

A Security State of Mind: Container Security

Chris Van Tuin
Chief Technologist, West
cvantuin@redhat.com



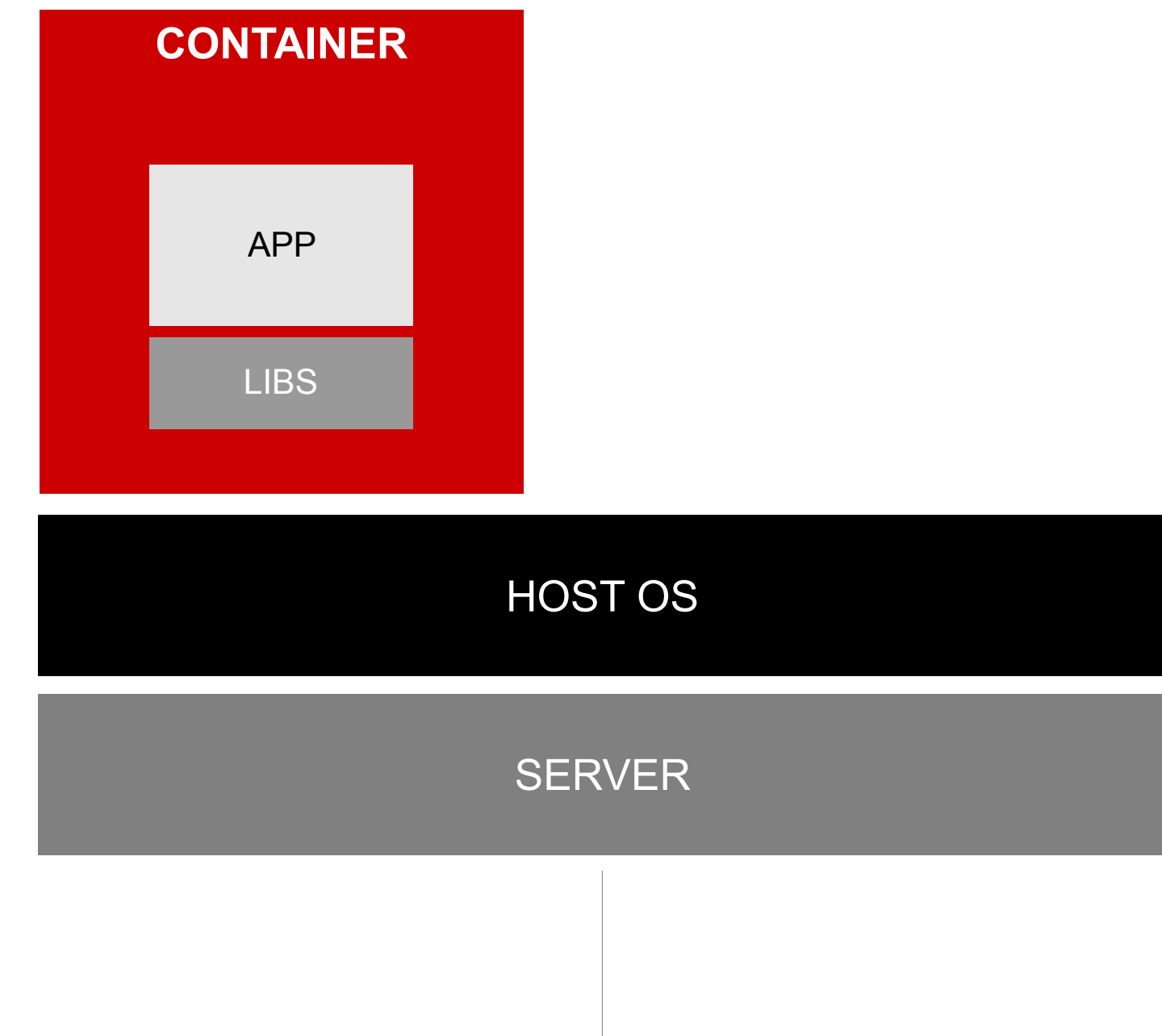
AGENDA

Why Linux Containers?

What are Linux Containers?

Container Security

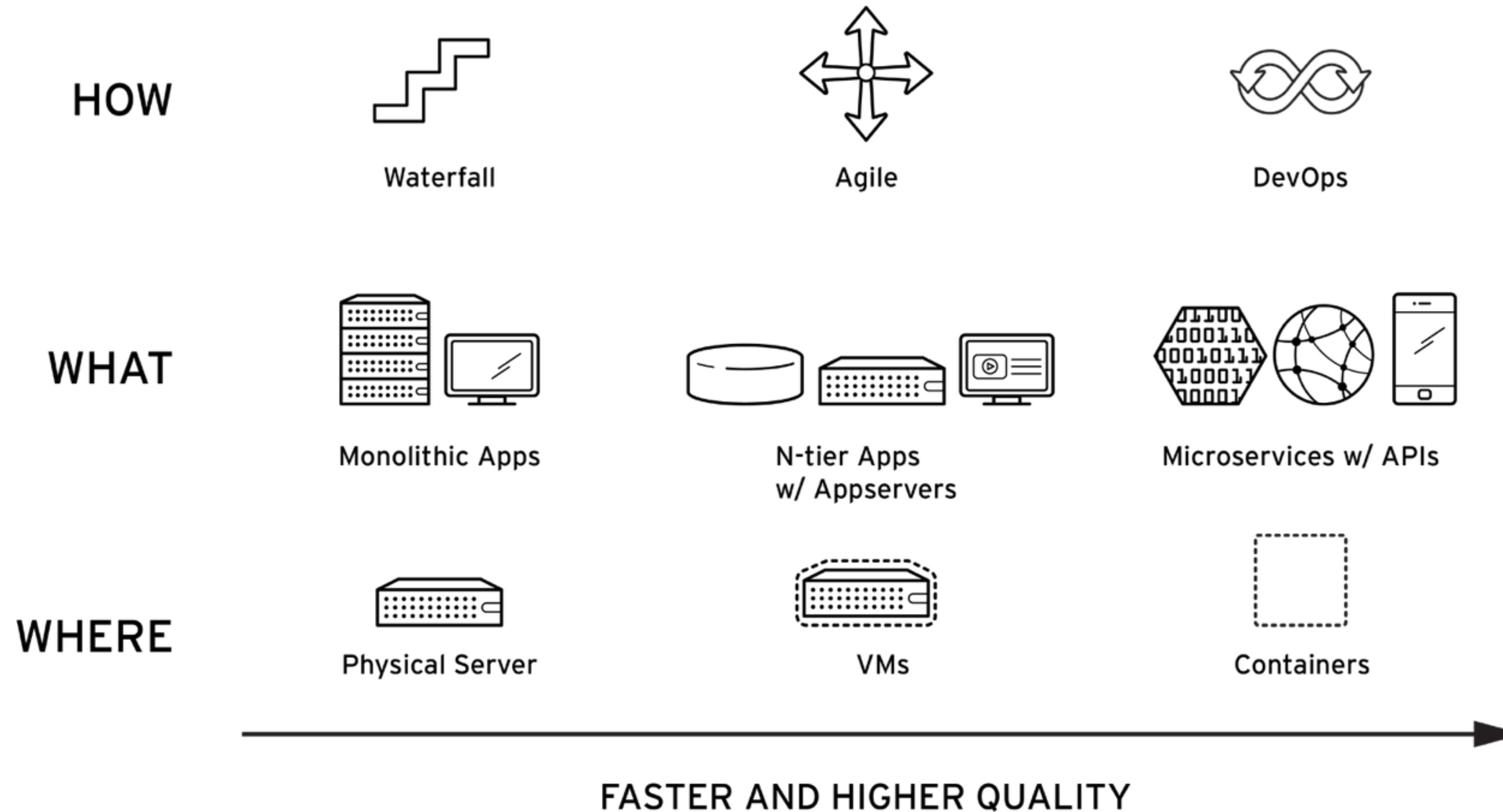
OpenSCAP



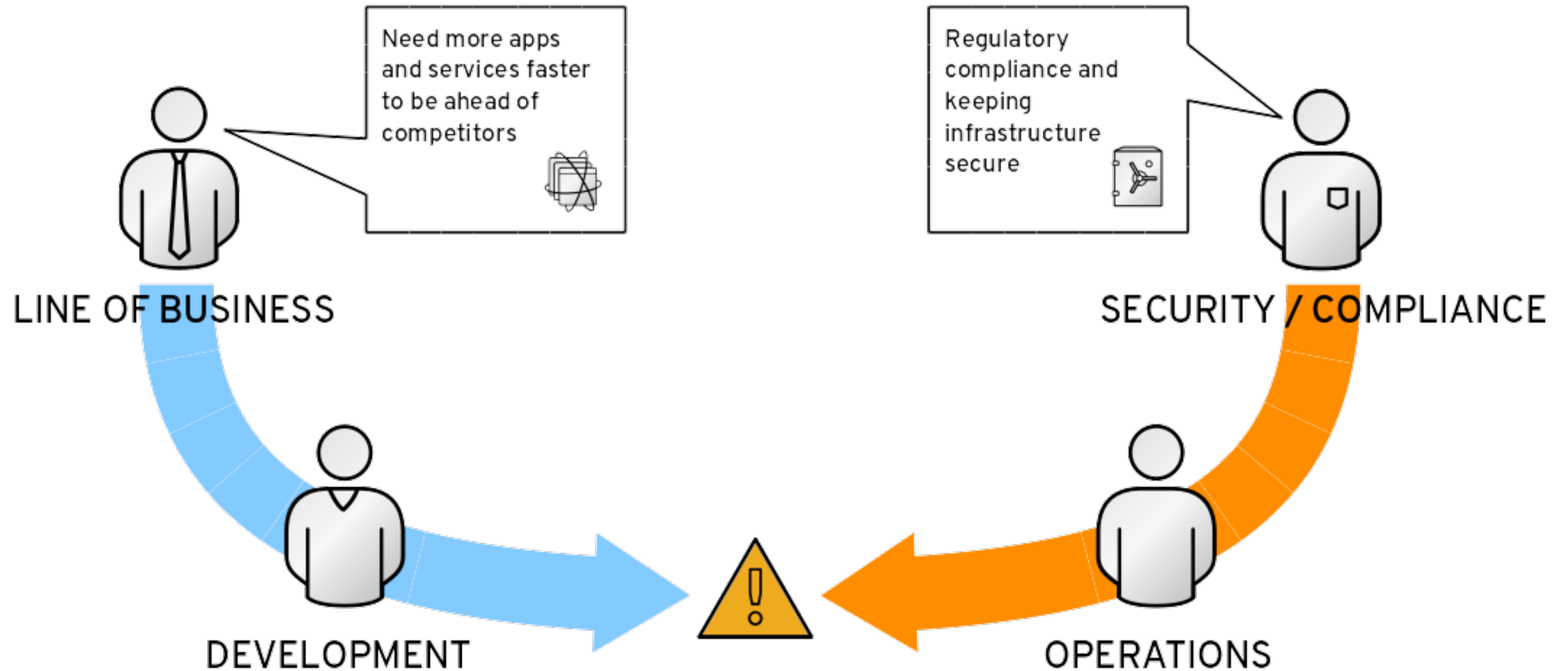


THE NEED FOR SPEED

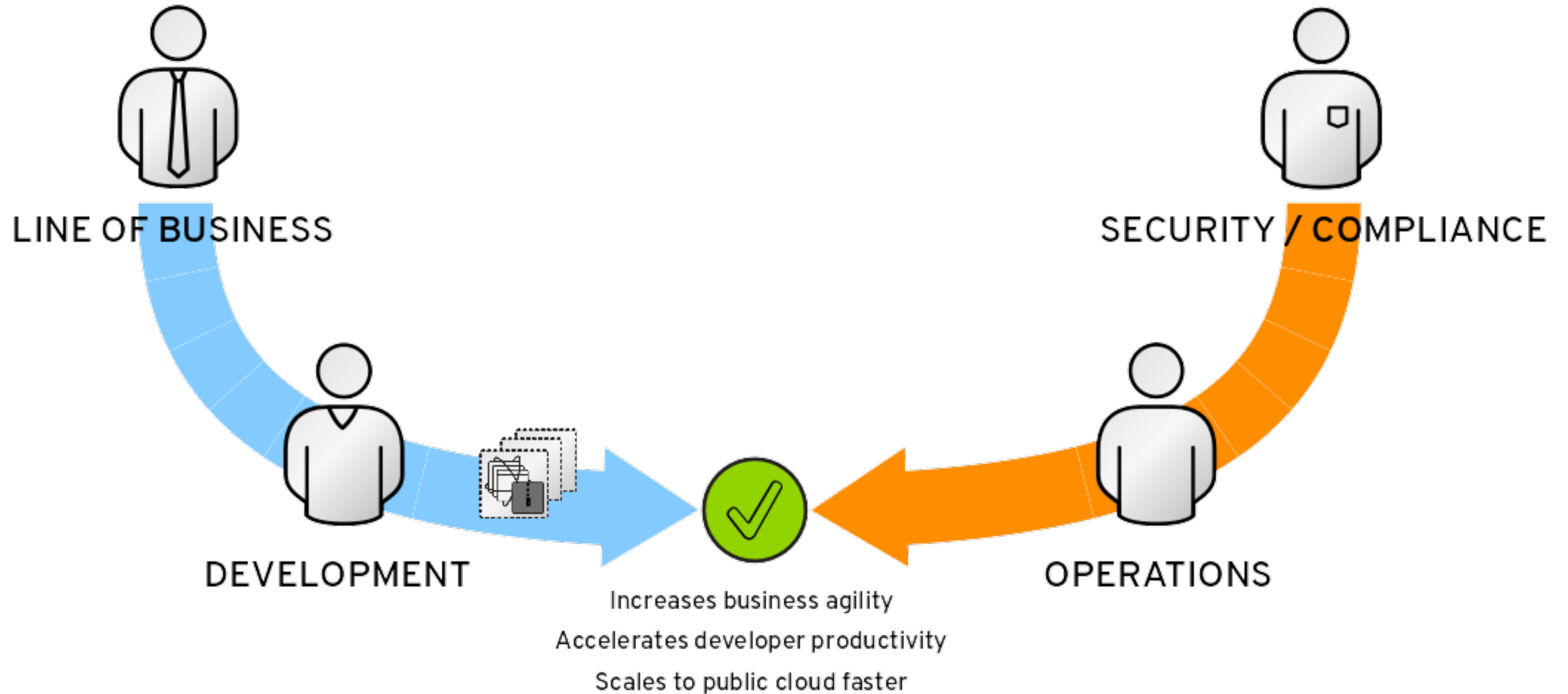
THE ACCELERATION OF APPLICATION DELIVERY FOR THE BUSINESS



THE PROBLEM: FRICTION



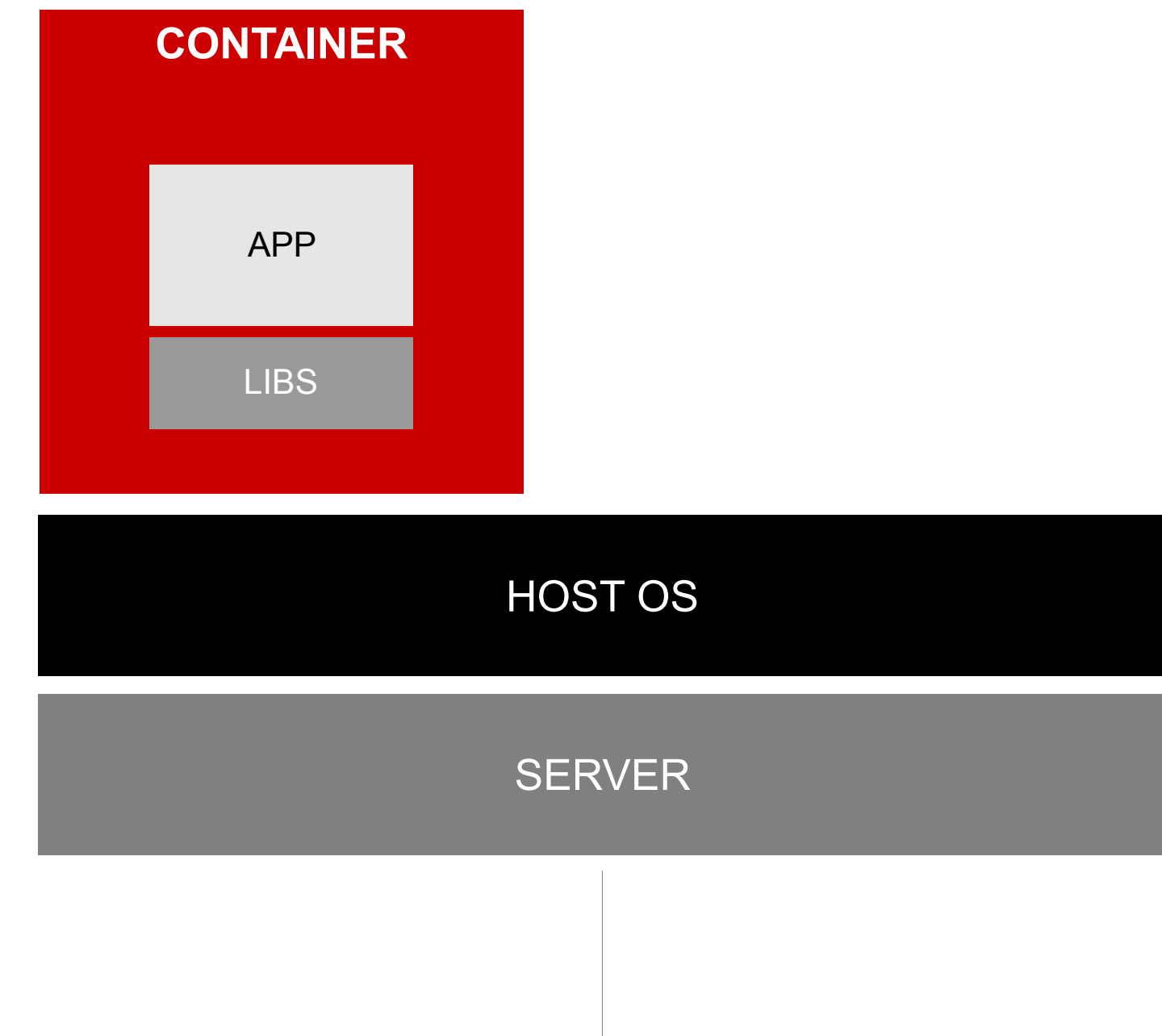
APPLICATION DELIVERY VIA CONTAINERS



LINUX CONTAINERS

WHAT ARE LINUX CONTAINERS?

- Package Once Deploy Anywhere
- Containers provide lightweight isolation of process, network, filesystem spaces
- Docker builds on Linux containers, adds an API, image format, runtime, and a delivery and sharing model



OPEN CONTAINER INITIATIVE

LINUX FOUNDATION COLLABORATIVE PROJECTS



BUILD, SHIP, RUN

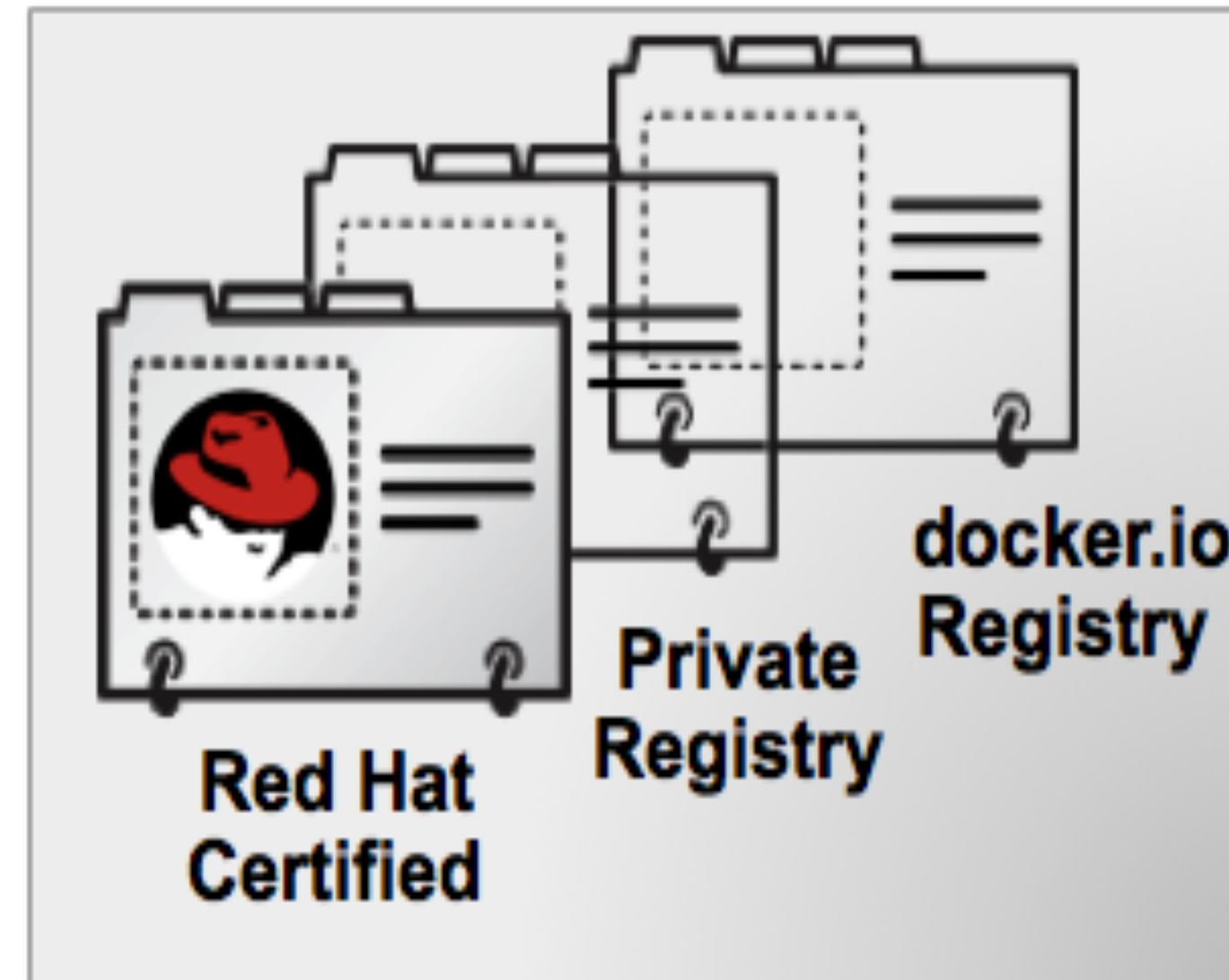
Dockerfile

```
FROM fedora:latest  
CMD echo "Hello"
```

Build

“docker build or commit”

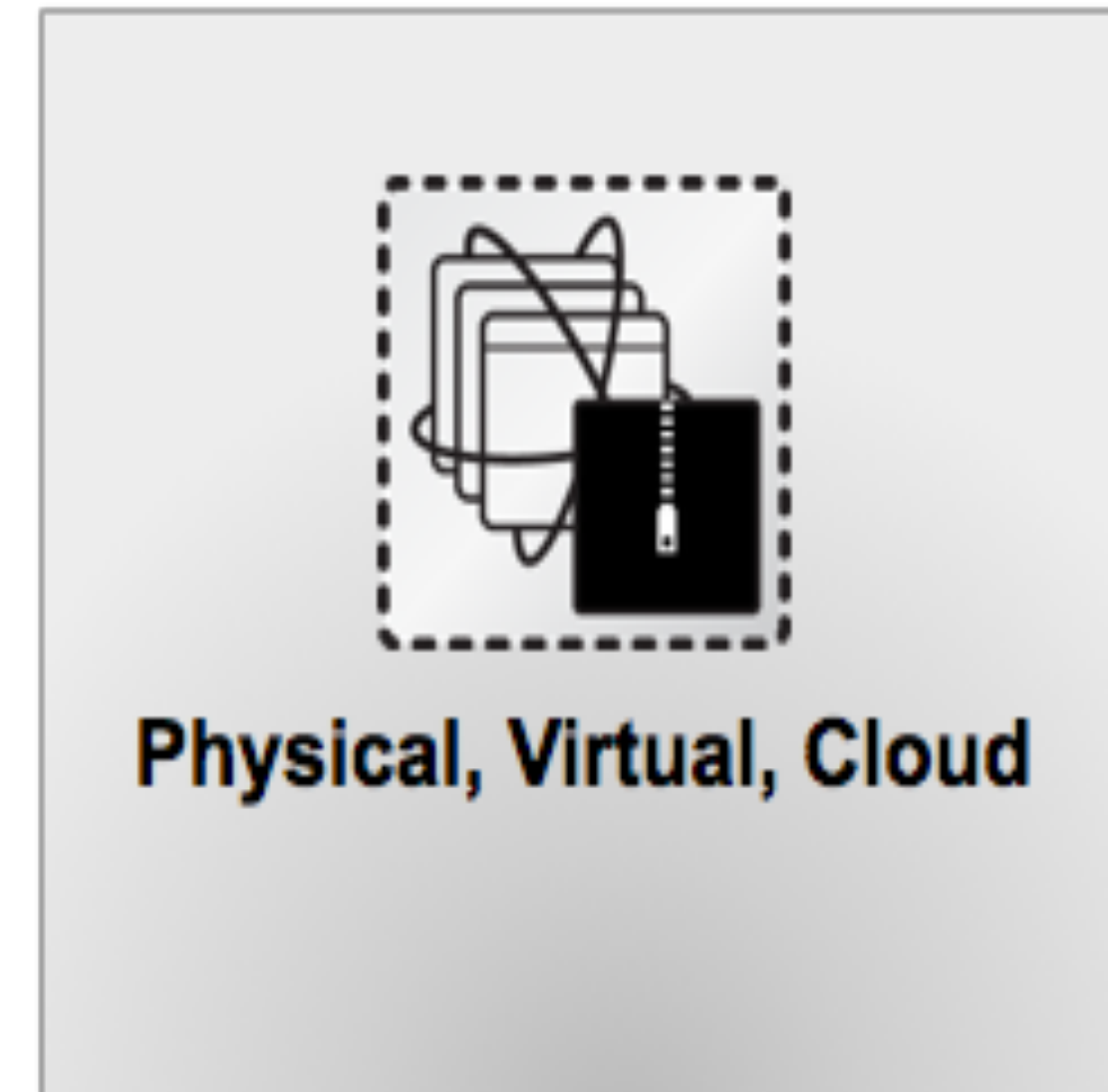
Image



Ship

“docker push or pull
<IMAGE_ID>”

Container

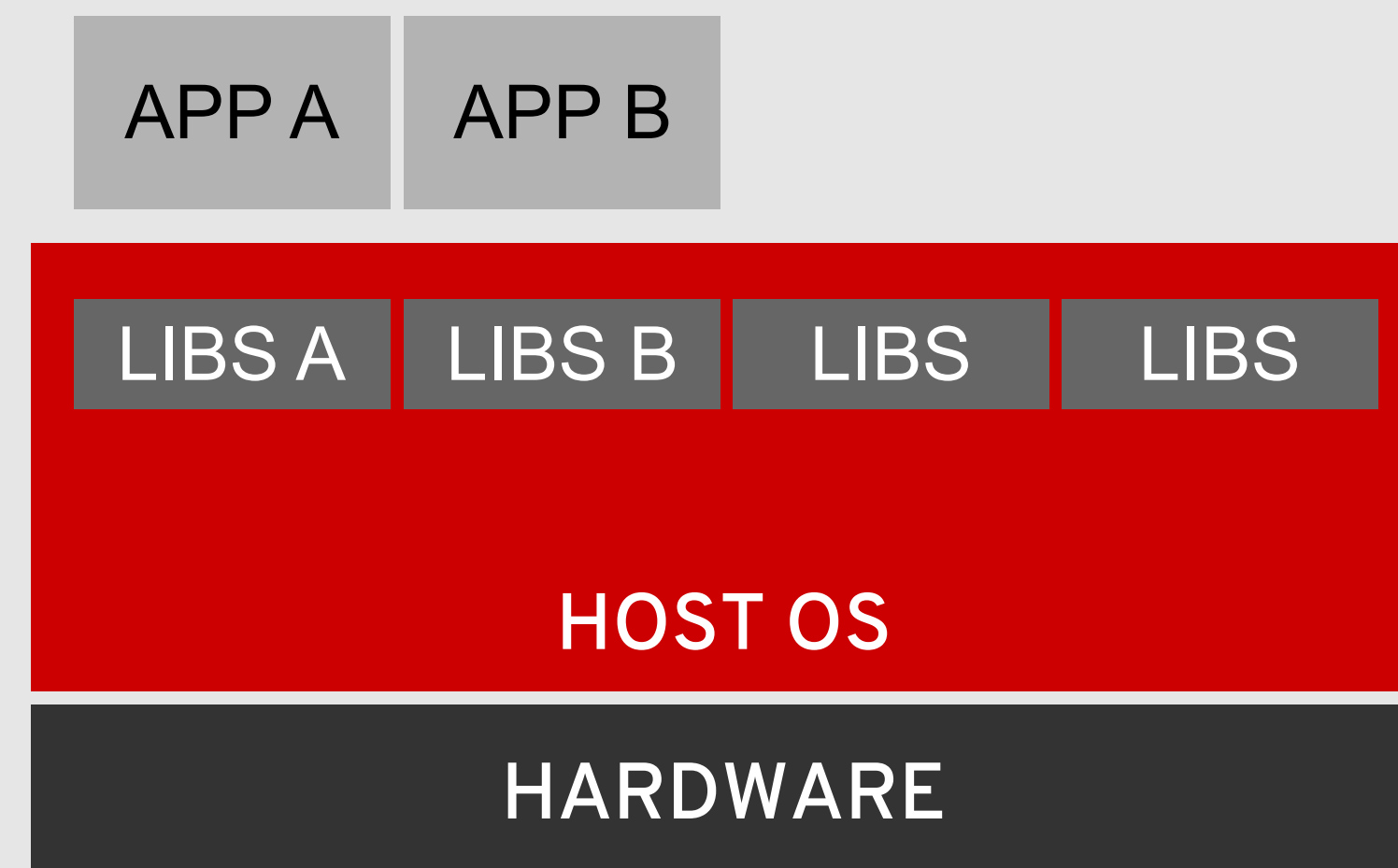


Run

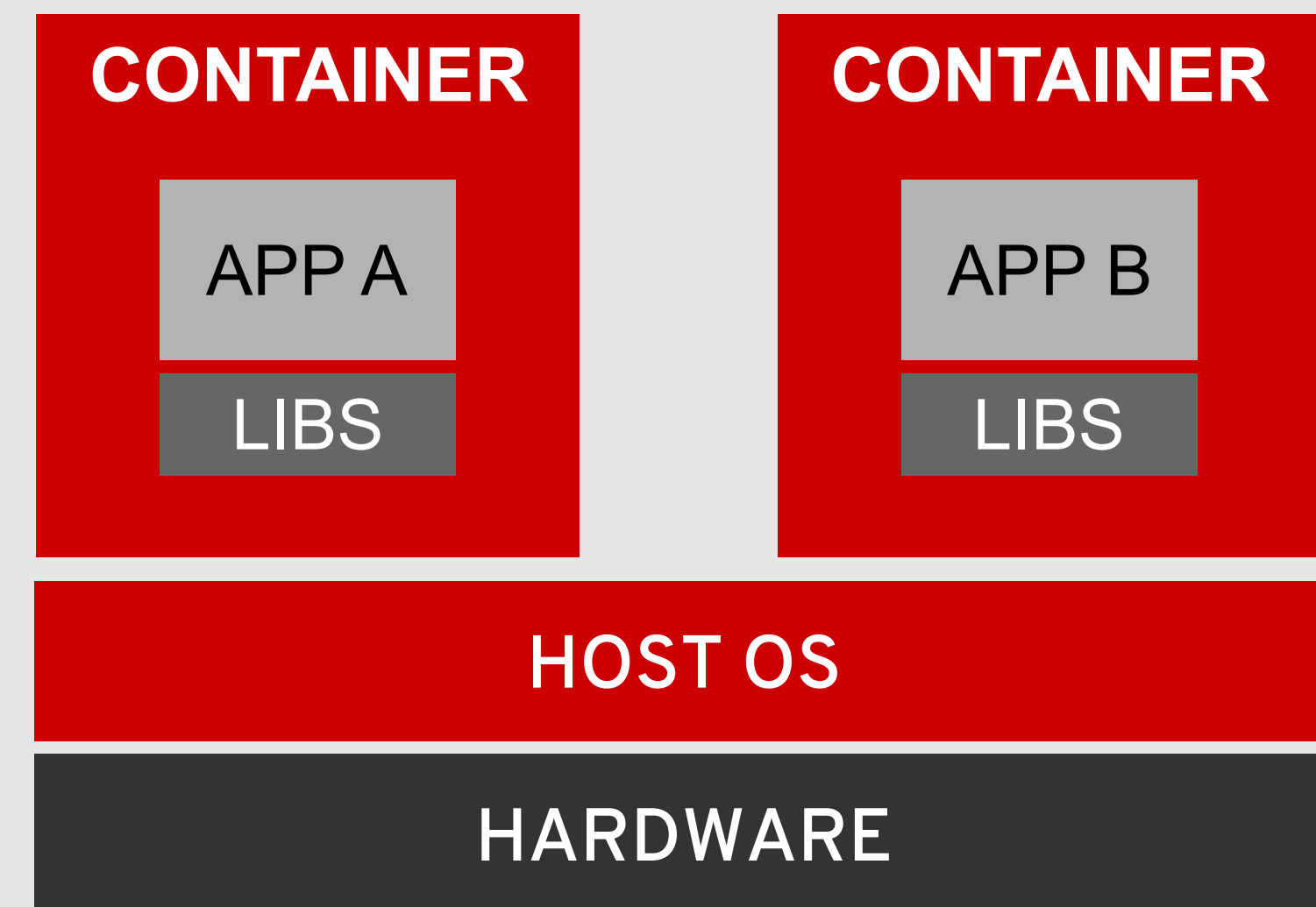
“docker run
<IMAGE_ID>”

TRADITIONAL OS VS CONTAINERS

Traditional OS



Containers



UNDERLYING TECHNOLOGY

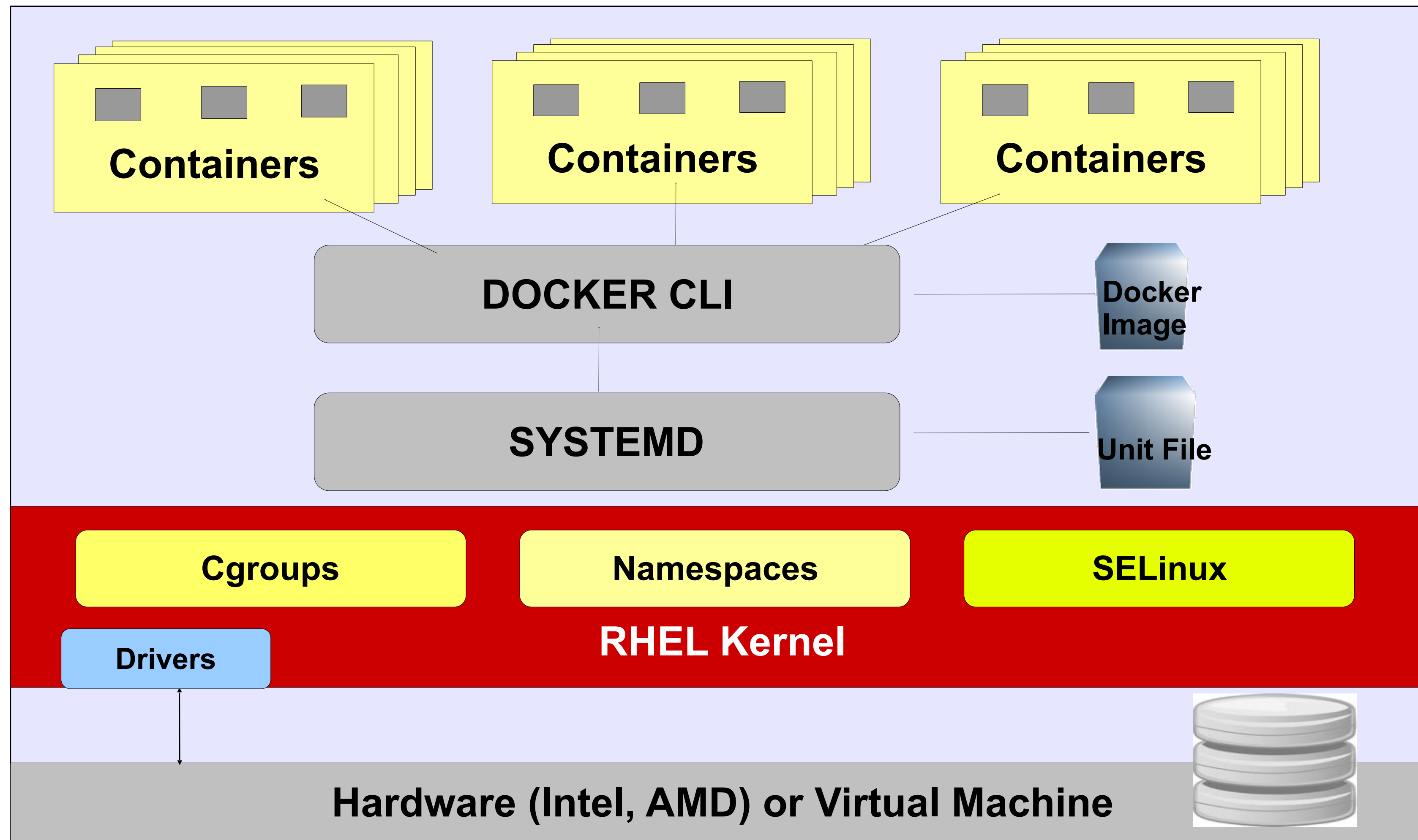
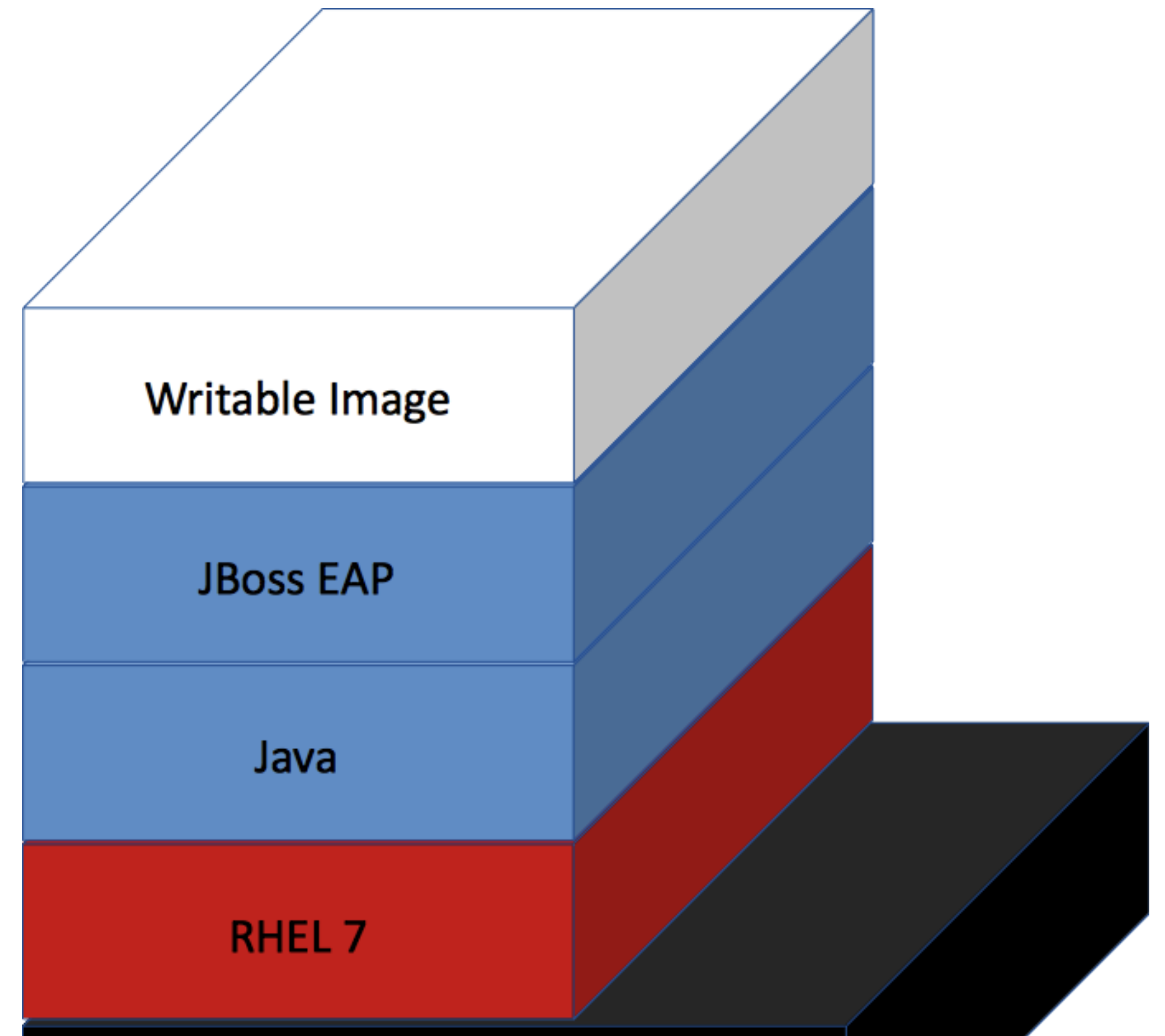


IMAGE-BASED CONTAINERS WITH DOCKER TECHNOLOGY

- Docker container images have layers
- All image layers are read only
- When a container is run the topmost layer is read-write



CONTAINER SECURITY



J.P.Morgan

Neiman Marcus

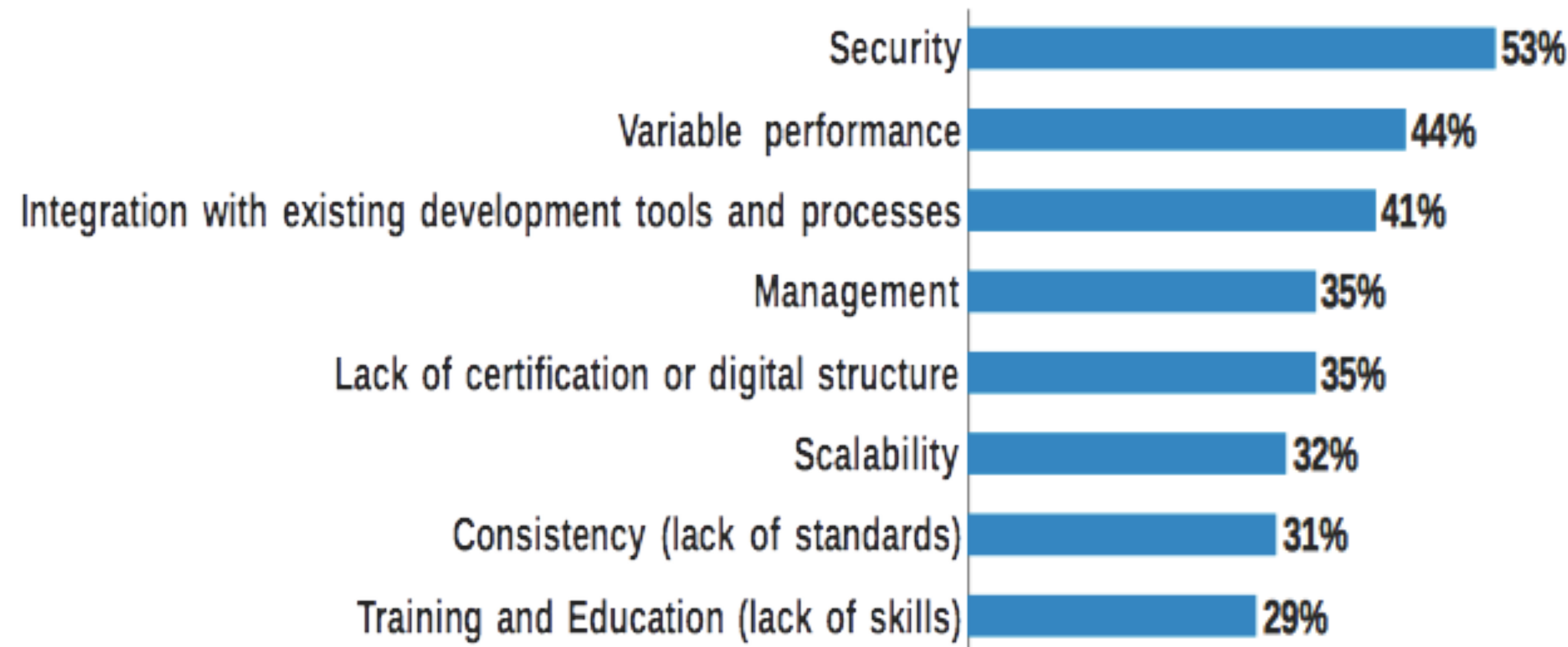


<http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

TOP CURRENT CONTAINER CHALLENGES

■ Total mentions (sum of responses of '1', '2', and '3')

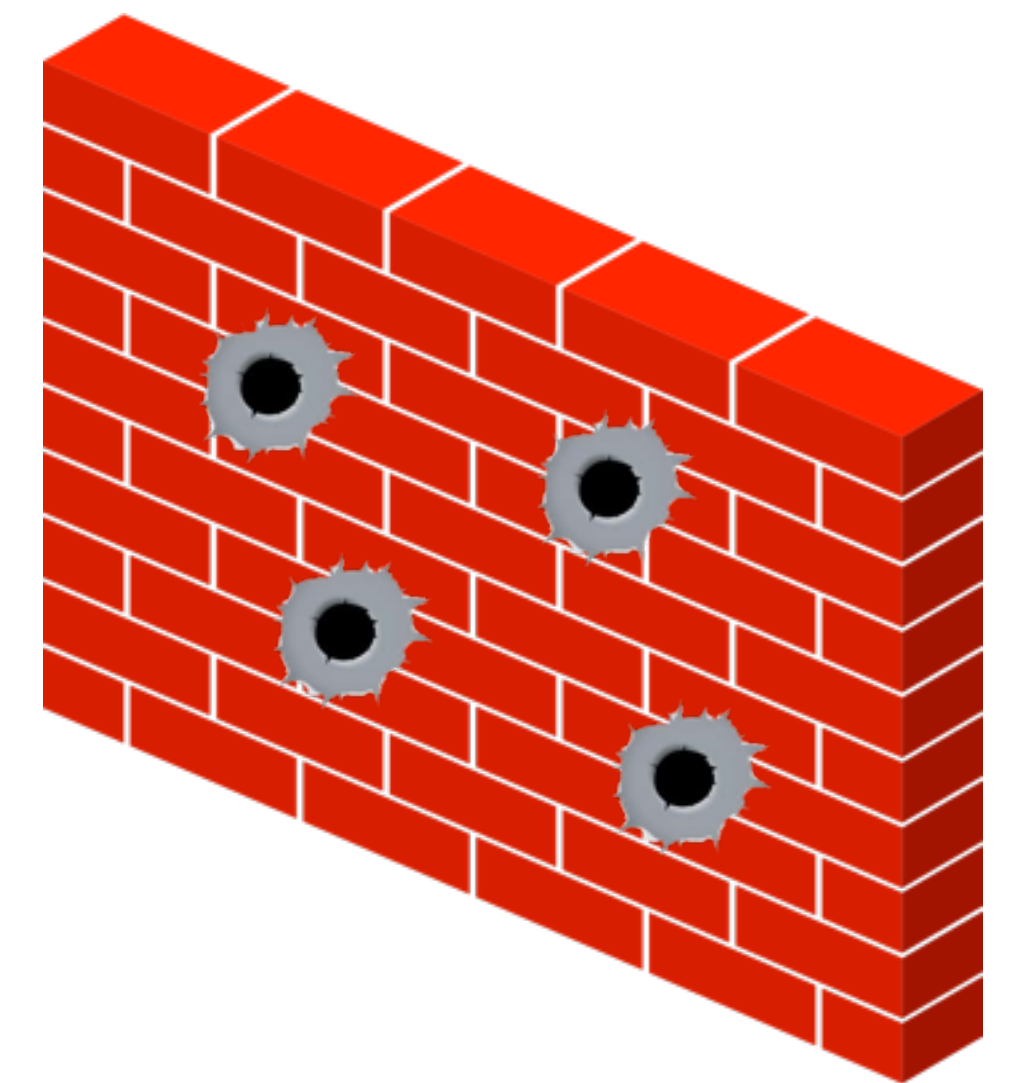
What are the top three challenges your organization has experienced so far in its use of containers?



Base: 171 IT and Developer/programmer decision-makers at companies with 500+ employees in APAC, EMEA, and NA
Source: A commissioned study conducted by Forrester Consulting on behalf of Red Hat, January, 2015

“Patch? The servers are behind the firewall.”

- Anonymous (far too many to name), 2005 - ...

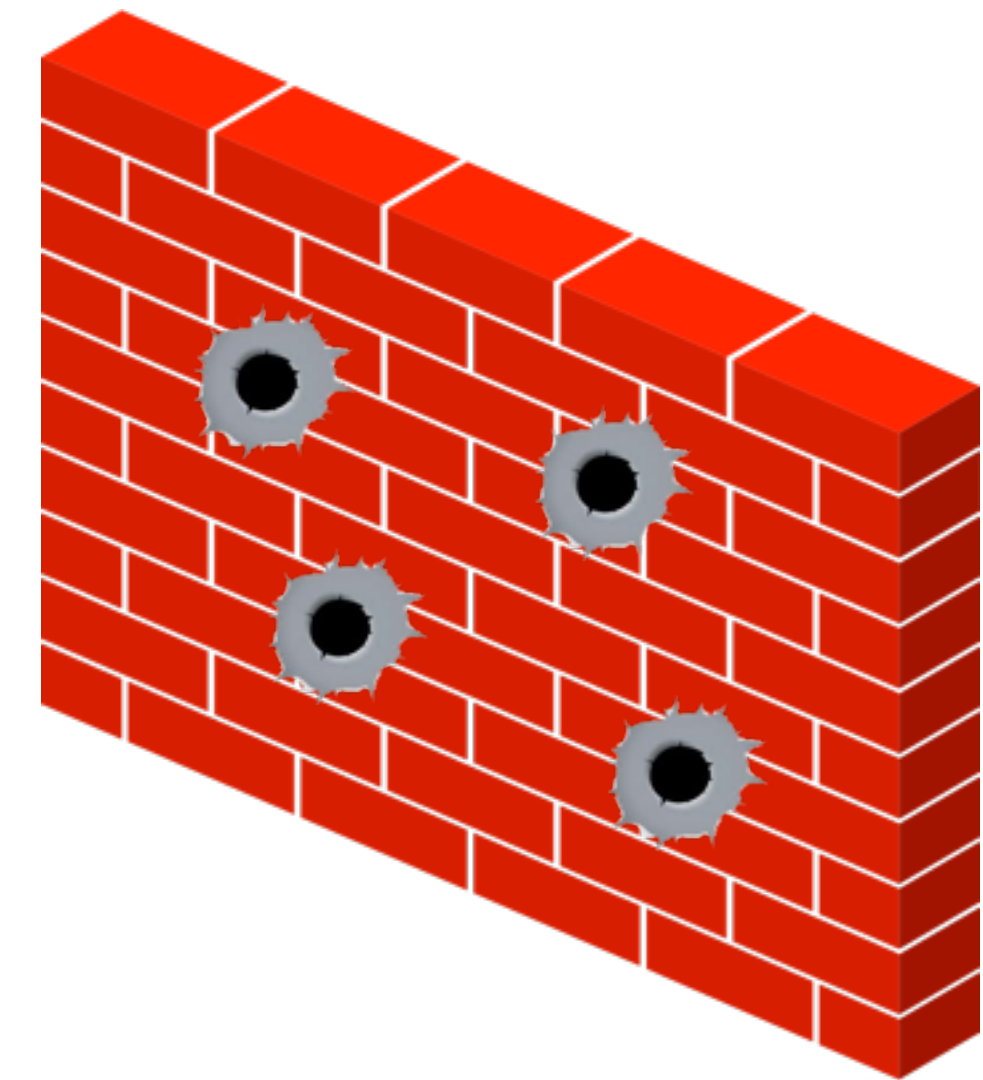


“CONTAINERS DO NOT CONTAIN”

- Dan Walsh, Red Hat

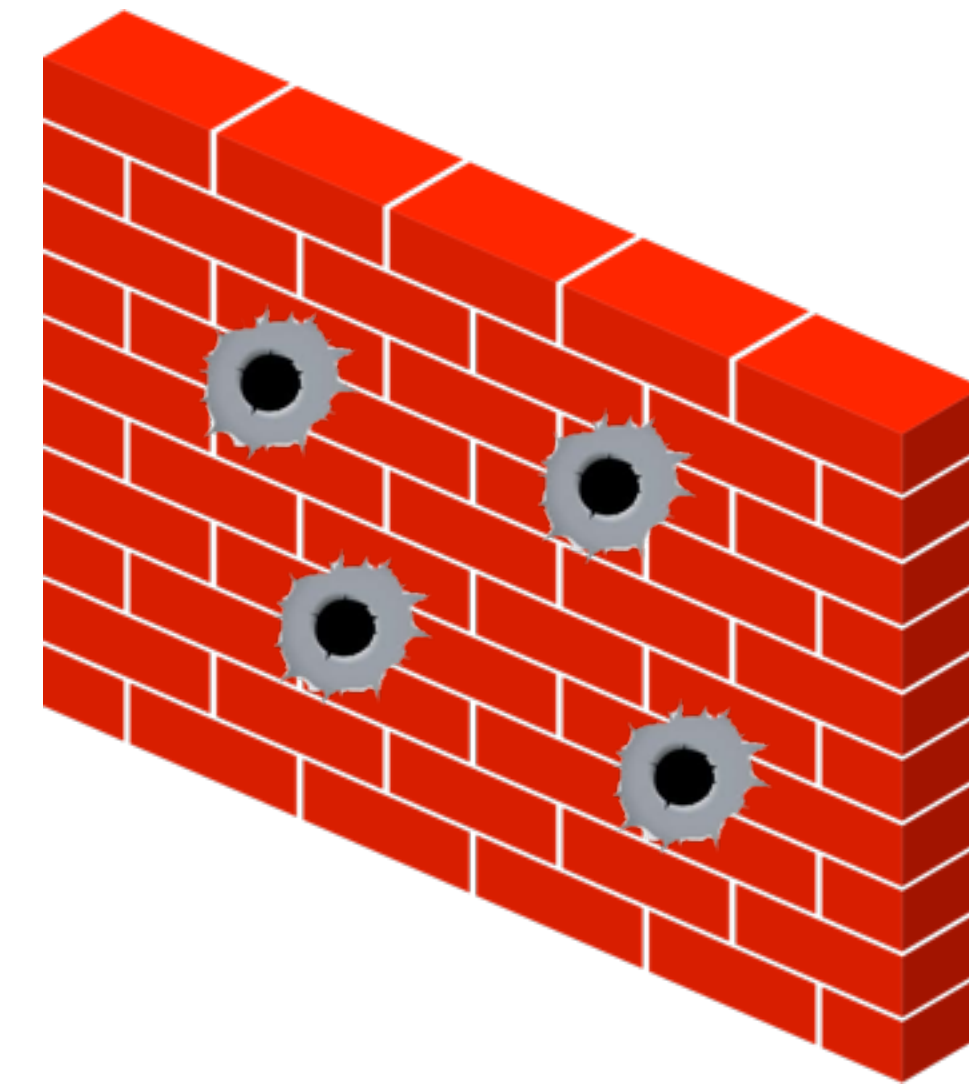
RESOURCES NOT NAMESPACED

- Kernel keyring
- Kernel itself and modules
- Devices
- System time
- UIDs*
 - *RHEL 7.2 Tech Preview
 - *Kernel boot option, `user_namespace.enable=1`



CONTAINER SECURITY RISKS

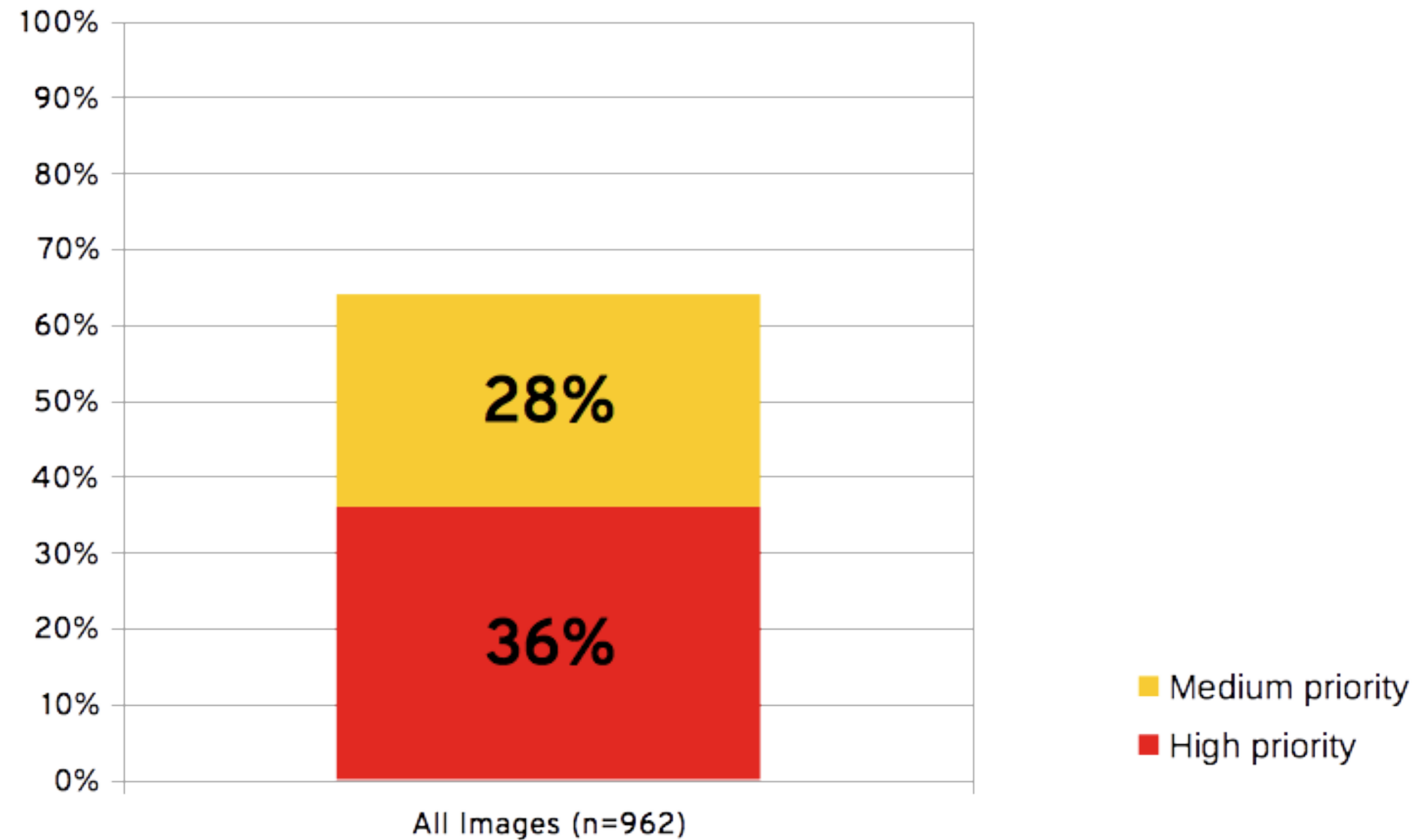
- Kernel exploits
- Denial of Service attacks
- Container breakouts
- Poisoned images
- Compromised secrets



CONTAINER IMAGES

WHAT'S INSIDE THE CONTAINER MATTERS

64% of official images in Docker Hub
contain **high** priority security vulnerabilities



examples:

ShellShock (bash)

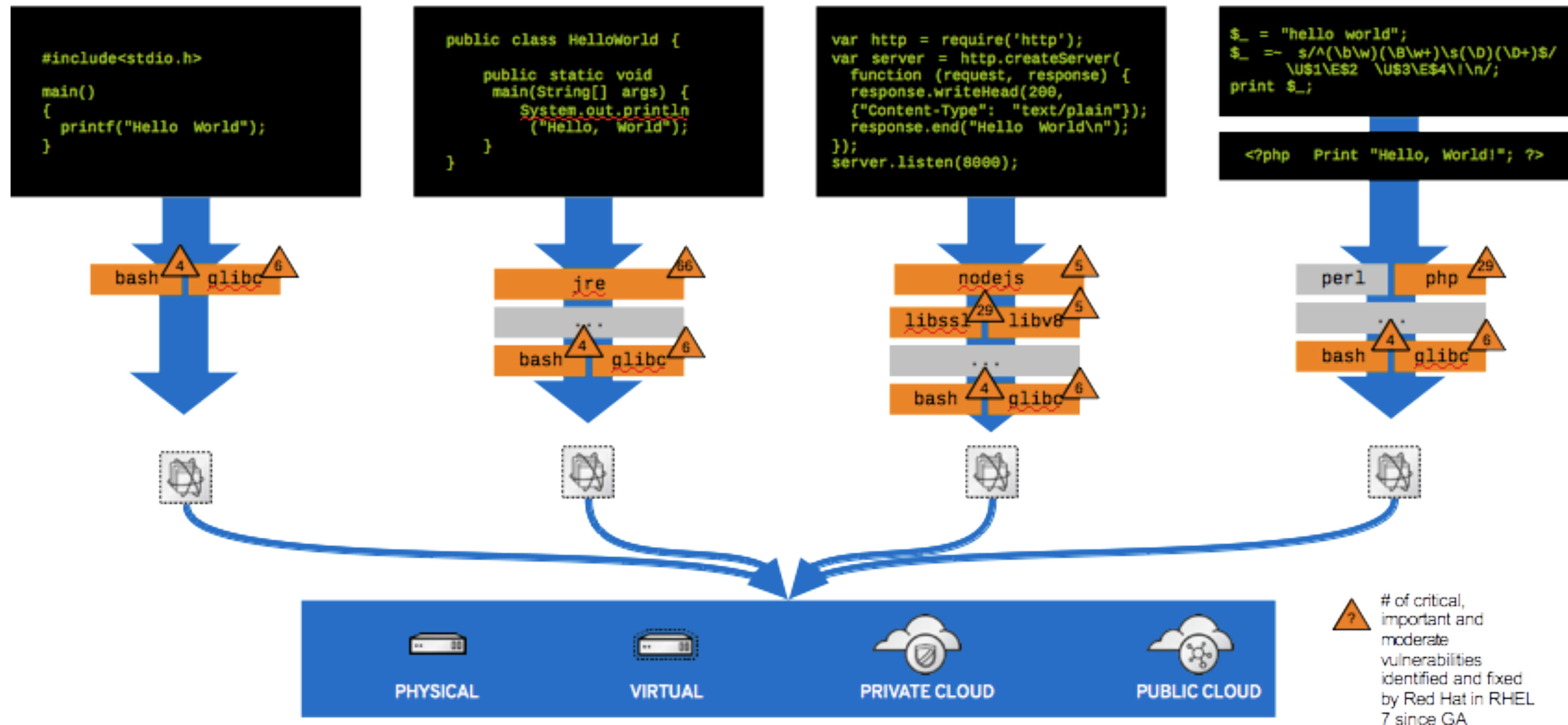
Heartbleed (OpenSSL)

Poodle (OpenSSL)

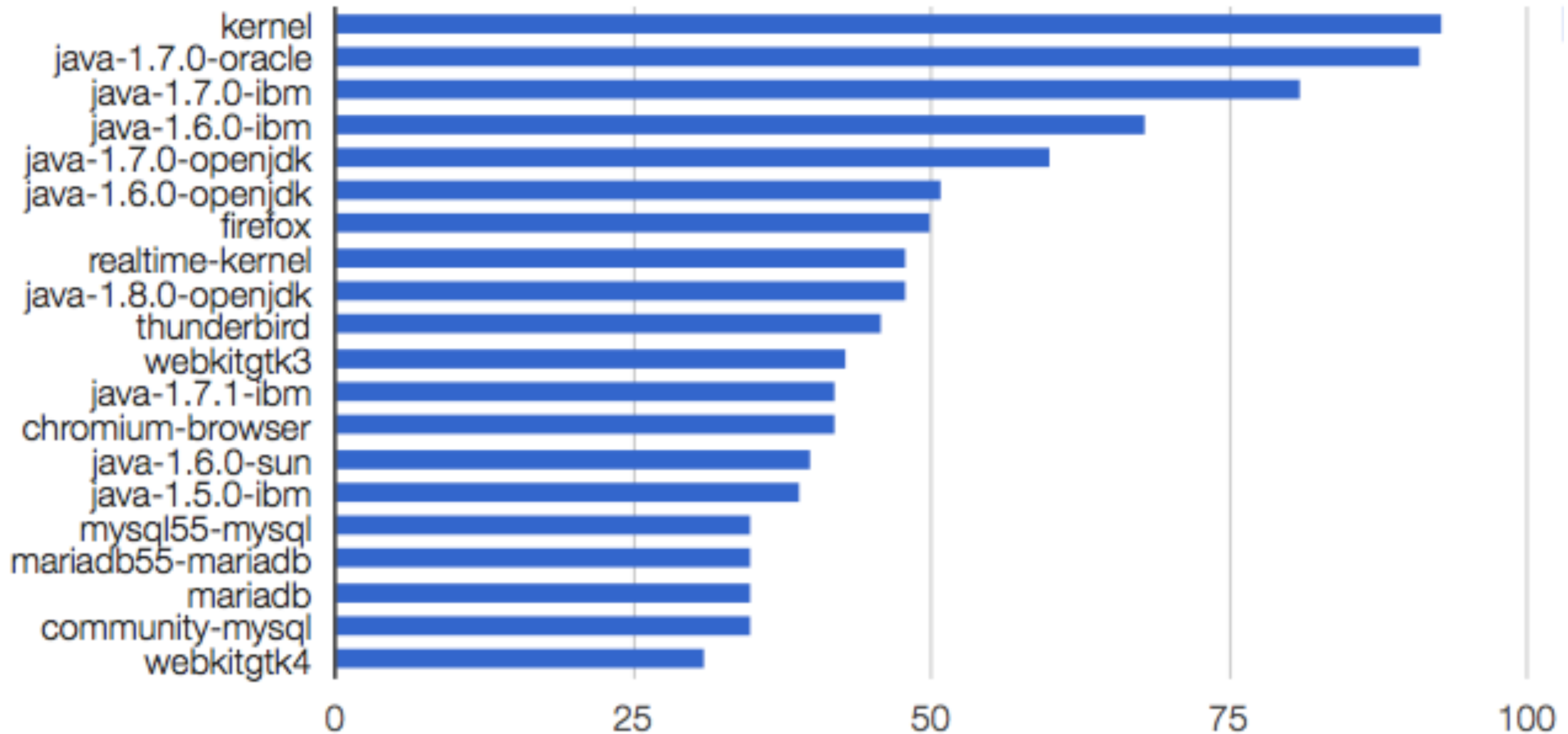
Source: *Over 30% of Official Images in Docker Hub Contain High Priority Security Vulnerabilities*, Jayanth Gummaraju, Tarun Desikan, and Yoshio Turner, BanyanOps, May 2015 (<http://www.banyanops.com/pdf/BanyanOps-AnalyzingDockerHub-WhitePaper.pdf>)

SECURITY IMPLICATIONS

What's inside the container and where it comes from matters



VULNERABILITIES PER PACKAGE TOP 20 (2014)



Compliance and Vulnerability Audits with OpenSCAP

NIST

National Institute of Standards and Technology



automating vulnerability management, security management, and compliance checking

Common Vulnerability and Exposures (CVE)

CVE DATABASE

CVE-2015-5477

Impact:	Important
Public:	2015-07-28
CWE:	CWE-456->CWE-617
Bugzilla:	1247361 : CVE-2015-5477 bind: TKEY query handling flaw leading to denial of service

Details

A flaw was found in the way BIND handled requests for TKEY DNS resource records. A remote attacker could use this flaw to make named (functioning as an authoritative DNS server or a DNS resolver) exit unexpectedly with an assertion failure via a specially crafted DNS request packet.

Find out more about CVE-2015-5477 from the [MITRE CVE dictionary](#) and [NIST NVD](#).

Common Configuration Enumeration (CCE)

CCE Database

CCE-27002-5

Set Password Minimum Length in login.defs

To specify password length requirements for new accounts, edit the file `/etc/login.defs` and add or correct the following lines:

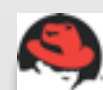
`PASS_MIN_LEN`

The DoD requirement is 14. The FISMA requirement is 12. If a program consults `/etc/login.defs` and also another PAM module (such as `pam_cracklib`) during a password change operation, then the most restrictive must be satisfied. See PAM section for more information about enforcing password quality requirements.

OpenSCAP

Scan physical servers, virtual machines, docker images and containers for Compliance (CCEs) and known Vulnerabilities (CVEs)

Content



SCAP Security
Guide
for RHEL

CCE-27002-5

Set Password Minimum
Length

CVE DATABASE

CVE-2015-5477

Impact: **important**
Public: 2015-07-28

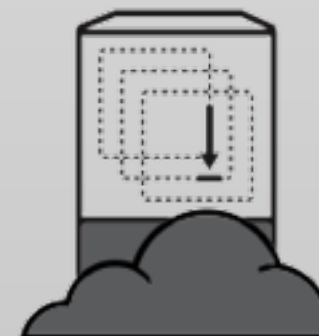
Scan



OpenSCAP



FOREMAN



Reports

Compliance and Scoring

The target system did not satisfy conditions of 33 rules! Please review rule results and consider applying remediation.

Rule result breakdown

34 passed 33 failed

Failed rules by severity breakdown

3 high 16 medium 14 low

Score

Scoring system	Score	Maximum	%
umaxscoredefault	48.935184	100.000000	48.94%

Existence of Password Hashes (1x fail)		
Accounts With Empty Password	high	fail
Password Hashes are Shadowed	medium	pass
Parameters (2x fail)		
Length in login.defs	medium	fail
Age	medium	fail
Age	low	pass
Using PAM (10x fail)		
Requirements (5x fail)		
Prompt Permitted Per-Session	low	pass
Minimum Digit Characters	low	fail
Minimum Uppercase Characters	low	fail
Minimum Special Characters	low	fail
Minimum Lowercase Characters	low	fail

OpenSCAP Tools



USE CASE #1: Scan for Compliance

Are password
quality
requirements set?

Are obsolete
services enabled,
e.g. telnet?

Is openssh properly
configured?

Is /tmp on a
separate partition?

SCAN

```
oscap xccdf eval --profile rhsccp \
--report /var/www/html/report.html \
--results /var/www/html/results.html \
--cpe /usr/share/xml/scap/ssg/content/ssg-rhel7-cpe-dictionary.xml \
/usr/share/xml/scap/ssg/content/ssg-rhel7-xccdf.xml
```

Title	Disable Host-Based Authentication
Rule	disable_host_auth
Ident	CCE-26870-6
Result	pass
Title	Disable SSH Root Login
Rule	sshd_disable_root_login
Ident	CCE-26946-4
Result	fail
Title	Disable SSH Access via Empty Passwords
Rule	sshd_disable_empty_passwords
Ident	CCE-26864-9
Result	fail


REPORT

xccdf_org.open-scap_testresult_rht-ccp | OpenSCAP Evaluation Report

172.16.205.216/report.html

Most Visited FB

Search

 OpenSCAP Evaluation Report

Evaluation Characteristics

Target machine	ose-master1.chrisvantuin.com
Benchmark URL	/usr/share/xml/scap/ssg/content/ssg-rhel7-xccdf.xml
Profile ID	rht-ccp
Started at	2015-07-31T14:56:59
Finished at	2015-07-31T14:57:17
Performed by	root

CPE Platforms

- cpe:/o:redhat:enterprise_linux:7
- cpe:/o:redhat:enterprise_linux:7::client

Addresses

- IPv4 127.0.0.1
- IPv4 172.16.205.216
- IPv4 172.17.42.1
- IPv4 10.1.2.1
- IPv6 0:0:0:0:0:0:1
- IPv6 fe80:0:0:0:20c:29ff:fe75:e207
- IPv6 fe80:0:0:0:f80f:c5ff:fe1e:2b79
- IPv6 fe80:0:0:0:24a6:54ff:fe0f:f872
- IPv6 fe80:0:0:0:6c9e:c0ff:fef6:68f2
- IPv6 fe80:0:0:0:6c01:85ff:fe7f:39d4
- MAC 00:00:00:00:00:00
- MAC 00:0C:29:75:E2:07
- MAC 56:84:7A:FE:97:99
- MAC FA:0F:C5:1E:2B:79
- MAC 6E:9E:C0:F6:68:F2
- MAC 26:A6:54:0F:F8:72

REPORT

Compliance and Scoring

The target system did not satisfy conditions of 33 rules! Please review rule results and consider applying remediation.


Rule result breakdown



Failed rules by severity breakdown



Score

Scoring system	Score	Maximum	%
urn:xccdf:scoring:default	48.935184	100.000000	 48.94%

REPORT

▼ Verify Proper Storage and Existence of Password Hashes 1x fail		
Prevent Log In to Accounts With Empty Password	high	fail
Verify All Account Password Hashes are Shadowed	medium	pass
▼ Set Password Expiration Parameters 2x fail		
Set Password Minimum Length in login.defs	medium	fail
Set Password Minimum Age	medium	fail
Set Password Warning Age	low	pass
▼ Protect Accounts by Configuring PAM 10x fail		
▼ Set Password Quality Requirements 5x fail		
▼ Set Password Quality Requirements, if using pam_pwquality 5x fail		
Set Password Retry Prompts Permitted Per-Session	low	pass
Set Password Strength Minimum Digit Characters	low	fail
Set Password Strength Minimum Uppercase Characters	low	fail
Set Password Strength Minimum Special Characters	low	fail
Set Password Strength Minimum Lowercase Characters	low	fail

REMEDIATION

Set Password Strength Minimum Digit Characters

Rule ID	accounts_password_pam_dcredit
Result	<div>fail</div>
Time	2015-07-31T14:57:17
Severity	low
Identifiers and References	<div>identifiers: CCE-27163-5</div> <div>references: IA-5(b), IA-5(c), 194, 194, 71,</div>

The pam_pwquality module's dcredit parameter controls requirements for usage of digits in a password. When set to a negative number, any password will be required to contain that many digits. When set to a positive number, pam_pwquality will grant +1 additional length credit for each digit. Add dcredit=-1 after pam_pwquality.so to require use of a digit in passwords.

Remediation script:

```
var_password_pam_dcredit="-1"
if grep -q "dcredit=" /etc/pam.d/system-auth; then
    sed -i --follow-symlink "s/\(dcredit *= *\).*$/\1$var_password_pam_dcredit/" /etc/pam.d/system-auth
else
    sed -i --follow-symlink "/pam_pwquality.so/ s/$/ dcredit=$var_password_pam_dcredit/" /etc/pam.d/system-auth
fi
```


USE CASE #2: Scan for Known Vulnerabilities

What RPMs need updating?

What is the criticality of the vulnerability?

What is the vulnerability?

What CVEs have and have not been addressed?

SCAN

```
# obtain RHSA file from Red Hat for RHEL
wget http://www.redhat.com/security/data/oval/com.redhat.rhsa-all.xml

# run Vulnerability scan
oscap oval eval --results /var/www/html/rhsa-results-oval.xml \
--report /var/www/html/oval-report.html com.redhat.rhsa-all.xml

# view the Report
firefox /var/www/html/oval-report.html
```

```
m.redhat.rhsa:def:20040050: false
m.redhat.rhsa:def:20040047: false
m.redhat.rhsa:def:20040041: false
m.redhat.rhsa:def:20040033: false
m.redhat.rhsa:def:20040031: false
m.redhat.rhsa:def:20040023: false
m.redhat.rhsa:def:20040017: false
m.redhat.rhsa:def:20040015: false
m.redhat.rhsa:def:20040008: false
m.redhat.rhsa:def:20040005: false
m.redhat.rhsa:def:20040004: false
m.redhat.rhsa:def:20040002: false
m.redhat.rhsa:def:20030416: false
Definition oval:com.redhat.rhsa:def:20030404: false
Definition oval:com.redhat.rhsa:def:20030399: false
Definition oval:com.redhat.rhsa:def:20030395: false
Definition oval:com.redhat.rhsa:def:20030386: false
Definition oval:com.redhat.rhsa:def:20030334: false
Definition oval:com.redhat.rhsa:def:20030324: false
Definition oval:com.redhat.rhsa:def:20030317: false
Definition oval:com.redhat.rhsa:def:20030315: false
Evaluation done.
[root@ose-master1 var]#
[root@ose-master1 var]#
```


REPORT

OVAL Results Generator Information				
Schema Version	Product Name	Product Version	Date	Time
5.10.1	cpe:/a:open-scap:oscap		2015-07-31	15:03:03
#x	#✓	#Error	#Unknown	#Other
6	2665	0	0	0

OVAL Definition Generator Information				
Schema Version	Product Name	Product Version	Date	Time
5.10.1	Red Hat OVAL Patch Definition Merger	3	2015-07-30	13:16:01
#Definitions	#Tests	#Objects	#States	#Variables
2671 Total 0 0 0 2671 0	23552	2353	4093	0

System Information		
Host Name	ose-master1.chrisvantuin.com	
Operating System	Linux	
Operating System Version	#1 SMP Fri May 15 21:38:46 EDT 2015	
Architecture	x86_64	
	Interface Name	lo
	IP Address	127.0.0.1
	MAC Address	00:00:00:00:00:00

REPORT

OVAL Definition Results				
<div> <div>×</div> <div>✓</div> <div>Error</div> <div>Unknown</div> <div>Other</div> </div>				
ID	Result	Class	Reference ID	Title
oval:com.redhat.rhsa:def:20151513	true	patch	[RHSA-2015:1513-00], [CVE-2015-5477]	RHSA-2015:1513: bind security update (Important)
oval:com.redhat.rhsa:def:20151483	true	patch	[RHSA-2015:1483-00], [CVE-2015-3245], [CVE-2015-3246]	RHSA-2015:1483: libuser security update (Important)
oval:com.redhat.rhsa:def:20151443	true	patch	[RHSA-2015:1443-00], [CVE-2015-4620]	RHSA-2015:1443: bind security update (Important)
oval:com.redhat.rhsa:def:20151137	true	patch	[RHSA-2015:1137-01], [CVE-2014-9420], [CVE-2014-9529], [CVE-2014-9584], [CVE-2015-1573], [CVE-2015-1593], [CVE-2015-1805], [CVE-2015-2830]	RHSA-2015:1137: kernel security and bug fix update (Important)
oval:com.redhat.rhsa:def:20150987	true	patch	[RHSA-2015:0987-00], [CVE-2015-3331]	RHSA-2015:0987: kernel security and bug fix update (Important)
oval:com.redhat.rhsa:def:20150726	true	patch	[RHSA-2015:0726-00], [CVE-2014-8159], [CVE-2015-1421]	RHSA-2015:0726: kernel security and bug fix update (Important)
oval:com.redhat.rhsa:def:20151526	false	patch	[RHSA-2015:1526-00], [CVE-2015-2590], [CVE-2015-2601], [CVE-2015-2621], [CVE-2015-2625], [CVE-2015-2628], [CVE-2015-2632], [CVE-2015-2808], [CVE-2015-4000], [CVE-2015-4731], [CVE-2015-4732], [CVE-2015-4733], [CVE-2015-4748], [CVE-2015-4749], [CVE-2015-4760]	RHSA-2015:1526: java-1.6.0-openjdk security update (Important)
oval:com.redhat.rhsa:def:20151515	false	patch	[RHSA-2015:1515-00], [CVE-2015-5477]	RHSA-2015:1515: bind97 security update (Important)

USE CASE #3: Containers

Is the docker
image compliant?

Is the docker
image patched?

Is the docker
container
compliant?

Is the docker
container patched?

INSTALL

install oscap-docker

```
yum install openscap-utils
```

install docker

```
subscription-manager repos --enable=rhel-7-server-extras-rpms  
subscription-manager repos --enable=rhel-7-server-optional-rpms  
yum install openscap-scanner docker  
systemctl stop firewalld.service  
systemctl disable firewalld.service  
systemctl start docker.service  
systemctl enable docker.service
```

get RHEL6.2 docker image

```
docker pull docker.io/richxsl/rhel6.2
```


SCAN

DOCKER IMAGES (“offline”)

Compliance Scan

```
oscap-docker image docker.io/richxsl/rhel6.2 xccdf eval --profile xccdf_org.ssgproject.content_profile_rht-ccp \
/usr/share/xml/scap/ssg/content/ssg-rhel6-ds.xml
```

Vulnerability Scan on RHEL 6.2 image

```
oscap-docker image-cve docker.io/richxsl/rhel6.2 --results /var/www/html/image-oval.xml --report /var/www/html/image-
rhel62.html
```

DOCKER CONTAINERS (“online”)

start a container named myrhel62

```
docker run --name myrhel62 -it docker.io/richxsl/rhel6.2 /bin/bash
```

Compliance Scan

```
oscap-docker container myrhel62 xccdf eval --profile xccdf_org.ssgproject.content_profile_rht-ccp \
/usr/share/xml/scap/ssg/content/ssg-rhel6-ds.xml
```

Vulnerability Scan

```
oscap-docker container-cve docker.io/richxsl/rhel6.2 --results /var/www/html/container-oval.xml --report /var/www/
html/container-rhel62.html
```





SCAP

WORKBENCH

Title **Guide to the Secure Configuration of Fedora**

Customization (no customization) ▼

Profile Common Profile for General-Purpose Fedora Systems ▼

Customize

Target ☒ Local Machine

☐ Remote Machine (over SSH)

- ▶ Password Minimum Length
- ▶ Password Minimum Age
- ▶ Password Maximum Age
- ▶ Password Warning Age

fail

fail

fail

pass



OSCAP

ANACONDA ADDON

LOCALIZATION



DATE & TIME

Europe/Prague timezone



LANGUAGE SUPPORT

English (United States)

SECURITY



SECURITY PROFILE

Misconfiguration detected

SOFTWARE



INSTALLATION SOURCE

Closest mirror



SOFTWARE SELECTION

Custom software selected

Data stream:

scap_org.open-scap_datastream_tst ▾

Choose profile below:

My testing profile

A profile for testing purposes.

My testing profile2

Another profile for testing purposes.

Changes that were done or need to be done:



/tmp must be on a separate partition or logical volume



root password was too short, a longer one with at least 10 characters will be required



package 'iptables' has been added to the list of to be installed packages



package 'telnet' has been added to the list of excluded packages



OSCAP

ANACONDA ADDON

Without

Compliance and Scoring

The target system did not satisfy the conditions of 44 rules! Please review rule results and consider applying remediation.

Rule results



Severity of failed rules



Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	64.126724	100.000000	64.13%

64%

With

Compliance and Scoring

The target system did not satisfy the conditions of 1 rules! Please review rule results and consider applying remediation.

Rule results



Severity of failed rules



Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	98.958328	100.000000	98.96%

99%

VS






Compliance Reports

Filter ...



Search

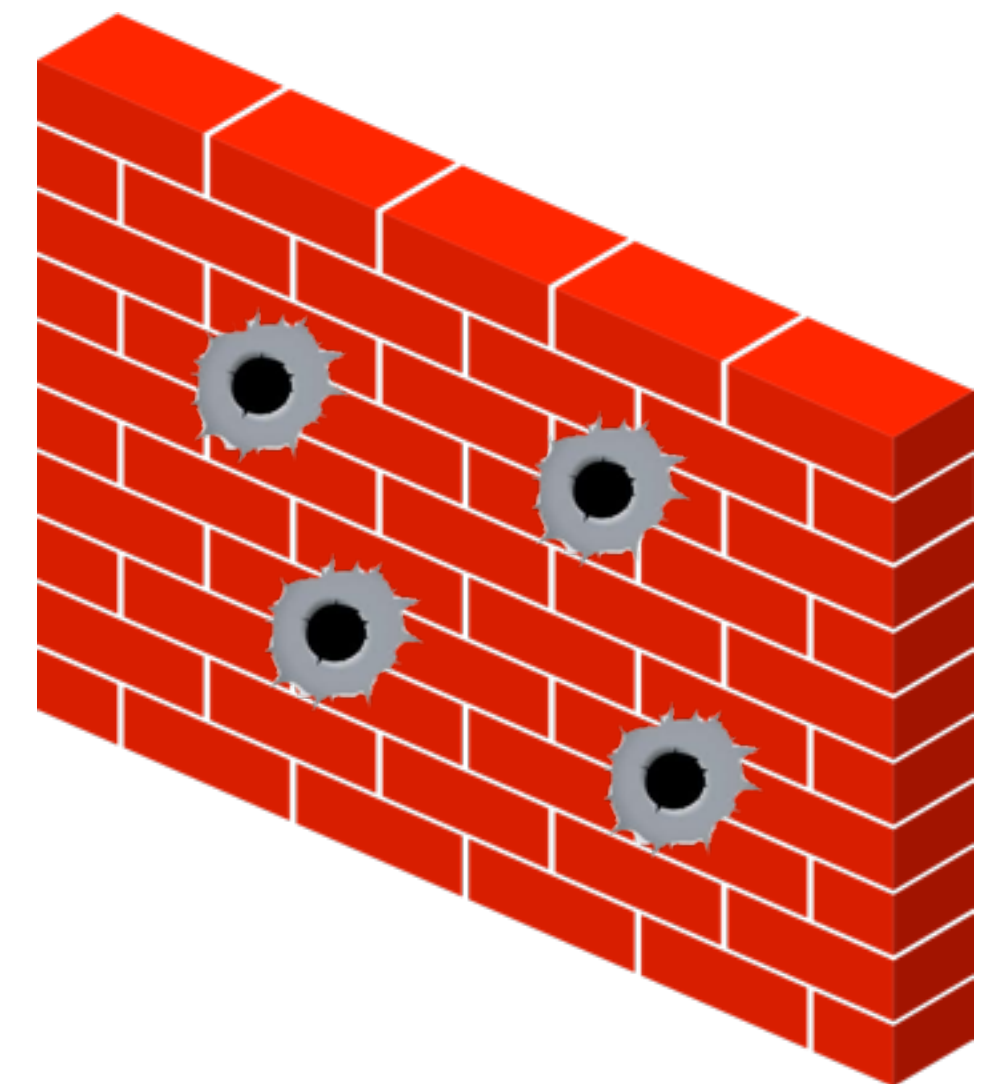


Host	Date	Passed	Failed	Other	
 scap1.local.lan	5 days ago	13	11	1	View Report ▾
 scap2.local.lan	5 days ago	13	11	1	View Report ▾
 scap2.local.lan	5 days ago	13	11	1	View Report ▾

Displaying **all 3** entries

CONTAINER BEST PRACTICES

- Only run container images from trusted parties
- Container apps should drop privileges
- Host operating system matters
- Apply kernel security fixes
- Do not disable selinux
- Examine container images for security flaws



RESOURCES

Best Practices	RHEL Security Guide
Hardening	SELinux
Audit Log	syslog / systemd-journald
Identity Management	RHEL IdM
Security Blog	securityblog.redhat.com
Three Pigs Coloring Book	https://t.co/4KH6iSZZ2H

THANK YOU!

Chris Van Tuin
cvantuin@redhat.com

