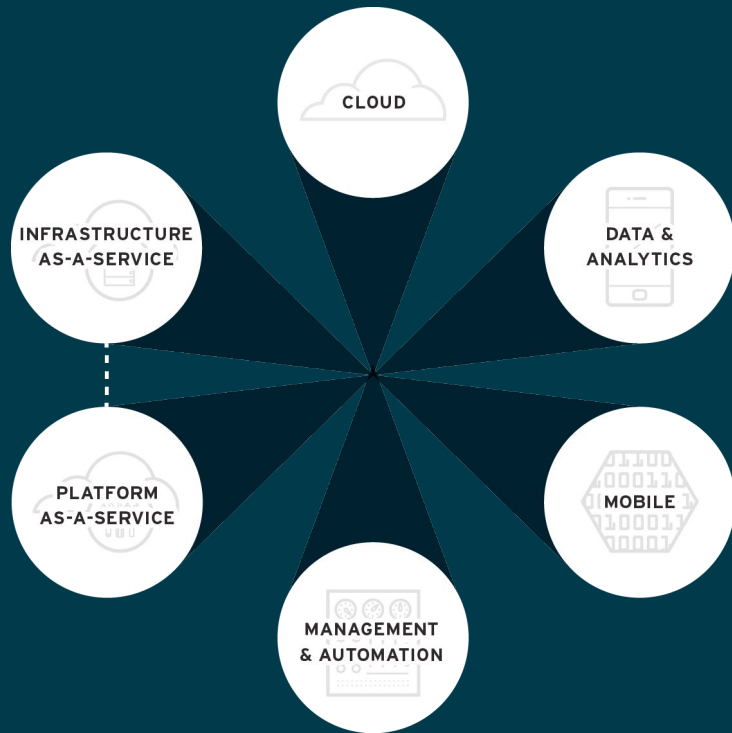




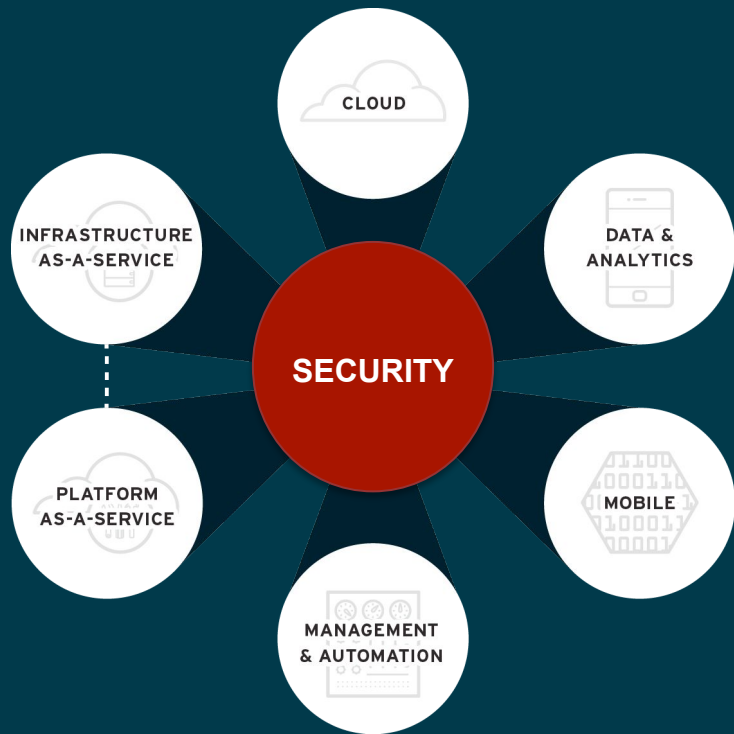
NEW ERA OF DIGITAL SECURITY

Shawn Wells
Chief Security Strategist
U.S. Public Sector
shawn@redhat.com || 443-534-0130

Technology for the Digital World



When New Technologies are adopted, the Security team gets involved



Securing the Enterprise is Harder Than Ever

The way we develop, deploy and manage IT is changing dramatically



Menacing
threat
landscape



Dissolving
security
perimeter



Software-defined
infrastructure



Cloud
computing



Applications &
devices outside
of IT control

TRADITIONAL NETWORK-BASED DEFENSES ARE NO LONGER ENOUGH

THE COST OF SECURITY BREACHES



**Total average costs
are increasing:**

2016 \$4.0 million

2015 \$3.8 million

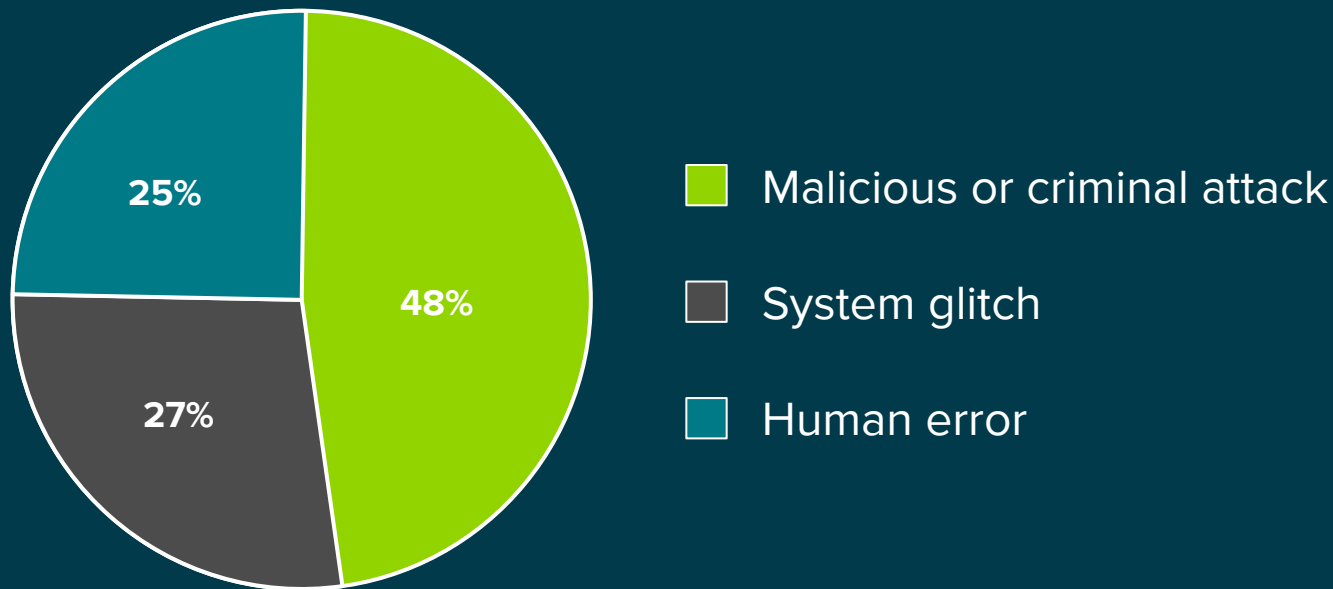
2014 \$3.5 million



**While “soft” costs are
impacting your business**

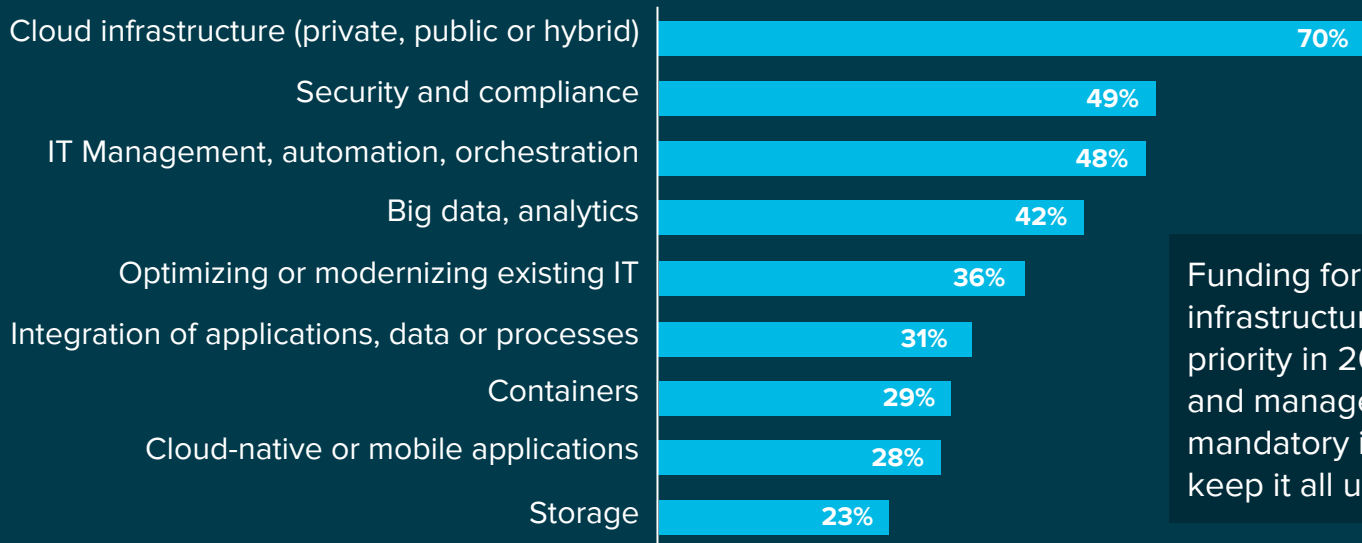
- Business disruption
- Lost employee and customer trust
- Brand erosion
- Shareholder anger
- etc

MULTIPLE SOURCES OF RISKS



TRYING TO INNOVATE AND REMAIN SECURE AT THE SAME TIME

What are you organization's top IT funding priorities for 2017?*



Funding for cloud infrastructure is taking a clear priority in 2017, with security and management still mandatory investments to keep it all under control.

*Select all that apply

IMPLEMENT BOTH AGILE & IMPROVED GOVERNANCE PROCESSES

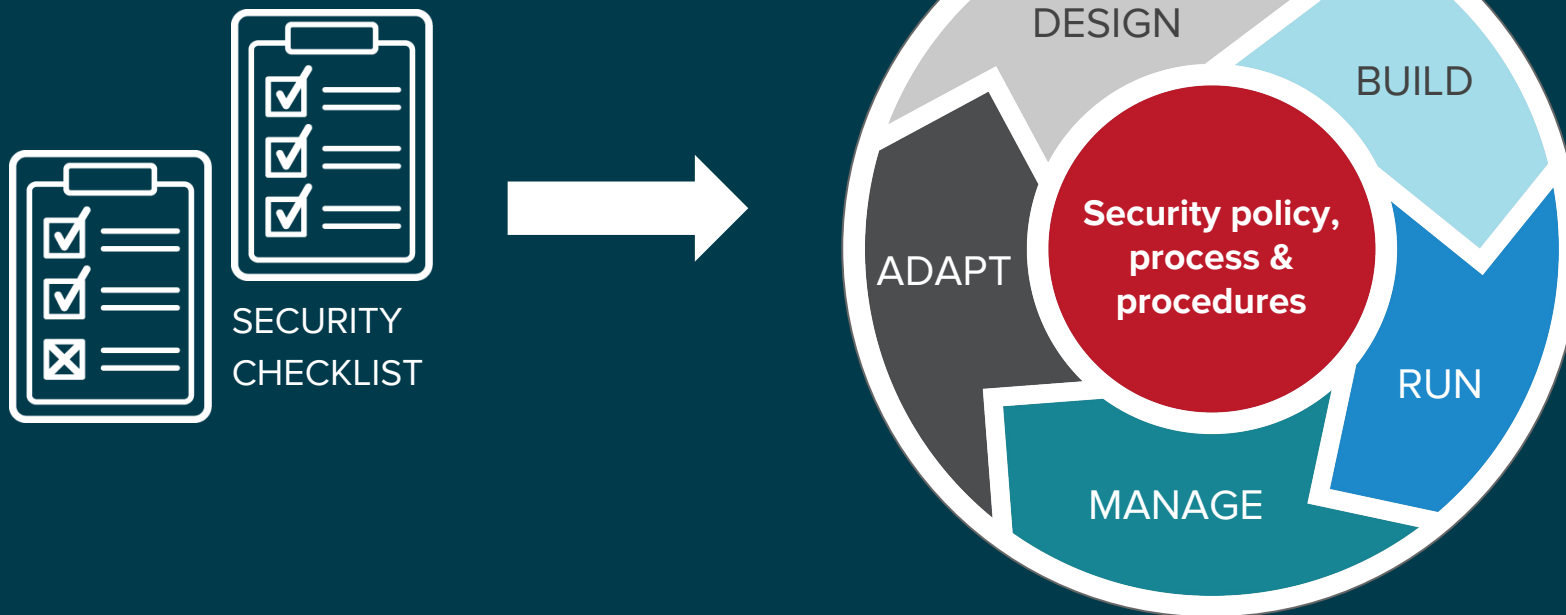
What are you organization's top priorities around IT cultural or process changes?*



Compliance and governance remain a top priority, but agile and DevOps processes have shot to the top of our customers list this year. This is the only way they will achieve innovation at the speed they need to compete and win.

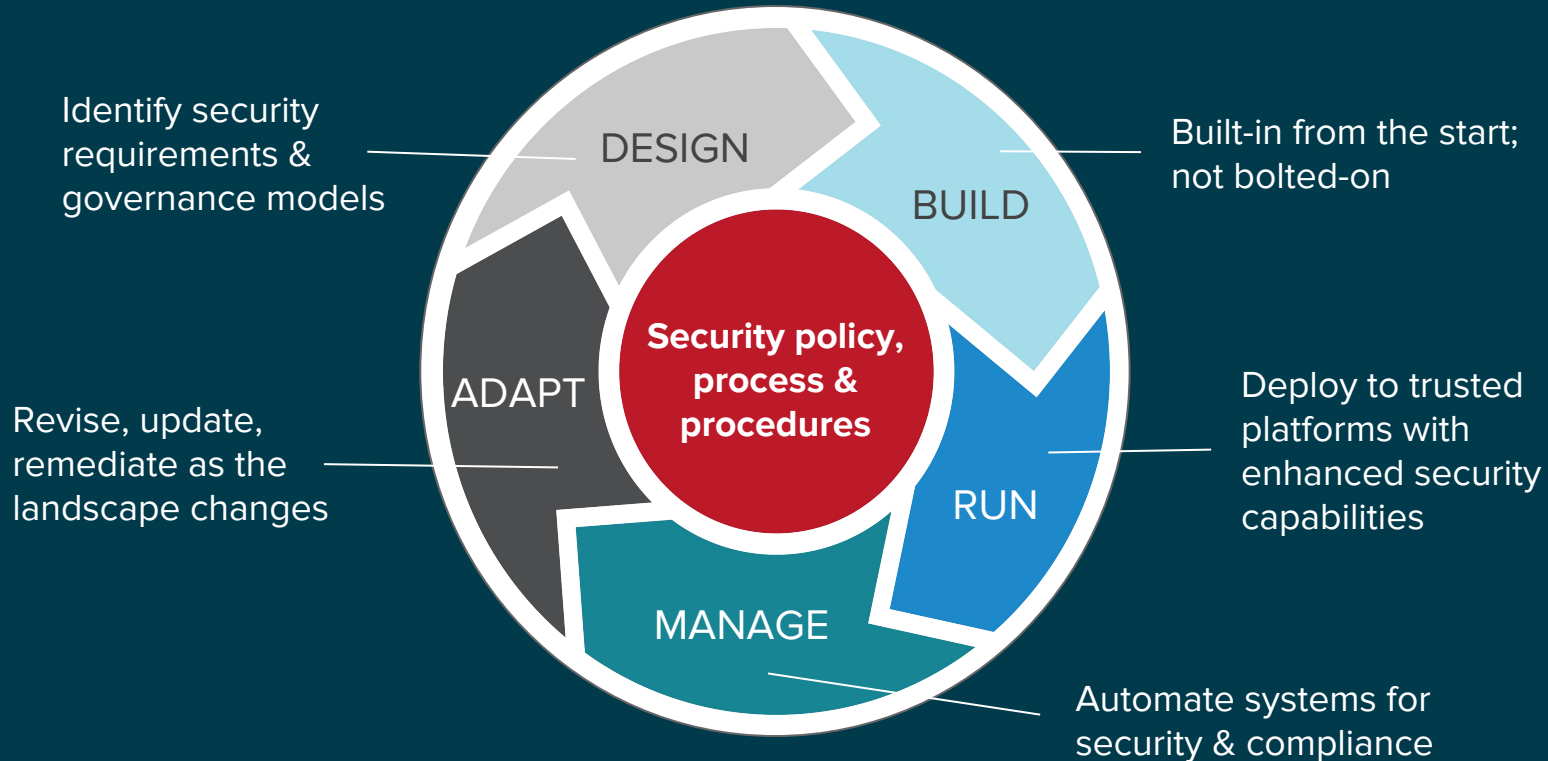
*Select all that apply

SECURITY MUST EVOLVE

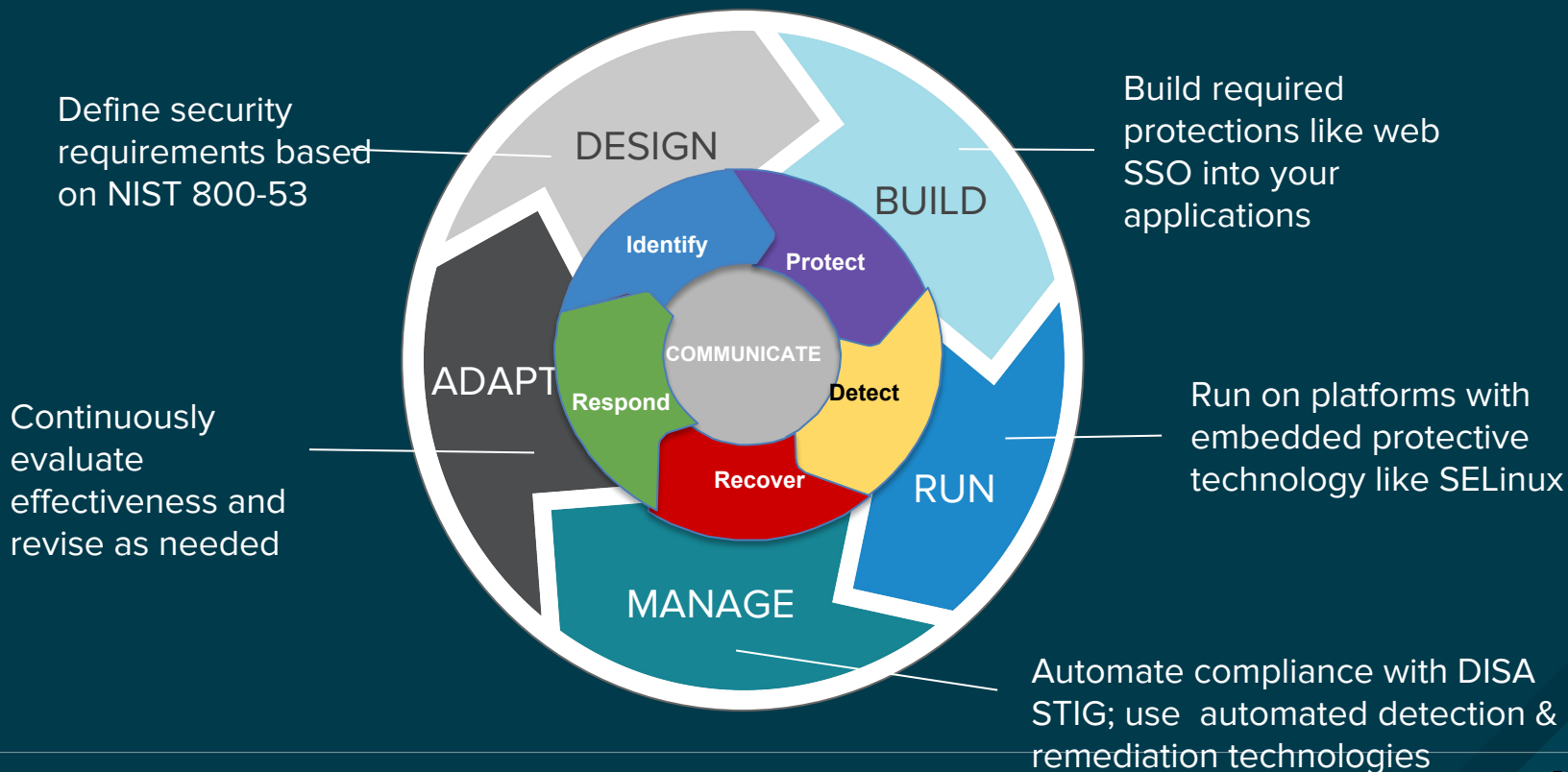


SECURITY MUST BE CONTINUOUS

And integrated throughout the IT lifecycle



CONTINUOUS SECURITY WITH NIST



Risk Management

The objectives of risk management are to identify, address, and eliminate software risk items before they become either threats to successful software operation or major sources of software rework.

Barry W Boehm

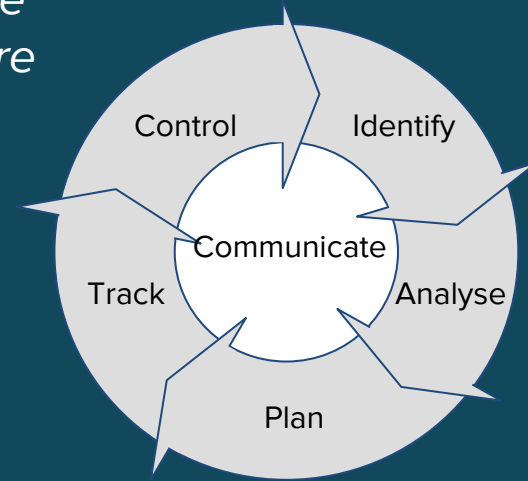
Approaches to dealing with risk:

- Reduction - reduce likelihood

- Protection - bottom-up prevention

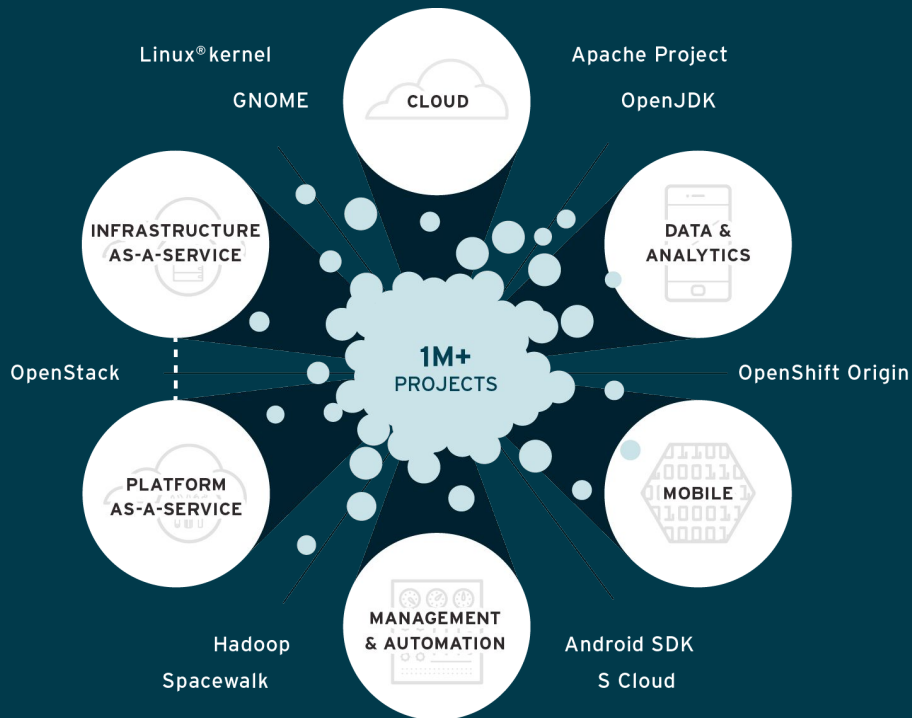
- Transfer - let someone else share or hold

- Pecuniary - set aside contingency fund of resources

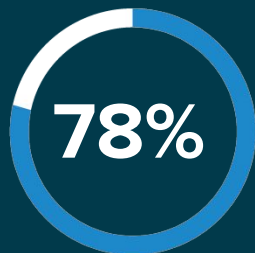


WHY OPEN SOURCE?

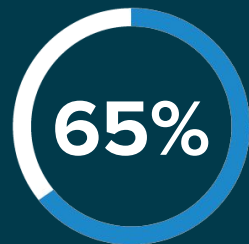
OPEN SOURCE DEVELOPMENT DRIVES RAPID INNOVATION



OPEN SOURCE ADOPTION...SOARING



of enterprises run open source. ^[1]

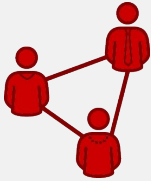


of companies are contributing to open software. ^[2]

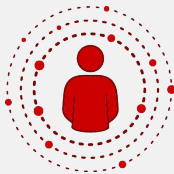
[1] Black Duck Software, [9th Annual Future of Open Source survey](http://www.blackducksoftware.com/2015-future-of-open-source), 2015. www.blackducksoftware.com/2015-future-of-open-source

[2] Black Duck Software, [10th Annual Future of Open Source survey](http://www.blackducksoftware.com/2016-future-of-open-source), 2016. www.blackducksoftware.com/2016-future-of-open-source

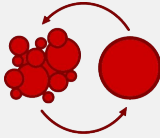
OPEN SOURCE CULTURE



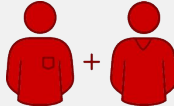
Collaboration



Transparency
(both access and the ability to act)



Shared problems are
solved faster



Working together creates
standardization



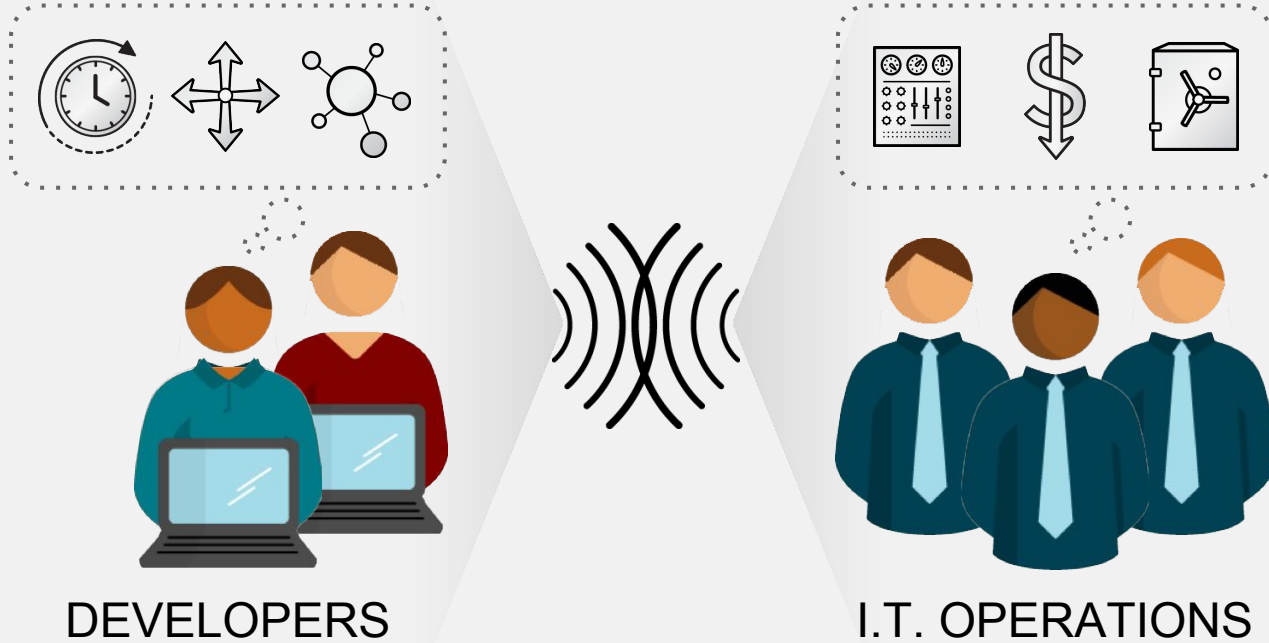
AGILITY, WITH SECURITY

The Problem

Applications require complicated installation and integration every time they are deployed



THE PROBLEM



DEVOPS

Everything as code

Automate everything

Continuous Integration/Delivery

Application is always “releaseable”

Application monitoring

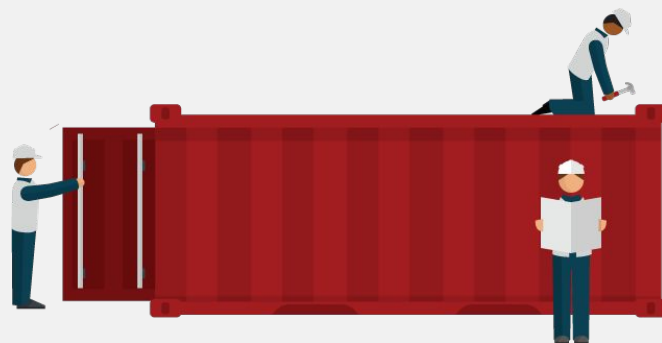
Rapid feedback

Rebuild vs. Repair

Delivery pipeline

A Solution

Adopting a container strategy will allow applications to be easily shared and deployed.



WHAT ARE CONTAINERS?

It Depends Who You Ask

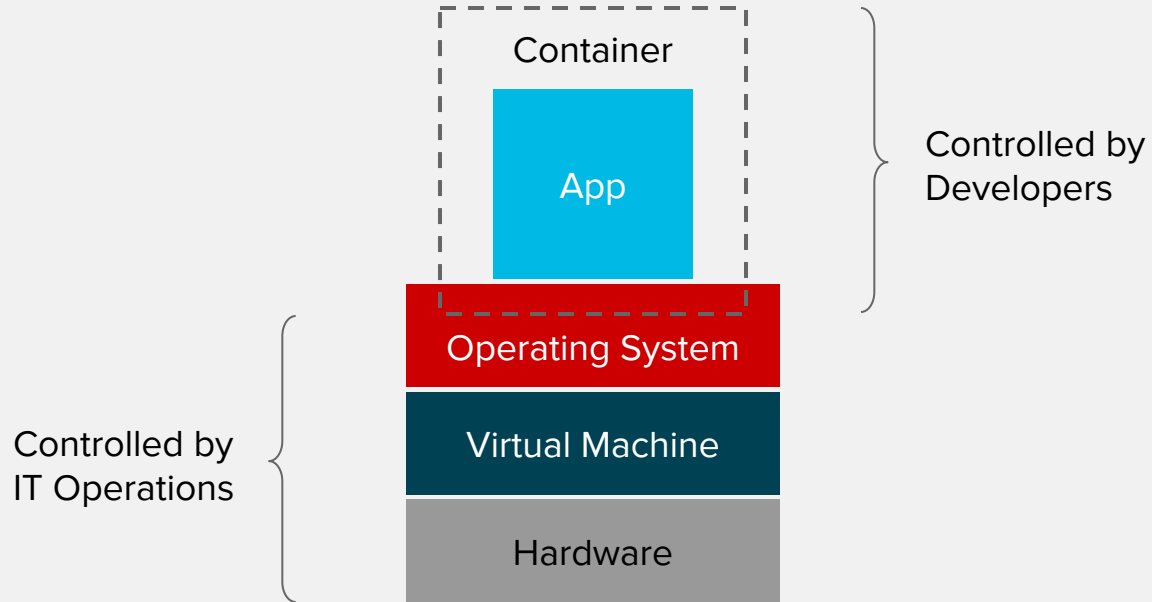
INFRASTRUCTURE

- Sandboxed application processes on a shared Linux OS kernel
- Simpler, lighter, and denser than virtual machines
- Portable across different environments

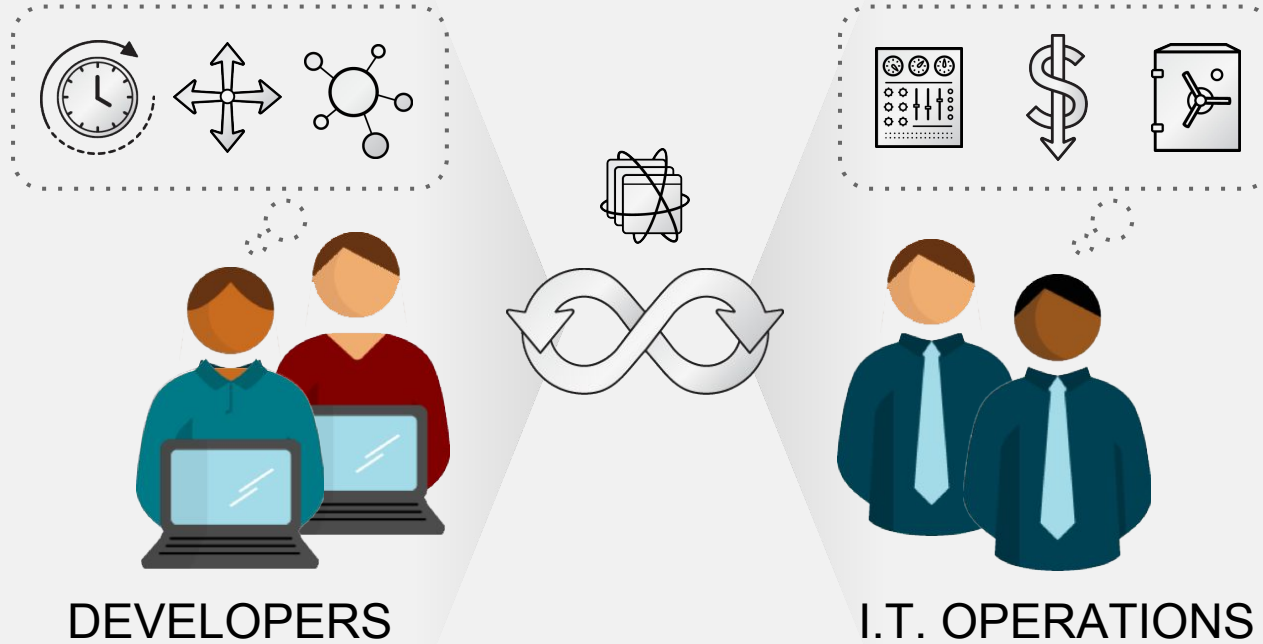
APPLICATIONS

- Package my application and all of its dependencies
- Deploy to any environment in seconds and enable CI/CD
- Easily access and share containerized components

A SOLUTION



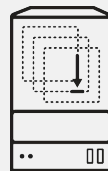
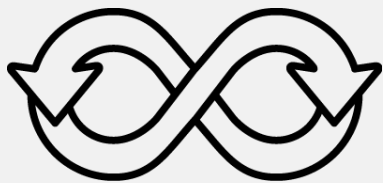
A SOLUTION



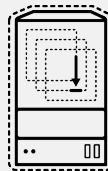

```
$ docker build -t app:v1 .
```

```
$ docker build -t app:v1 .
```

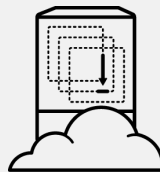
```
$ docker run app:v1
```



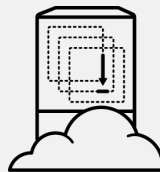
physical



virtual

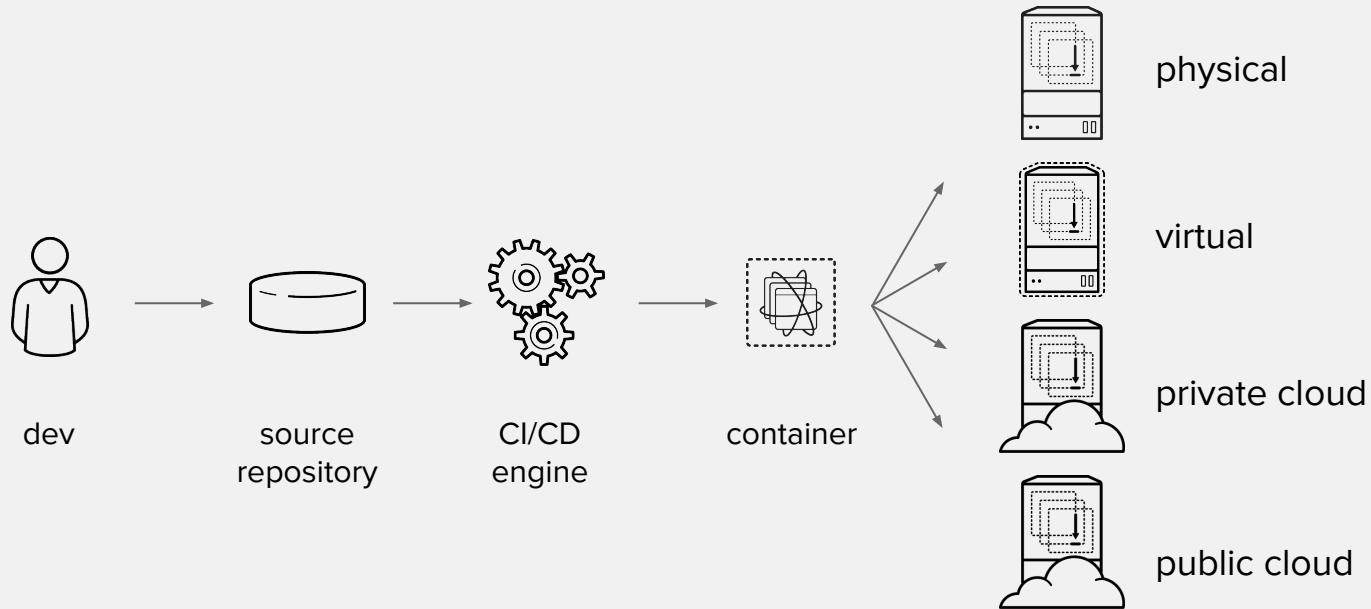


private cloud



public cloud

DEVOPS WITH CONTAINERS

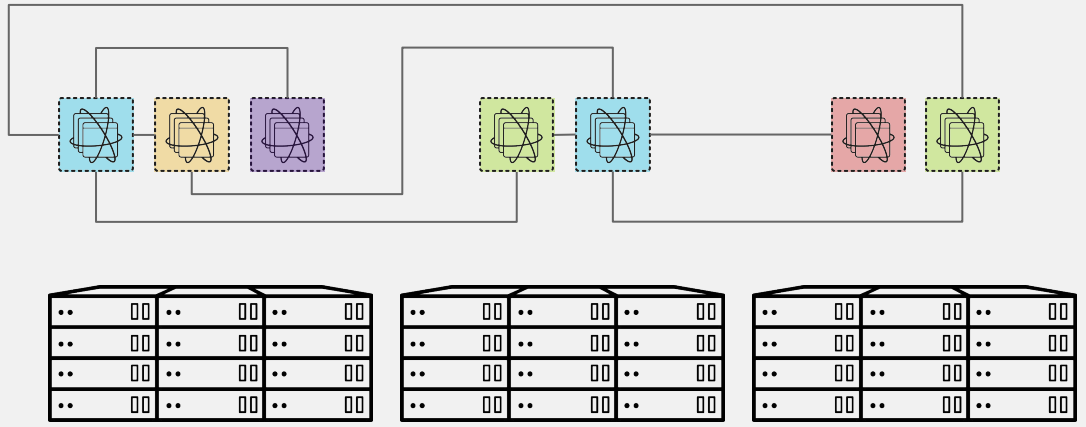
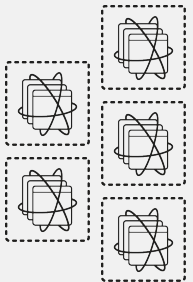




..	00	..	00	..	00
..	00	..	00	..	00
..	00	..	00	..	00
..	00	..	00	..	00

..	00	..	00	..	00
..	00	..	00	..	00
..	00	..	00	..	00
..	00	..	00	..	00

..	00	..	00	..	00
..	00	..	00	..	00
..	00	..	00	..	00
..	00	..	00	..	00



WE NEED MORE THAN JUST CONTAINERS

Scheduling

Decide where to deploy containers

Security

Control who can do what

Lifecycle and health

Keep containers running despite failures

Scaling

Scale containers up and down

Discovery

Find other containers on the network

Persistence

Survive data beyond container lifecycle

Monitoring

Visibility into running containers

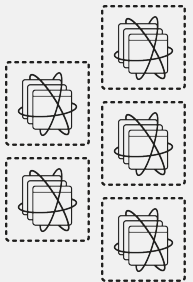
Aggregation

Compose apps from multiple containers

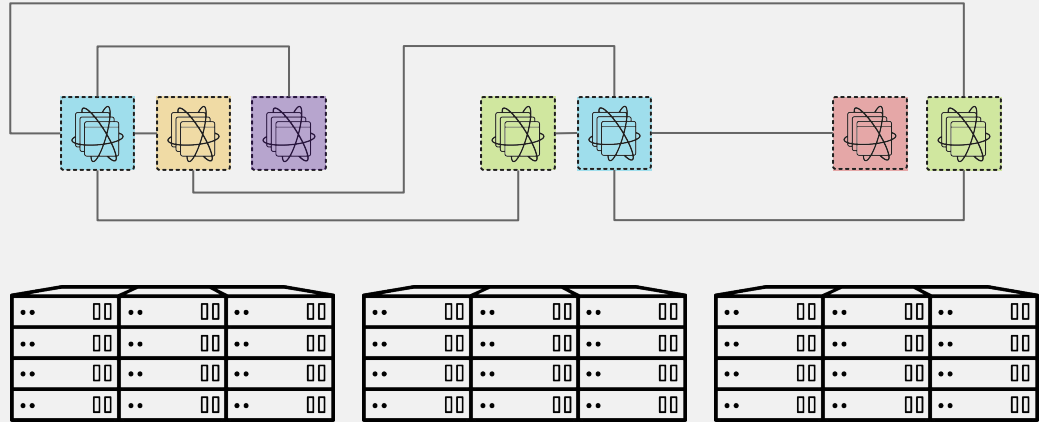
Kubernetes is an open-source system for automating deployment, operations, and scaling of containerized applications across multiple hosts



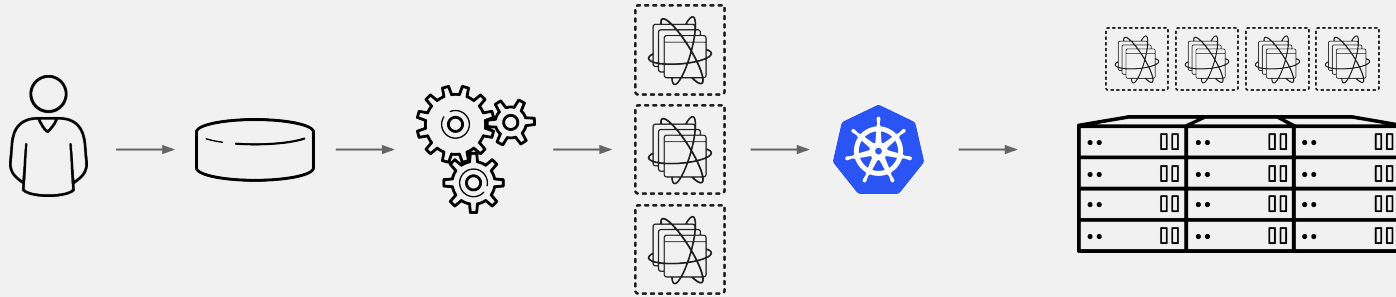
kubernetes



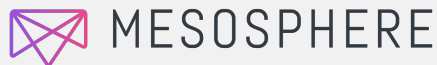
kubernetes



DEVOPS WITH CONTAINERS AND KUBERNETES



INDUSTRY CONVERGING ON KUBERNETES



INDUSTRY CONVERGING ON KUBERNETES

CSRA Achieves Highest Cloud Services Security Accreditation



[Home](#) > [Media Room](#) > [Multimedia Library](#) > [CSRA Achieves Highest Cloud Services Security Accreditation](#)

June 23, 2016

RELATED

[Digital Platforms / Digital Services / Amazon Web Services / Microsoft / FedRAMP FISMA High Baseline Accreditation](#)

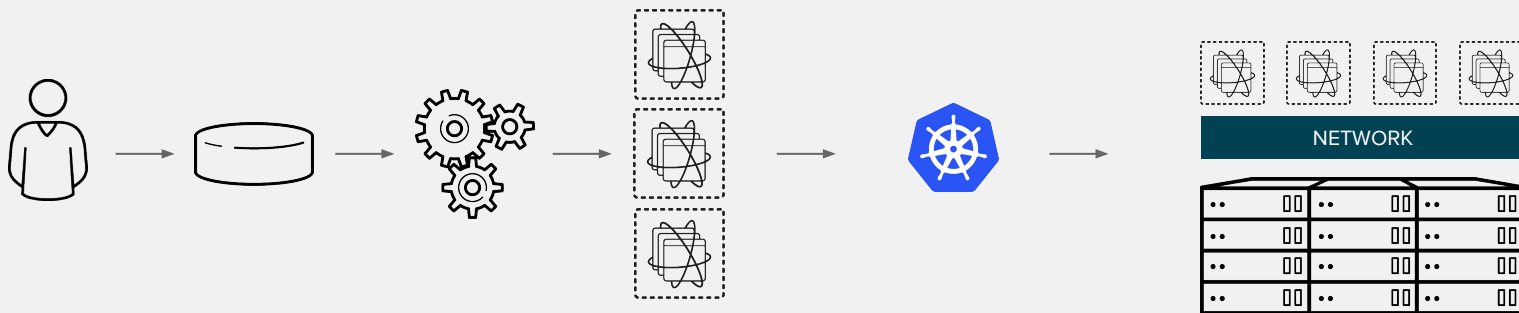
COLLECTIONS

[Cloud Integrated Technology Center](#)

CSRA, Amazon Web Services and Microsoft Azure Earn FedRAMP FISMA High Baseline Authority to Operate

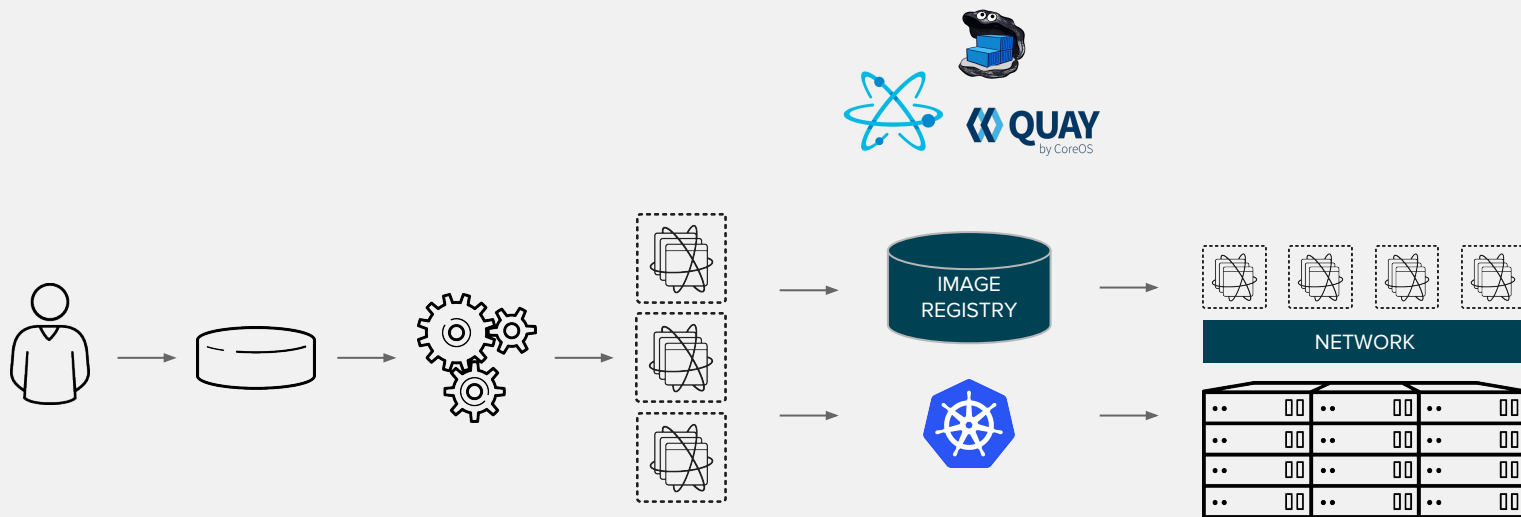
Falls Church, Va., June 23, 2016 – CSRA Inc. (NYSE:CSRA), a leading provider of next-generation IT solutions and professional services to government organizations, today announced its operating subsidiary, CSRA LLC (formerly CSC Government Solutions LLC), is one of three cloud service providers, including Amazon Web Services and Microsoft Azure to meet rigorous security standards and achieve a Federal Risk Authorization Management Program (FedRAMP) Federal Information Security Management (FISMA) High Baseline accreditation.

DEVOPS WITH CONTAINERS AND KUBERNETES



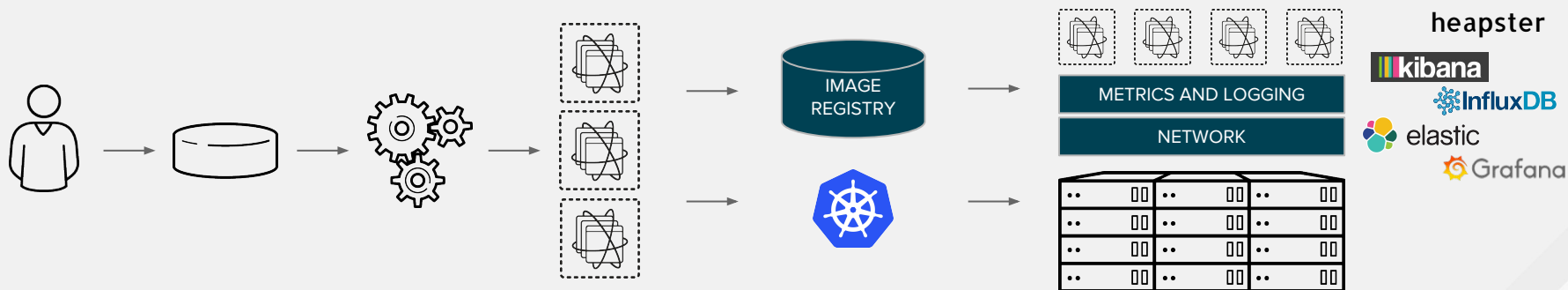
Not enough! Need networking

DEVOPS WITH CONTAINERS AND KUBERNETES



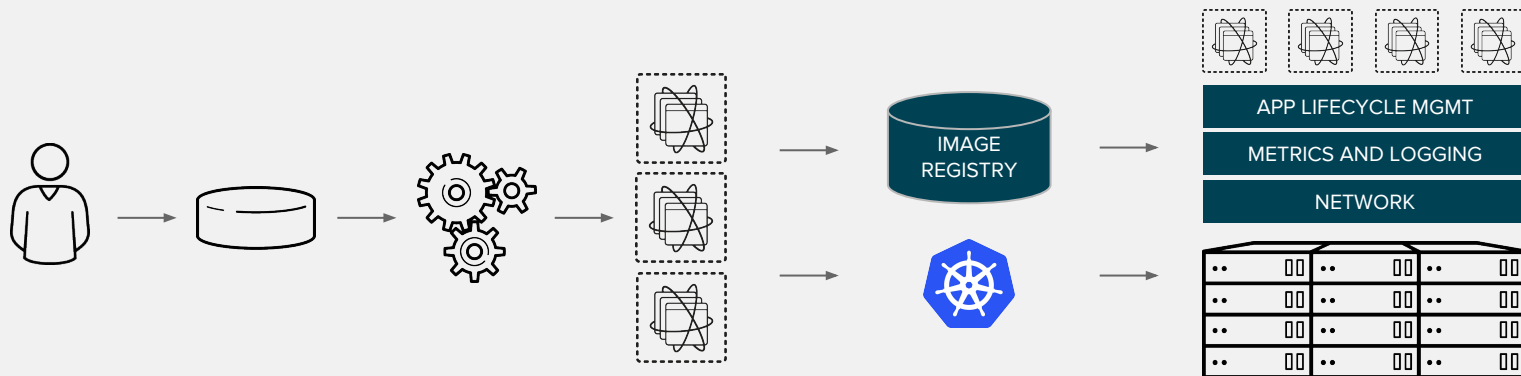
Not enough! Need an image registry

DEVOPS WITH CONTAINERS AND KUBERNETES



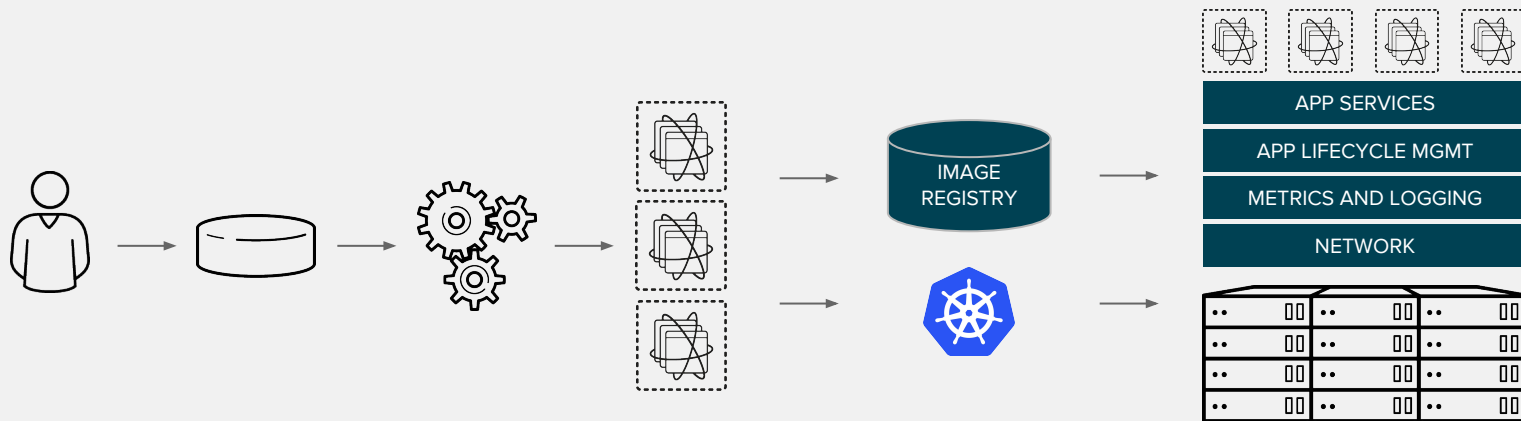
Not enough! Need metrics and logging

DEVOPS WITH CONTAINERS AND KUBERNETES



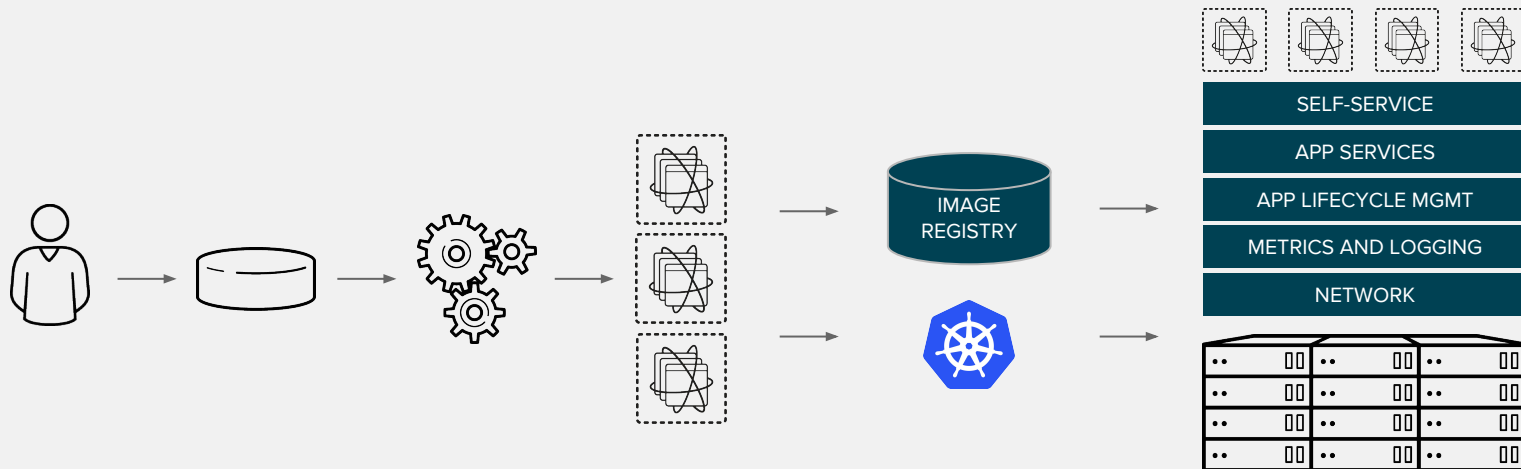
Not enough! Need application lifecycle management

DEVOPS WITH CONTAINERS AND KUBERNETES



Not enough! Need application services e.g. database and messaging

DEVOPS WITH CONTAINERS AND KUBERNETES



Not enough! Need self-service portal

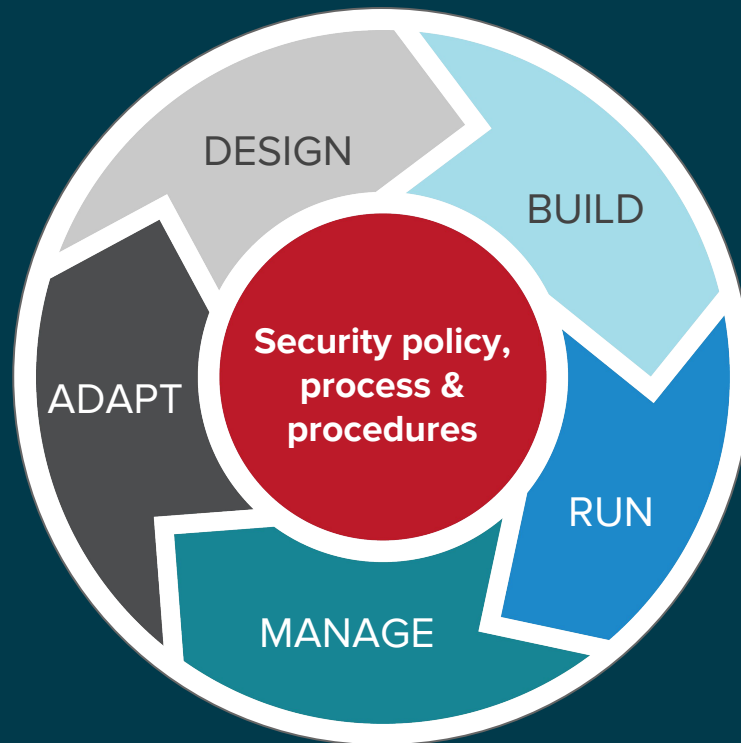
NOT ENOUGH, THERE IS MORE!

Multi-tenancy	Teams and Collaboration
Routing & Load Balancing	Quota Management
CI/CD Pipelines	Image Build Automation
Role-based Authorization	Container Isolation
Capacity Management	Vulnerability Scanning
Infrastructure Visibility	Chargeback

Container application
platform based on Docker
and Kubernetes for building,
distributing and running
containers at scale



REMEMBER THIS?



OpenShift for Government Accreditations & Standards

**OCTOBER
2016**

RHEL7 COMMON CRITERIA

- EAL4+
- Container Framework
- Secure Multi-tenancy

**DECEMBER
2016**

RHEL7 FIPS 140-2 CERTIFIED

- Data at Rest
- Data in Transport

**MARCH
2017**

INDUSTRY FIRST: NIST
CERTIFIED CONFIGURATION AND
VULNERABILITY SCANNER FOR
CONTAINER

JUNE 2017

OPENSIFT BLUEPRINT FOR
AZURE
(FedRAMP MODERATE)

WANT TO HEAR MORE?

2:30 - 3:20PM ET/11:20AM - 12:20PM PT - SESSION 4: CHANGING THE OPEN HYBRID CLOUD GAME

Shawn Wells, Chief Security Strategist, U.S. Public Sector, Red Hat
Harold Wong, Technical Evangelist, Microsoft

As government agencies increasingly look to adopt DevOps, public cloud computing, and Linux containers, building the underlying infrastructure on a trusted and secure foundation is critical. Building secure environments and ensuring adherence to FedRAMP authorization requirements can be complex and cumbersome.

Red Hat's OpenShift Container Platform provides a secure, government-ready platform for containers and DevOps. Microsoft and Red Hat teamed up to provide architectural guidance on deploying Red Hat OpenShift Container Platform in Azure Government, which is a hybrid cloud solution. This collaboration has created detailed reference architectures, Ansible playbooks, and template system security plans.

This session will show how to deploy Red Hat OpenShift Container Platform into Azure using the architectural guidance as well as the steps necessary to help meet FedRAMP certification.

TRIED. TESTED. TRUSTED.

100%

of airlines in the Fortune Global 500 rely on Red Hat



100%

of telcos in the Fortune Global 500 rely on Red Hat



100%

of healthcare companies in the Fortune Global 500 rely on Red Hat



100%

of commercial banks in the Fortune 500 rely on Red Hat



100%

of U.S. executive departments rely on Red Hat





THANK YOU



plus.google.com/+RedHat



facebook.com/redhatinc



linkedin.com/company/red-hat



twitter.com/RedHatNews



youtube.com/user/RedHatVideos