Devel

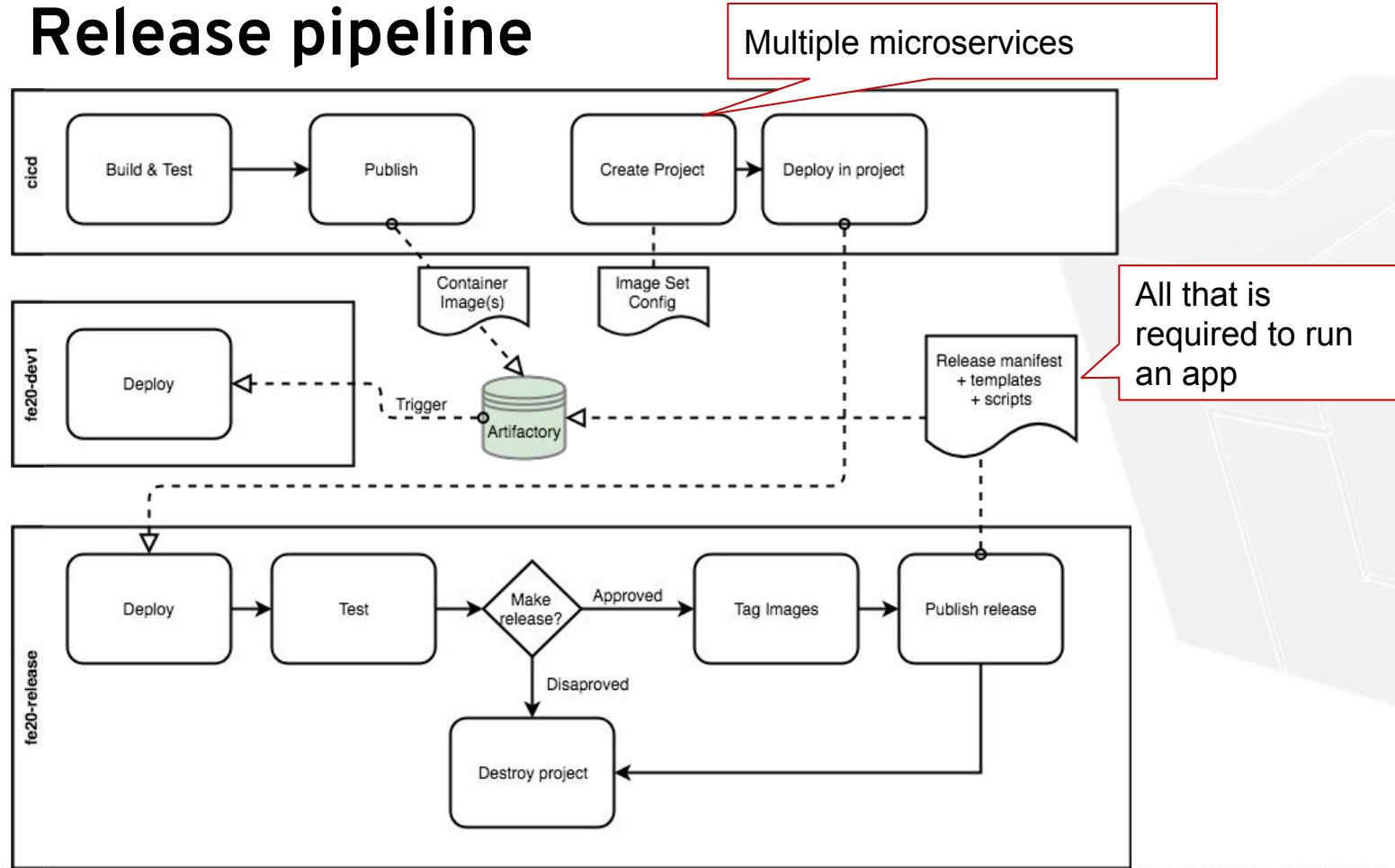
# Continuous Deployment pipeline



# Speeding up deployment with CD pipelines



# Release pipeline



# Release pipeline

	Checkout	Check release project	Delete project	Create project	Deploy application	Running smoke tests	Publish release	Email notification
Average stage times: (Average full run time: ~12min 10s)	11s	4s	5s	8s	17s	1min 6s	50s	1s
fe20-release-0.4.3	2s	2s (paused for 15s)	2s	4s	8s	1min 10s	46s	1s
fe20-release-0.4.2	14s	4s (paused for 1min 6s)	6s	9s	19s	55s	51s	1s
fe20-release-0.4.2	15s	4s (paused for 3s)	6s	9s	20s	1min 4s		
fe20-release-0.4.1	12s	4s (paused for 2s)	6s	9s	20s	51s	47s	1s
fe20-release-0.4.1	11s	4s (paused for 4min 23s)	7s	8s	20s			



Before  
Containers

World of  
Containers

OpenShift  
Infra Design

OpenShift  
Pipeline

OpenShift  
App Devel

# Creating secure and compliant container images

Before  
Containers

World of  
Containers

OpenShift  
Infra Design

OpenShift  
Pipeline

OpenShift  
App Dev

Use [github.com](https://github.com) to  
fork/clone images  
sources

Before  
Containers

World of  
Containers

OpenShift  
Infra Design

OpenShift  
Pipeline

OpenShift  
App Dev

Use [github.com](https://github.com) to  
fork/clone images  
sources

Need all images to  
be RHEL based

Before  
Containers

World of  
Containers

OpenShift  
Infra Design

OpenShift  
Pipeline

OpenShift  
App Dev!

Use [github.com](https://github.com) to  
fork/clone images  
sources

Need all images to  
be RHEL based

Sources not  
binaries! No docker  
hub!

## Before Containers

## World of Containers

## OpenShift Infra Design

## OpenShift Pipeline

## OpenShift App Dev!

Use [github.com](https://github.com) to  
fork/clone images  
sources

Need all images to  
be RHEL based

Sources not  
binaries! No docker  
hub!

Own proxies and  
repos

Before  
Containers

World of  
Containers

OpenShift  
Infra Design

OpenShift  
Pipeline

OpenShift  
App Dev

Use [github.com](https://github.com) to  
fork/clone images  
sources

Need all images to  
be RHEL based

Sources not  
binaries! No docker  
hub!

Own proxies and  
repos

Create own base  
images for s2i and  
other products

Before  
Containers

World of  
Containers

OpenShift  
Infra Design

OpenShift  
Pipeline

OpenShift  
App Dev

Use [github.com](https://github.com) to  
fork/clone images  
sources

Need all images to  
be RHEL based

Sources not  
binaries! No docker  
hub!

Own proxies and  
repos

Create own base  
images for s2i and  
other products

Internal non-public  
Certificate  
Authority

## Before Containers

## World of Containers

## OpenShift Infra Design

## OpenShift Pipeline

## OpenShift App Dev!

Use [github.com](https://github.com) to  
fork/clone images  
sources

Need all images to  
be RHEL based

Sources not  
binaries! No docker  
hub!

Own proxies and  
repos

Create own base  
images for s2i and  
other products

Internal non-public  
Certificate  
Authority

All exposed  
services protected  
by TLS

## Before Containers

## World of Containers

## OpenShift Infra Design

## OpenShift Pipeline

## OpenShift App Dev!

Use [github.com](https://github.com) to  
fork/clone images  
sources

Need all images to  
be RHEL based

Sources not  
binaries! No docker  
hub!

Own proxies and  
repos

Create own base  
images for s2i and  
other products

Internal non-public  
Certificate  
Authority

All exposed  
services protected  
by TLS

Need to provide  
boilerplates for  
developers

## Before Containers

## World of Containers

## OpenShift Infra Design

## OpenShift Pipeline

## OpenShift App Dev!

Use [github.com](https://github.com) to  
fork/clone images  
sources

Need all images to  
be RHEL based

Sources not  
binaries! No docker  
hub!

Own proxies and  
repos

Create own base  
images for s2i and  
other products

Internal non-public  
Certificate  
Authority

All exposed  
services protected  
by TLS

Need to provide  
boilerplates for  
developers

When you need  
adjustment you  
change it in one  
place

Before  
Containers

World of  
Containers

OpenShift  
Infra Design

OpenShift  
Pipeline

OpenShift  
App Dev

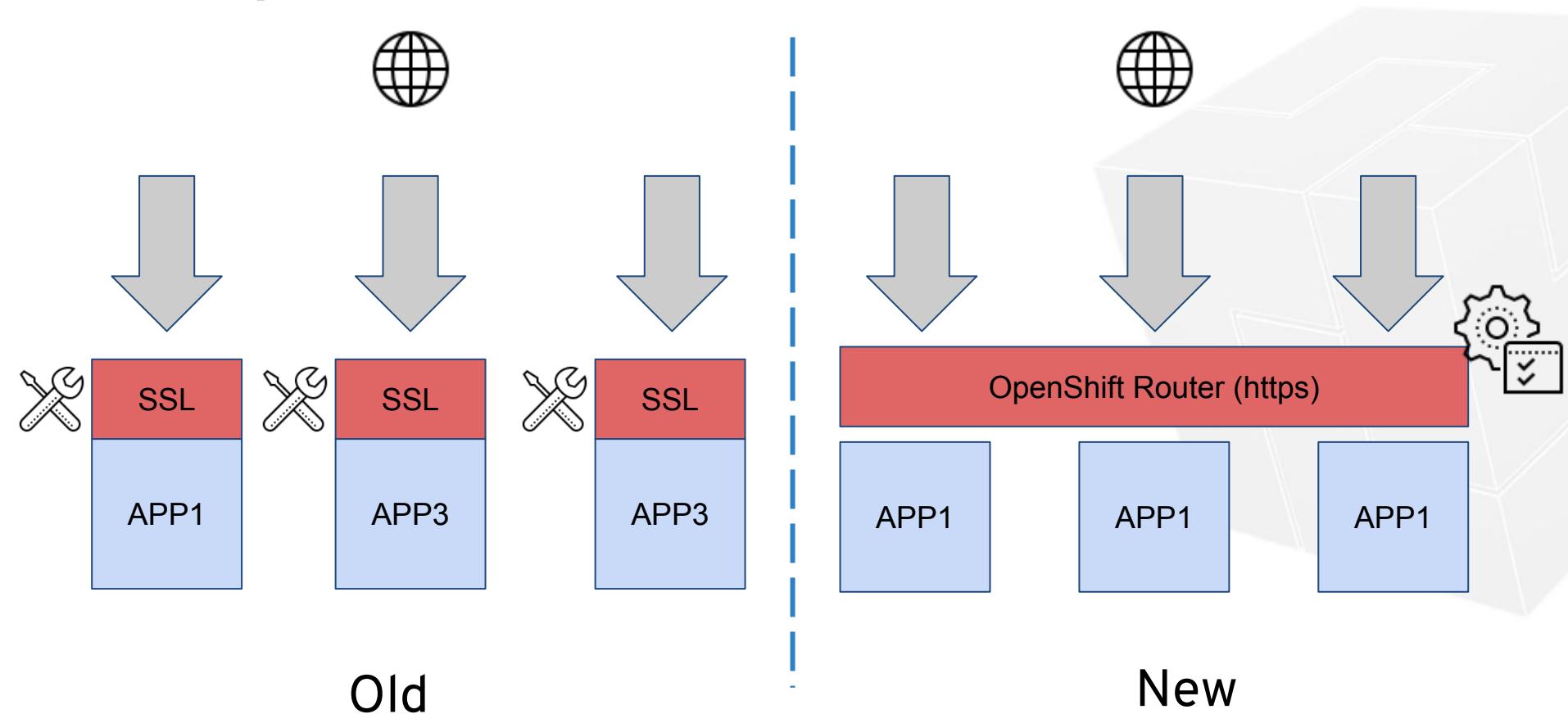
```
FROM registry.access.redhat.com/rhel7:latest

RUN ln -sf /usr/share/zoneinfo/Europe/Warsaw /etc/localtime
RUN cd /etc/pki/ca-trust/source/anchors/ && \
    curl -Awget -O "http://pki.bzwbk.pl/pki/CA1.crt" && \
    update-ca-trust extract
[...]
```

# Dealing with security and compliance requirements

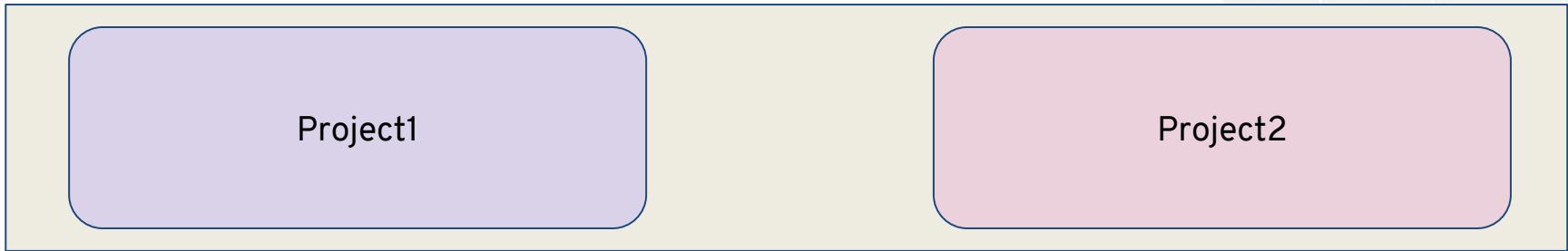


# Security controlled with code

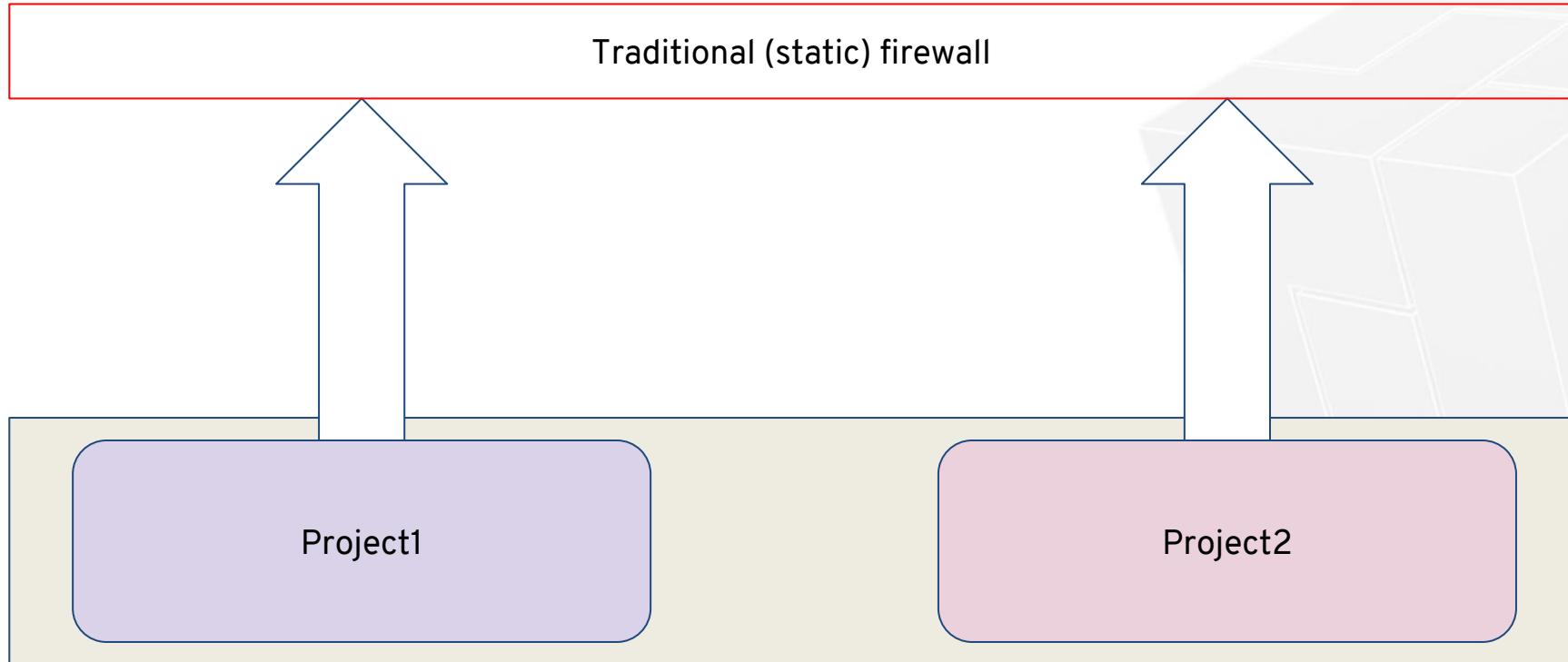


# Traffic isolation between applications

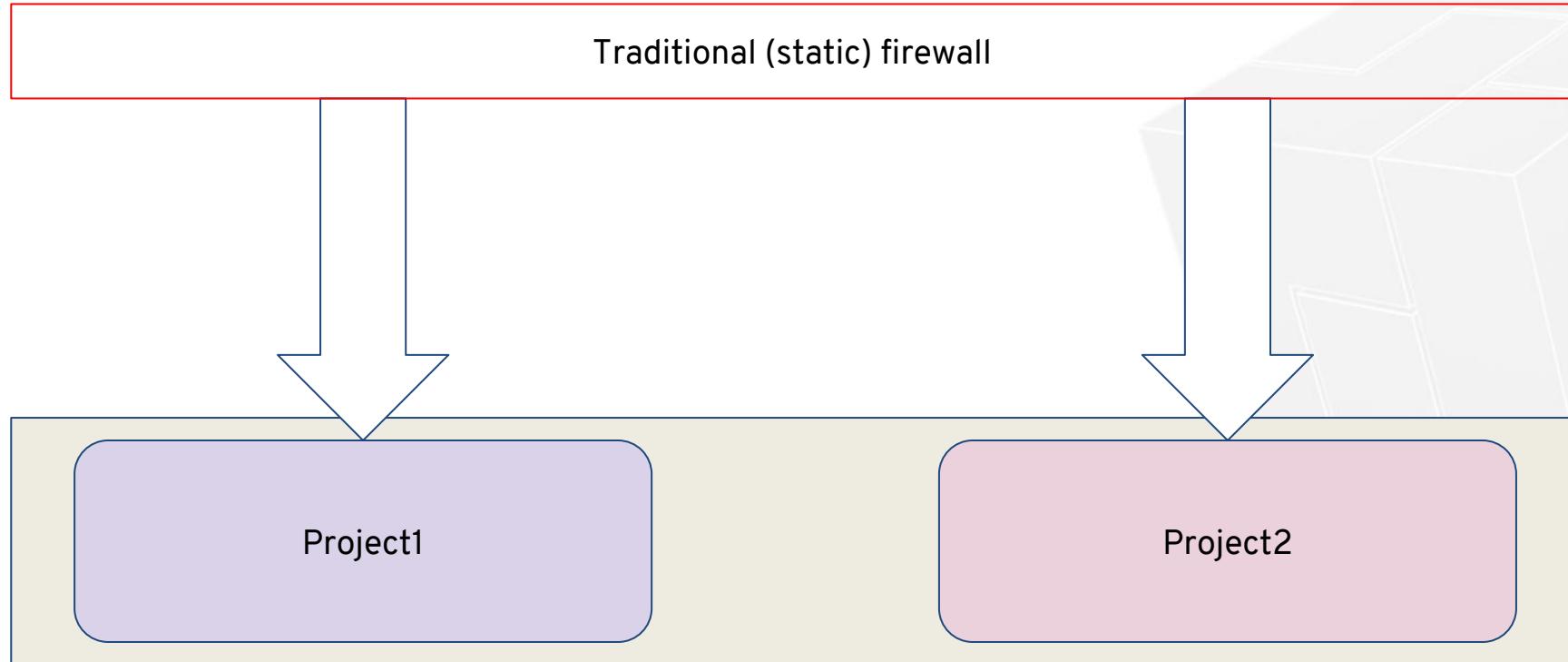
# Traffic isolation



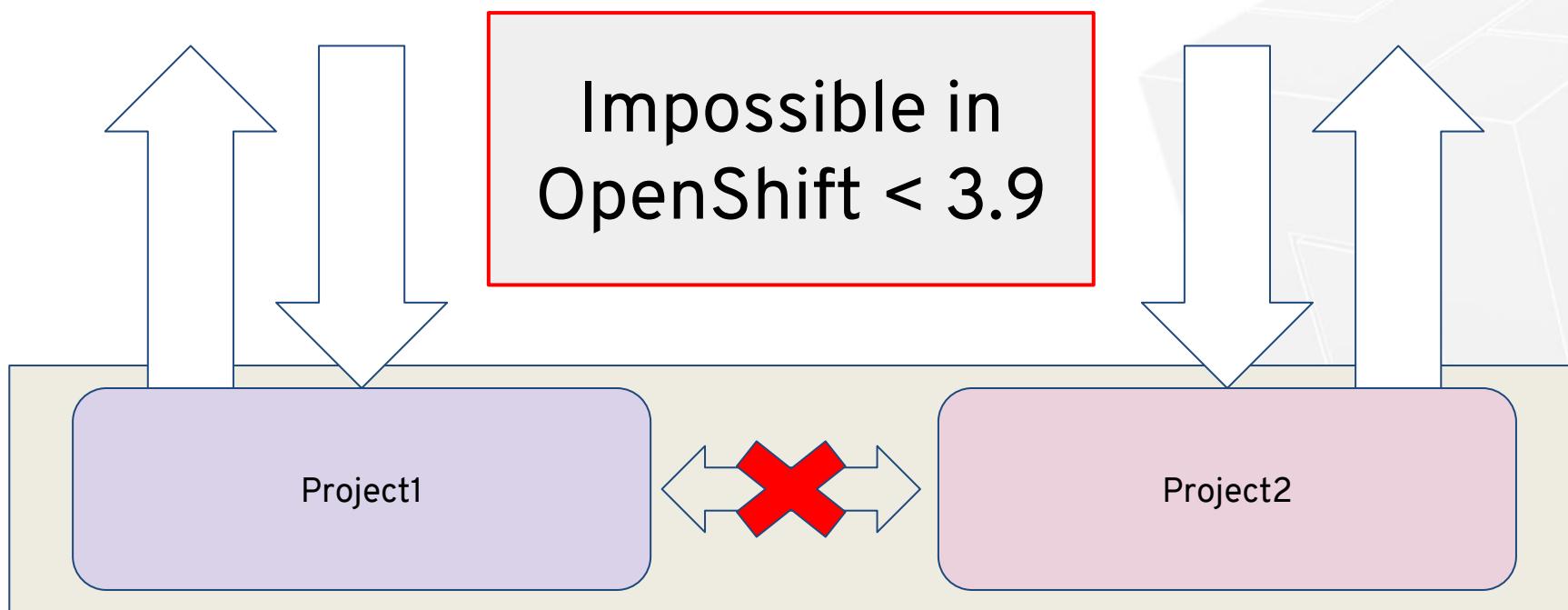
# Outbound traffic



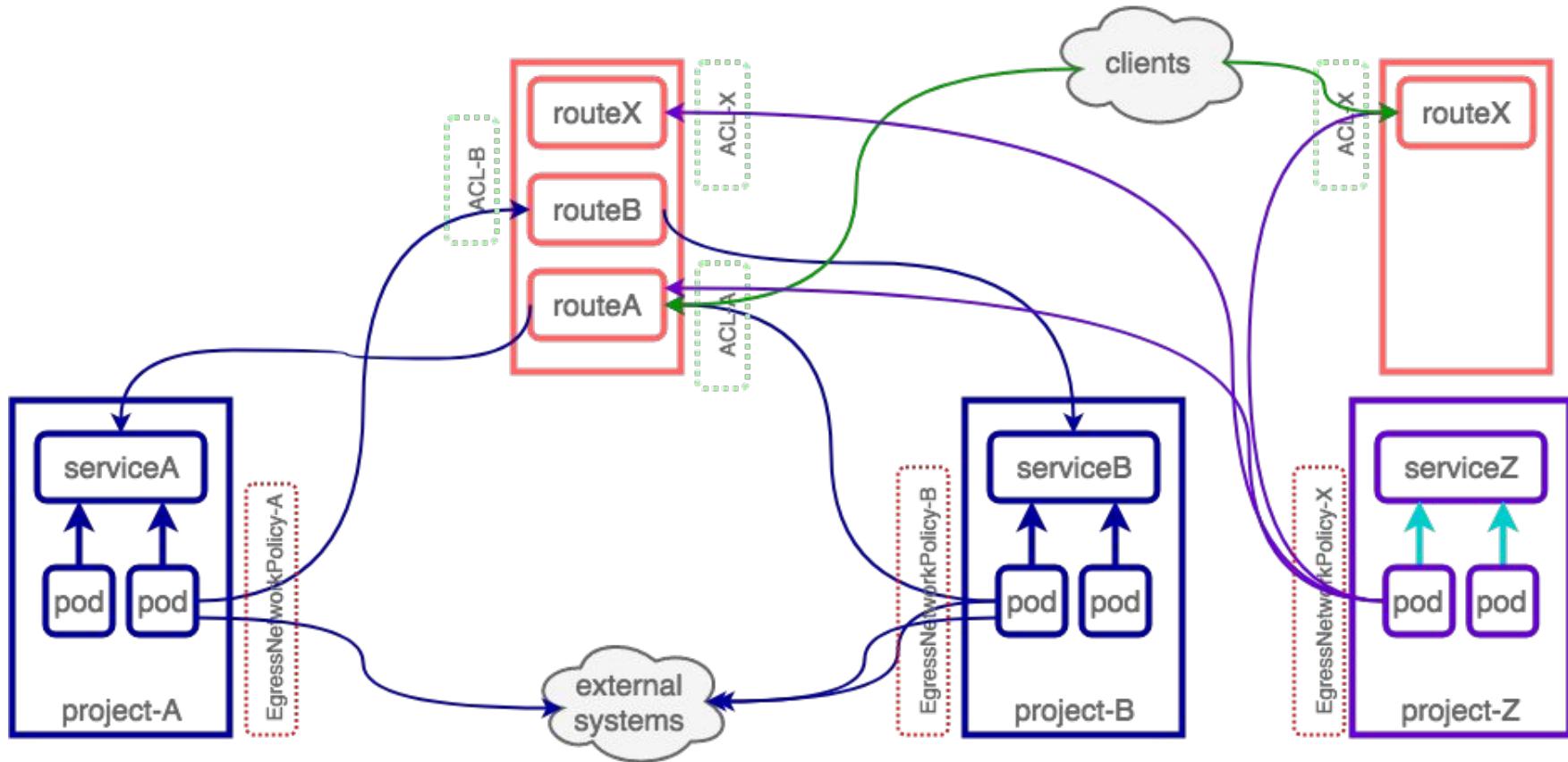
# Inbound traffic



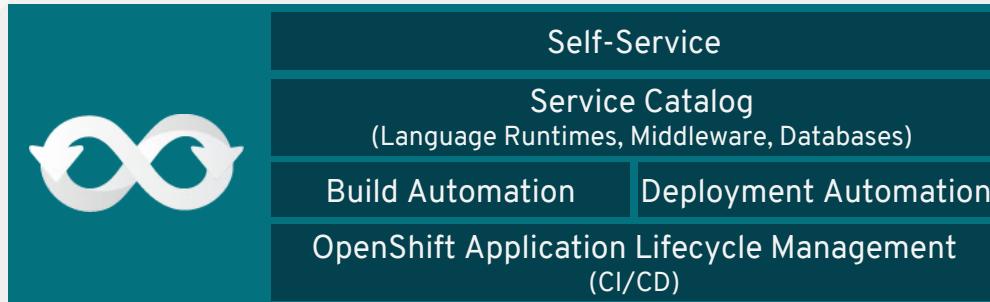
# You can't always get what you want



# Overcoming OpenShift shortcomings



# SECURITY ACROSS ALL LAYERS



**CONTROL**  
Application Security



**DEFEND**  
Infrastructure



**EXTEND**

# AUTOMATED & INTEGRATED SECURITY



## CONTROL

Application Security

Container Content

CI/CD Pipeline

Container Registry

Deployment Policies



## DEFEND

Infrastructure

Container Platform

Container Host Multi-tenancy

Network Isolation

Storage

Audit & Logging

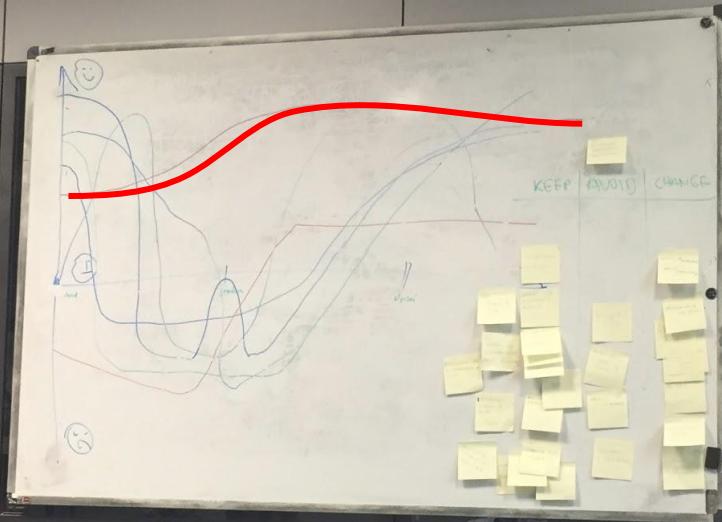
API Management



## EXTEND

Security Ecosystem

<https://www.redhat.com/en/resources/container-security-openshift-cloud-devops-whitepaper>



And  
this is what we call

**DevOps**

**IN A BANK!**

# Contact us



Tomasz Cholewa, Mindbox  
Lead Cloud Architect  
[tomasz.cholewa@mindboxgroup.com](mailto:tomasz.cholewa@mindboxgroup.com)  
<https://mindboxgroup.com>



Dawid Szymański, BZWBK  
IT Architect  
[dawid.szymanski@bzbwk.pl](mailto:dawid.szymanski@bzbwk.pl)  
<https://www.bzbwk.pl>



Jarosław Stakun, Red Hat  
Lead Solution Architect  
[jarek@redhat.com](mailto:jarek@redhat.com)  
<http://www.openshift.com>