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?

X86 VM

X86 VM

IBM LPAR

X86 VM

IBM LPAR

Technology obsolescence

X86 VM

IBM LPAR

Technology obsolescence

A lot of manual work

X86 VM

IBM LPAR

Technology obsolescence

A lot of manual work

Almost no control over development components

X86 VM

IBM LPAR

Technology obsolescence

A lot of manual work

Almost no control over development components

A lot of different versions of platforms

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 ...

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

Docker Swarm Architecture PoC

Docker Swarm Architecture PoC

FE 2.0 Project

- Docker Swarm Architecture PoC
- FE 2.0 Project
- Docker Swarm Infra PoC

- Docker Swarm Architecture PoC
- FE 2.0 Project
- Docker Swarm Infra PoC
- BZWBK24 Docker in Production

- Docker Swarm Architecture PoC
- FE 2.0 Project
- Docker Swarm Infra PoC
- BZWBK24 Docker in Production

We all go together!

Docker Swarm Architecture PoC

FE 2.0 Project

Docker Swarm Infra PoC

BZWBK24 Docker in Production

We all go together!

Docker Swarm issues

Docker Swarm Architecture PoC

FE 2.0 Project

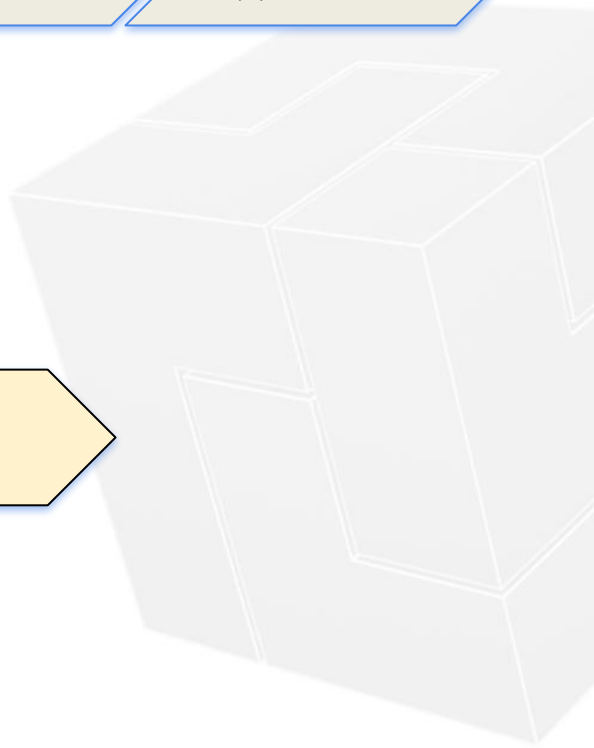
Docker Swarm Infra PoC

BZWBK24 Docker in Production

We all go together!

Docker Swarm issues

RFI
RFP



Docker Swarm Architecture PoC

FE 2.0 Project

Docker Swarm Infra PoC

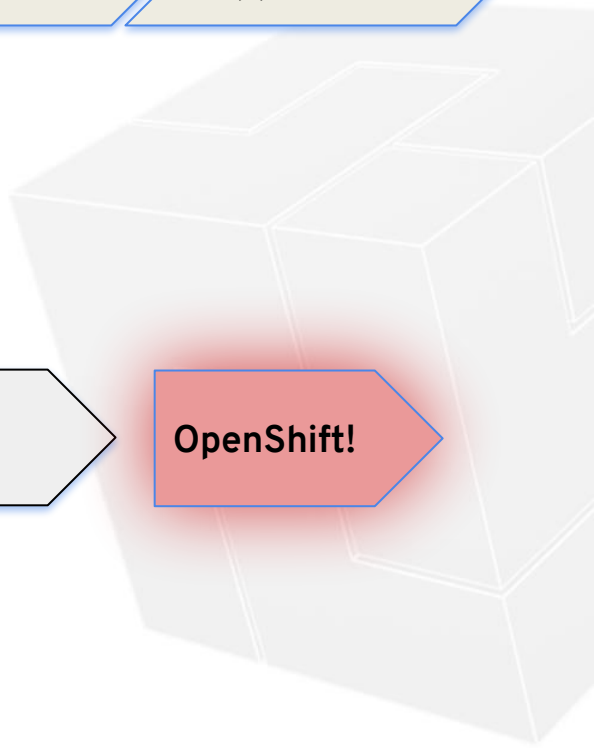
BZWBK24 Docker in Production

We all go together!

Docker Swarm issues

RFI RFP

OpenShift!



Service Serving Certificate Secrets!

Use internal registry and external if needed!

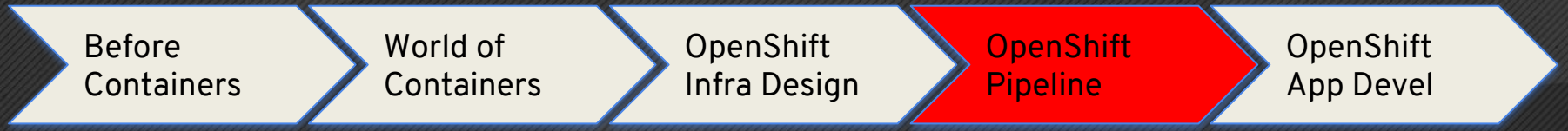
2 Clusters

1 Prod / 1 Test

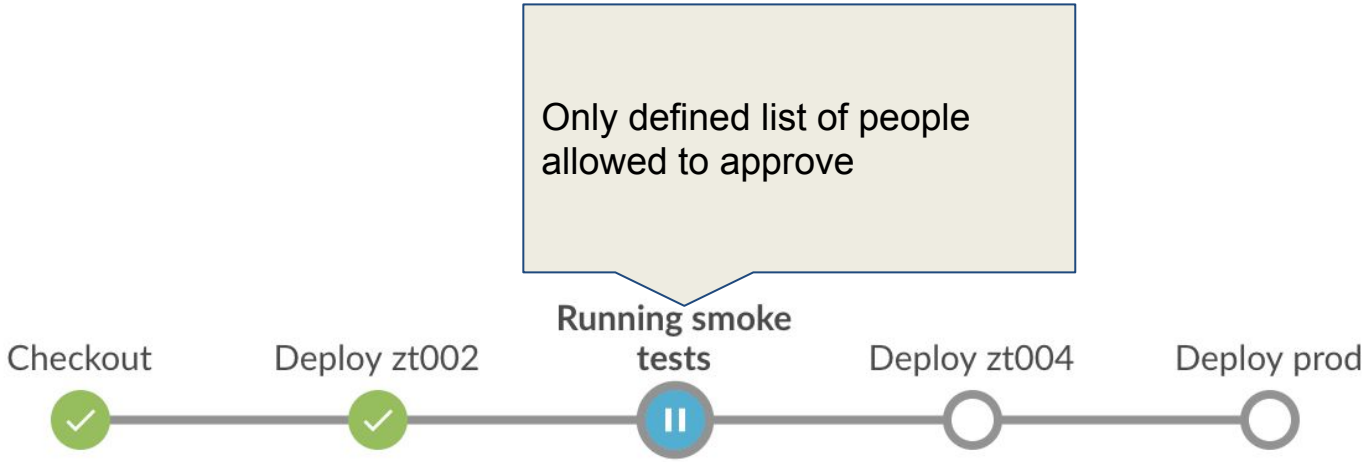
Adjusting deployments to new cloud native reality

Bank Zachodni WBK
Grupa Santander

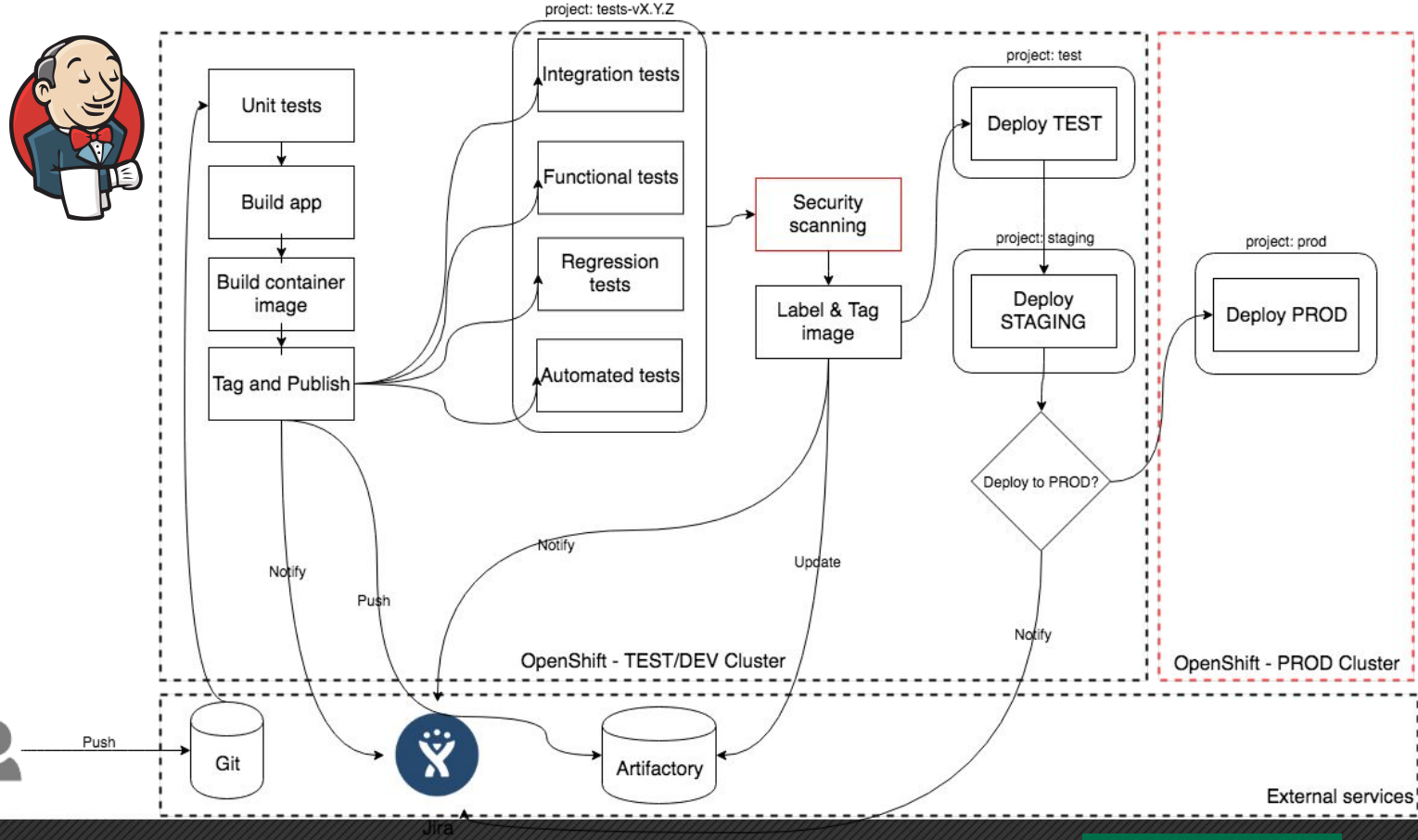
mindbox



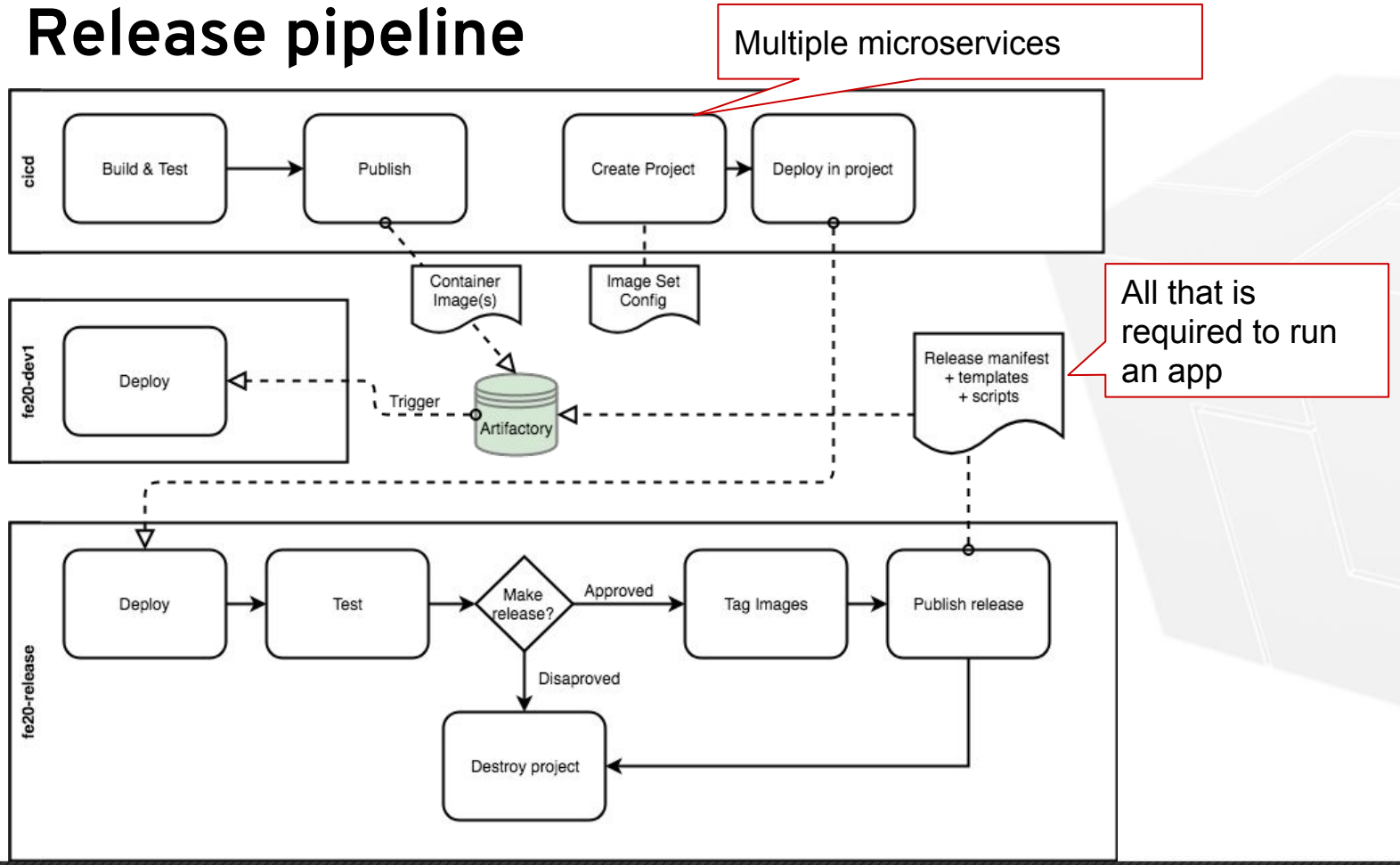
Continuous Deployment pipeline



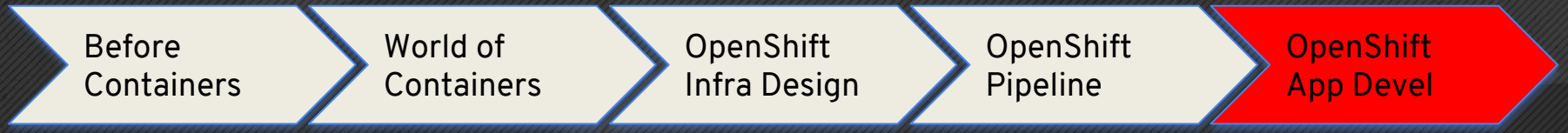
Speeding up deployment with CD pipelines



Release pipeline



Release pipeline



Creating secure and compliant container images

Use github.com to fork/clone images sources

Use github.com to fork/clone images sources

Need all images to be RHEL based

Use 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 Devel

Use github.com to fork/clone images sources

Need all images to be RHEL based

Sources not binaries! No docker hub!

Own proxies and repos

Use 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

Use 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

Use 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

Use 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 Devel**

Use 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

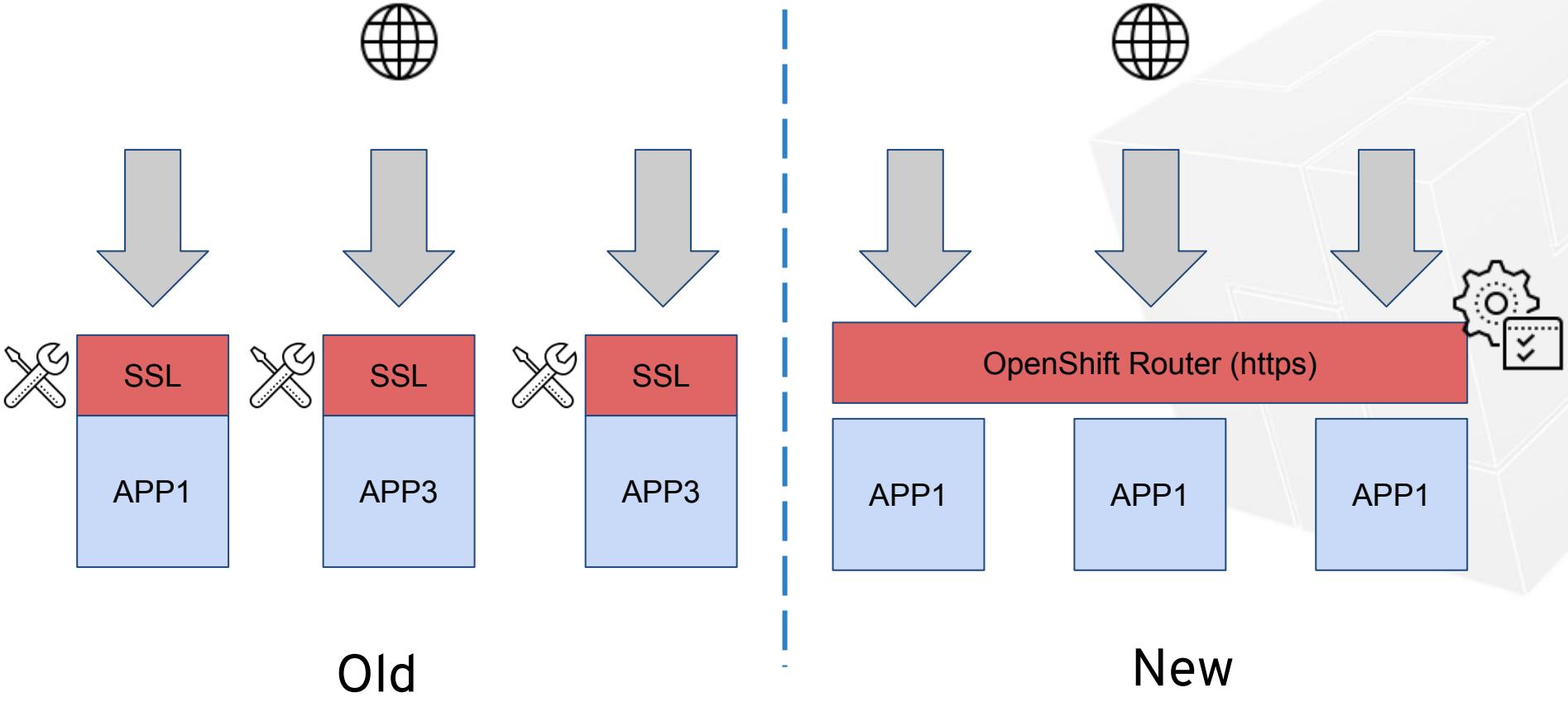
When you need adjustment you change it in one place

```
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
[...]
```

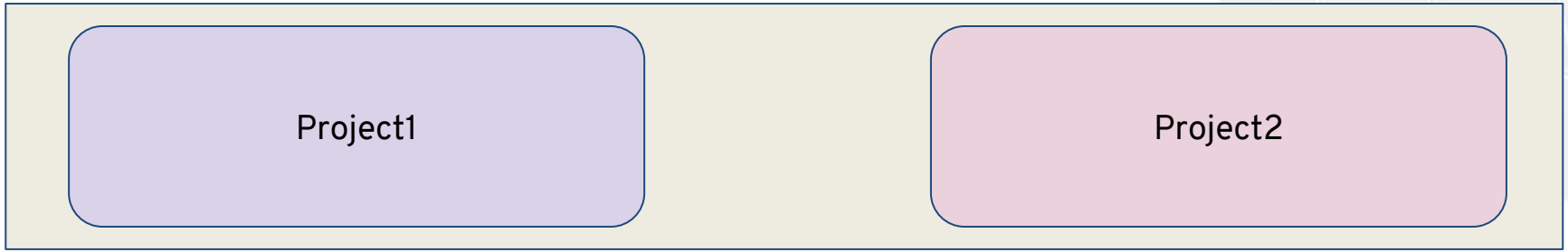
Dealing with security and compliance requirements

Security controlled with code

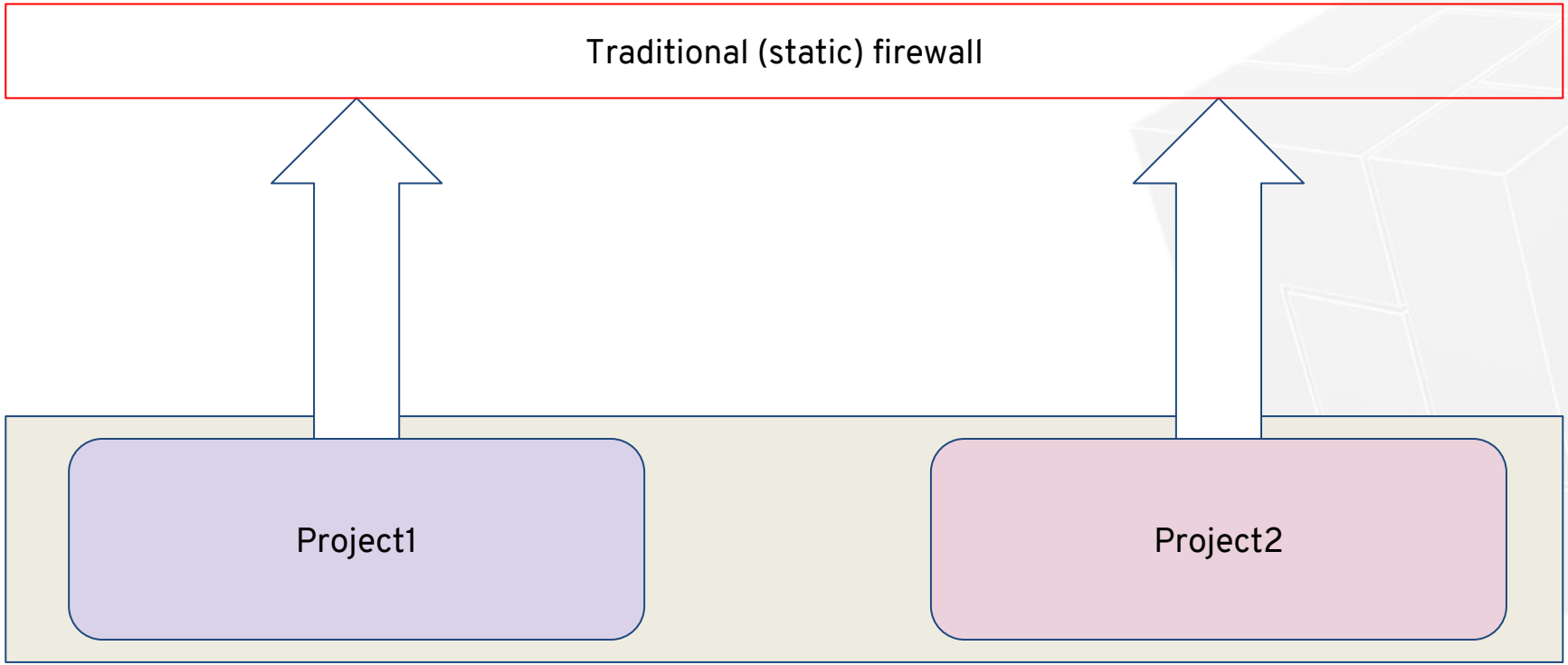


Traffic isolation between applications

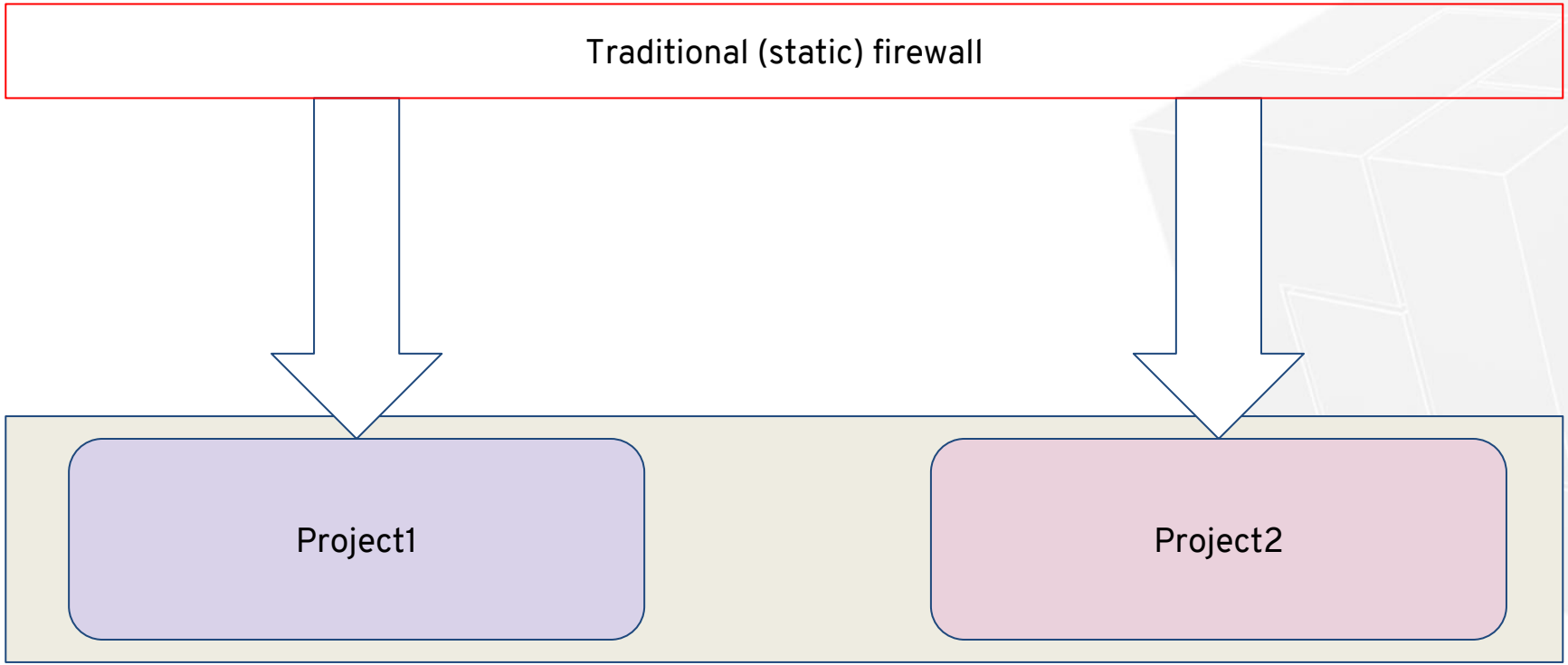
Traffic isolation



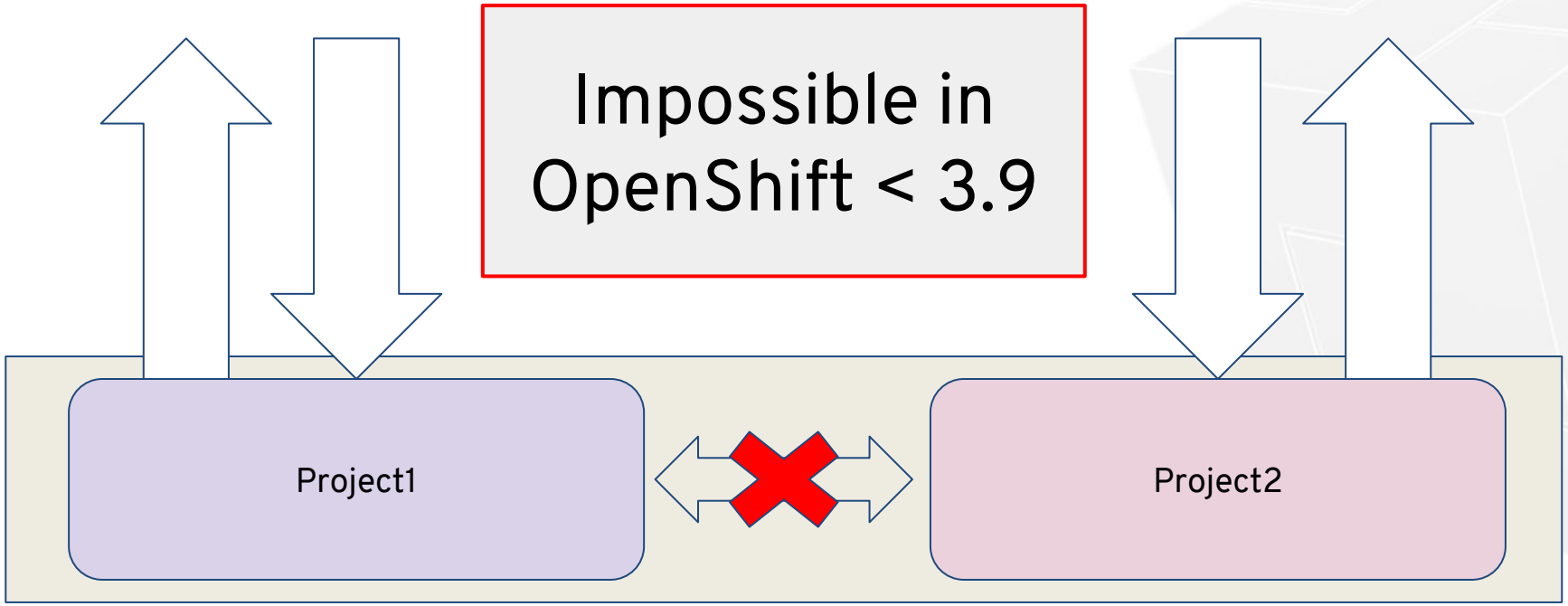
Outbound traffic



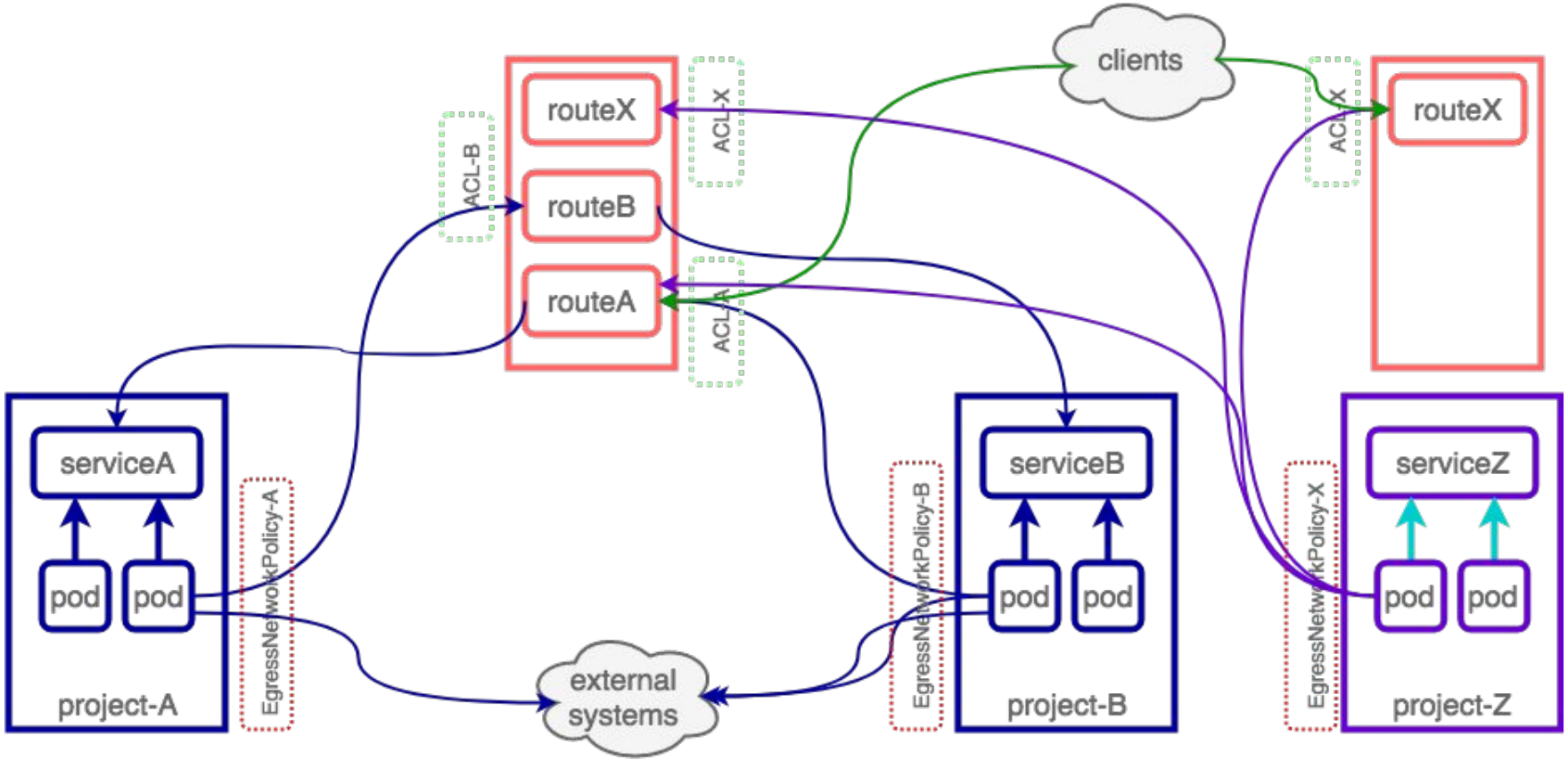
Inbound traffic



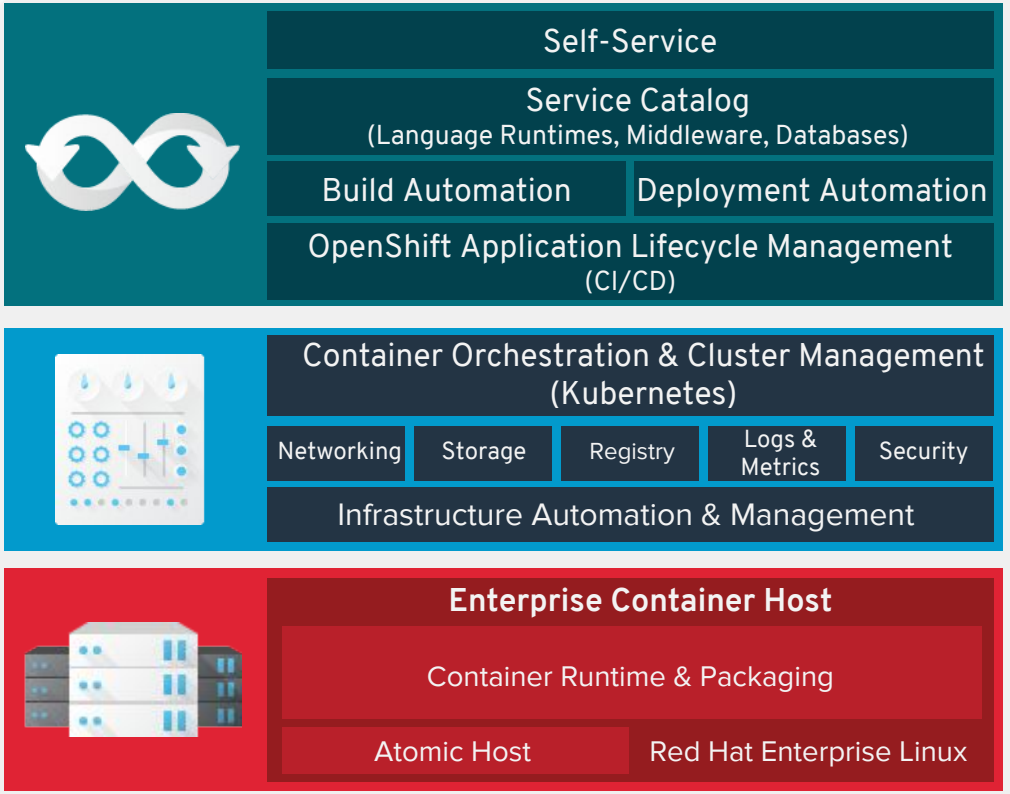
You can’t always get what you want



Overcoming OpenShift shortcomings



SECURITY ACROSS ALL LAYERS



CONTROL
Application Security

DEFEND
Infrastructure

EXTEND

AUTOMATED & INTEGRATED SECURITY

mindbox

CONTROL
Application Security

- Container Content
- CI/CD Pipeline
- Container Registry
- Deployment Policies

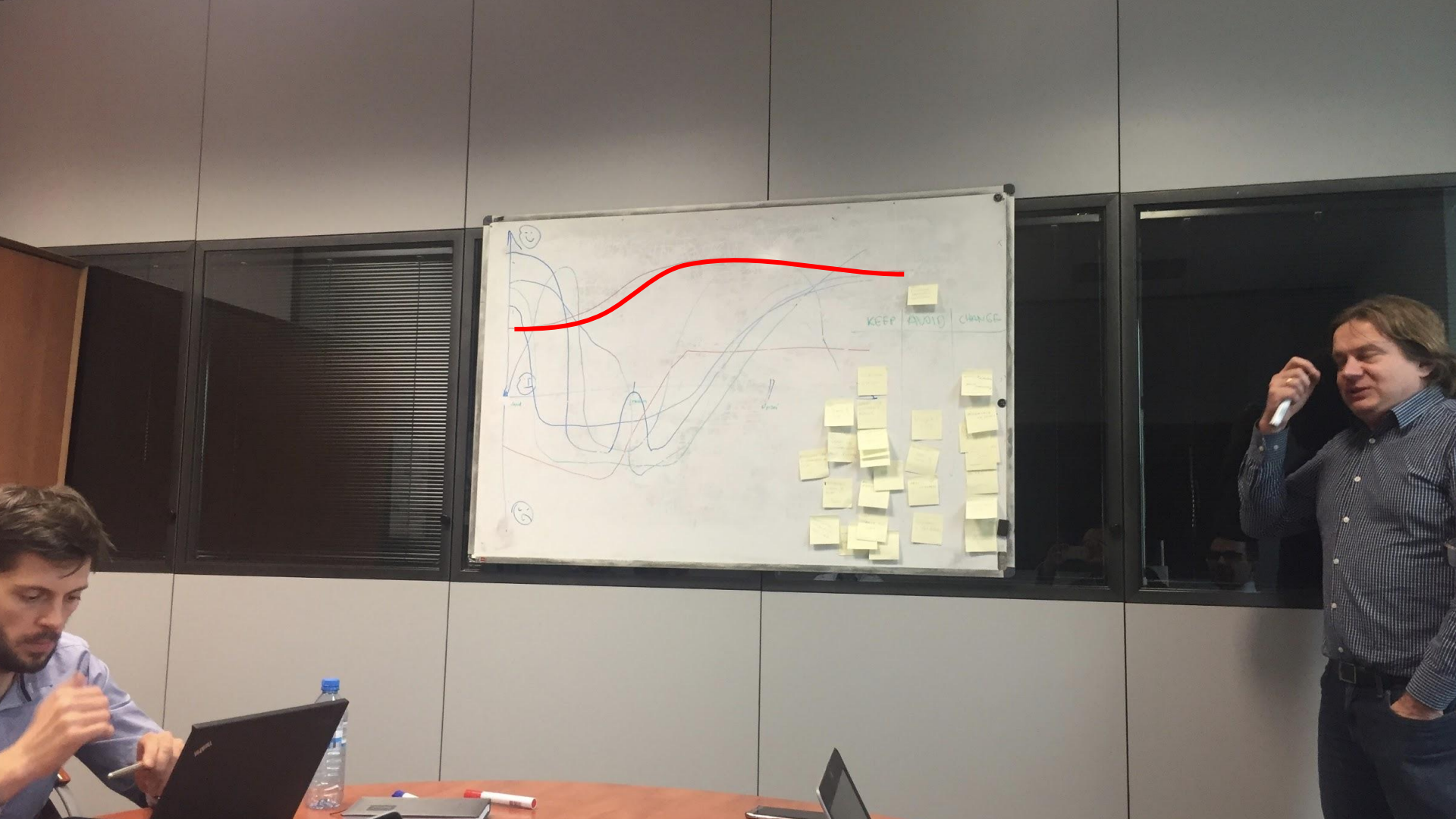
DEFEND
Infrastructure

- 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


KEEP
AVOID
CHANGE

And
this is what we call

DevOps

IN A BANK!

Bank Zachodni WBK
Grupa Santander

mindbox

Contact us

Tomasz Cholewa, Mindbox

Lead Cloud Architect

tomasz.cholewa@mindboxgroup.com

https://mindboxgroup.com

Dawid Szymański, BZWBK

IT Architect

dawid.szymanski@bzwbk.pl

https://www.bzwbk.pl

Jarosław Stakun, Red Hat

Lead Solution Architect

jarek@redhat.com

http://www.openshift.com