# Secure Container Development Pipelines with Jenkins

Anthony Bettini

Jenkins World

2016

#JenkinsWorld


# Secure Container Development Pipelines with Jenkins

Anthony Bettini, Founder & CEO of FlawCheck

#JenkinsWorld

# Topics


- About Me
- Who
- Evolution of the SDLC
- Secure SDLC Before Containerization
- High Stakes
- Enterprise Surveys
- Security for DevOps
- Plugins
- Conclusion
- Q&A


# About Me

20+ years in cybersecurity

# Anthony Bettini


Cybersecurity since 1996 (Netect, Bindview Team RAZOR, Guardent, Foundstone Labs, McAfee Avert Labs, Intel, Appthority, FlawCheck)

Was Research Manager of Foundstone at time of McAfee acquisition in 10/2004 – left Intel in 6/2011

Founding CEO of Appthority, which did static & dynamic analysis of mobile apps and was named the *Most Innovative Company of the Year* at RSA Conference 2012

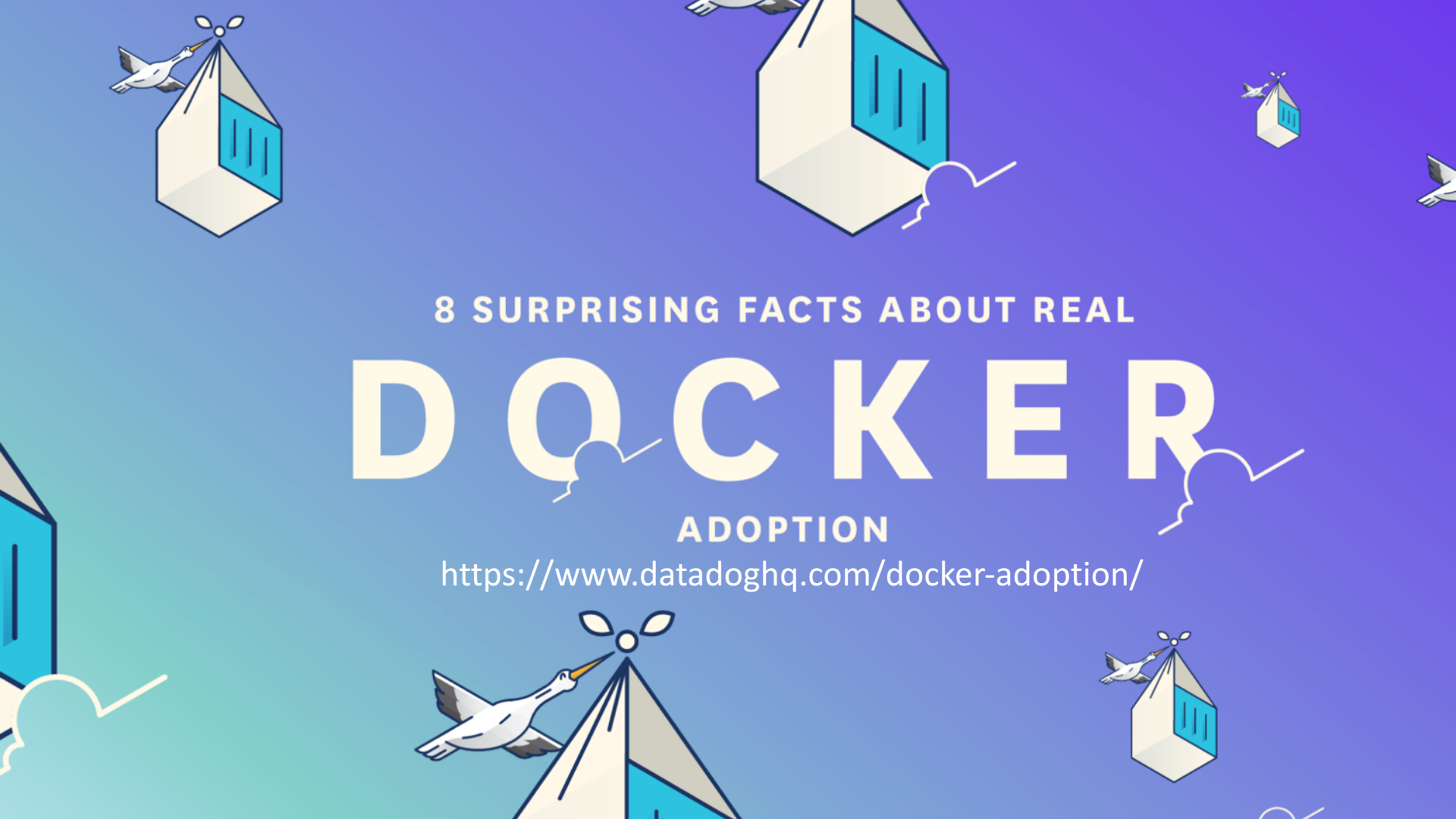
As CEO of Appthority, signed first 30+ enterprise customers

FlawCheck appthority TRUST YOUR APPS intel McAfee FOUNDSTONE GUARDENT BIND VIEW

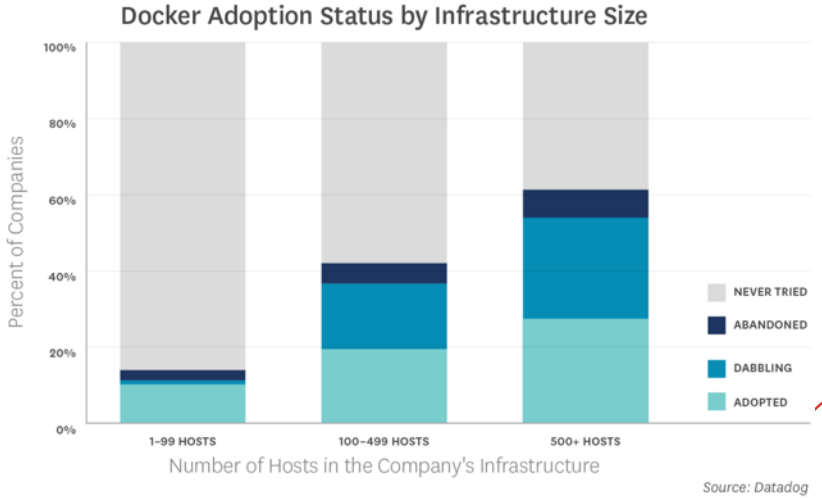
#JenkinsWorld


# Who

Who uses Docker? Who uses Jenkins? Who cares about security anyway?


8 SURPRISING FACTS ABOUT REAL
DOCKER
ADOPTION
https://www.datadoghq.com/docker-adoption/

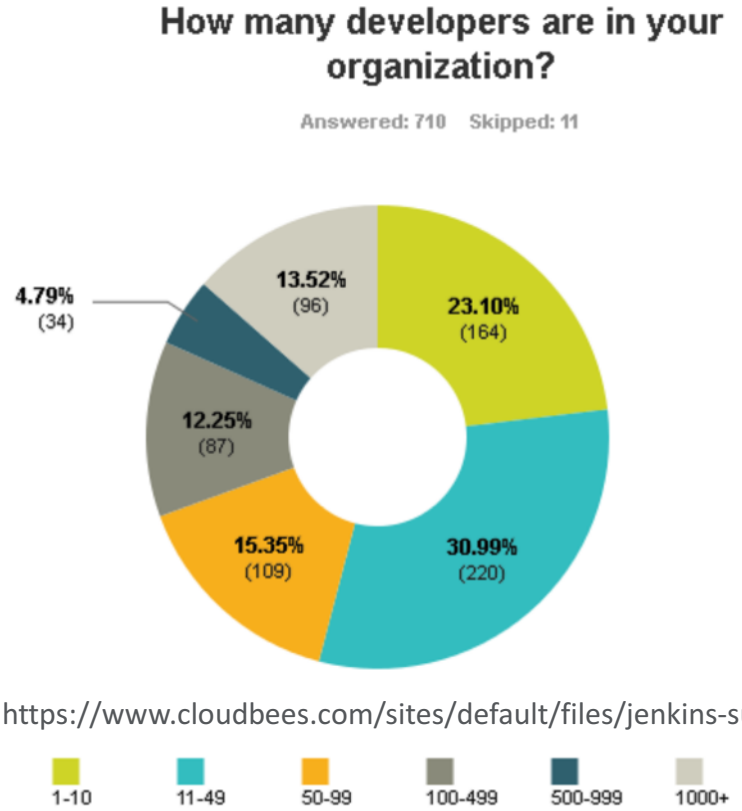
# Docker Adoption


## Larger Companies Are Leading Adoption

https://www.datadoghq.com/docker-adoption/

# Jenkins Adoption




https://www.cloudbees.com/sites/default/files/jenkins-survey-report-2012.pdf

- **Jenkins is useful for companies of any size, but 77% work for organizations with > 10 developers**
- **Jenkins is growing in Enterprises .**
  - 50% more respondents reported working for companies with > 500 developers (18% this year vs. 12% last year)

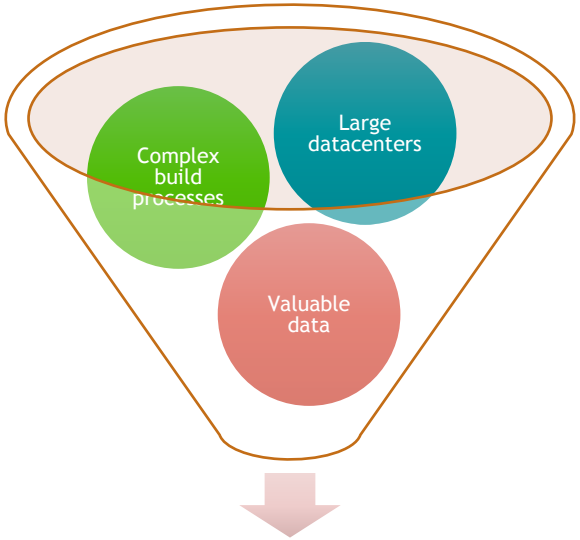
# Application Security Testing Market


- Gartner's 2015 MQ for AST are all enterprise-focused products
- Large enterprises are the ones spending the most on Application Security Testing, *not* necessarily large dev shops

**2015 Gartner Magic Quadrant for Application Security Testing (AST)**

# All roads lead to the Enterprise


- Those with the largest data centers have the most to gain by adopting Docker
- Those with the most complex build processes are most likely to use Jenkins
- Those whose data has the most value to an attacker are the ones most likely to spend the most on Application Security Testing programs



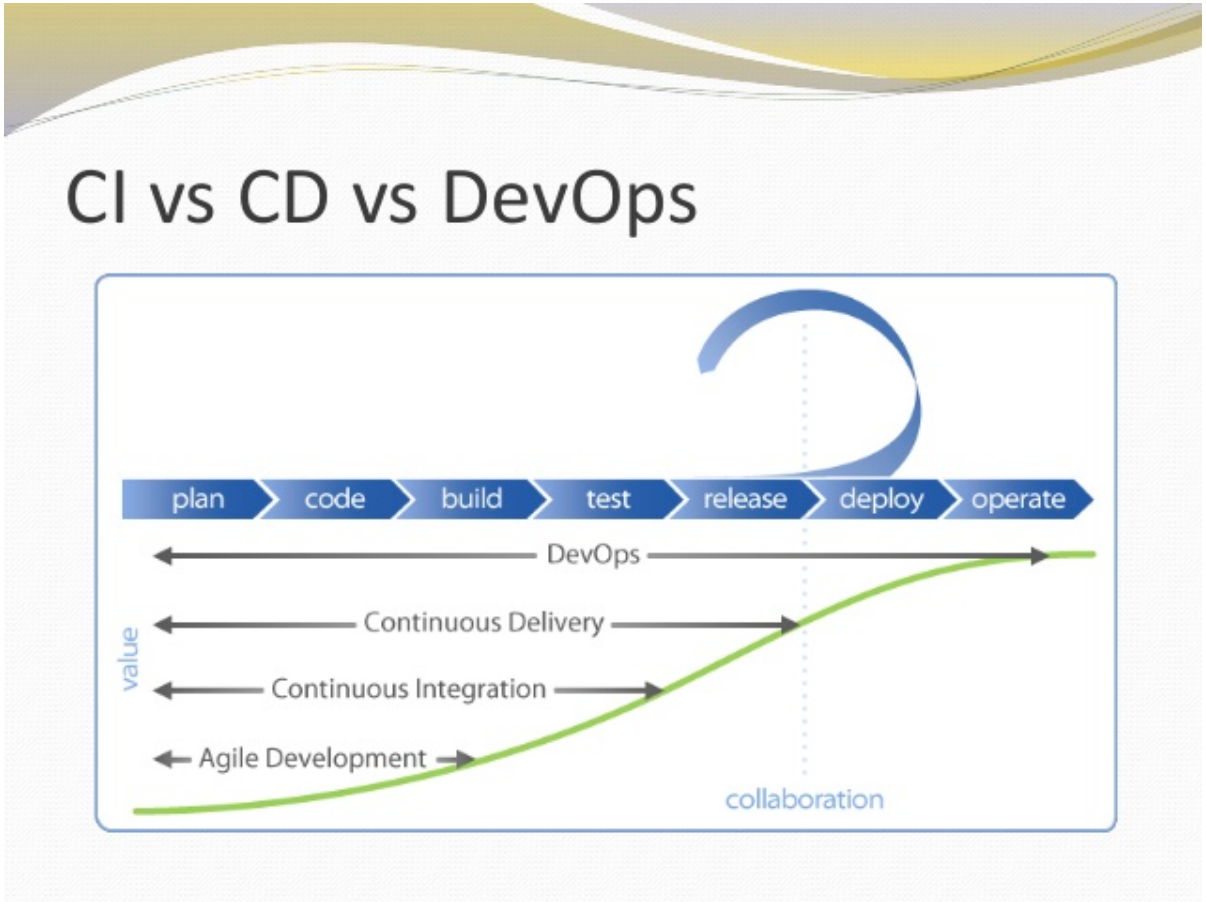

# Evolution of the SDLC

From Waterfall to DevOps (and everything in between) … What are we even talking about?

# Software Development Lifecycle (SDLC)


- Everything used to be waterfall, until Agile took over
- Then there was CI
- Some proceeded to do CD, if there regression testing, functional testing, and rollback processes were very mature
- And then there's DevOps …

# More Modern SDLCs



# Enterprises Securing DevOps?


- Before discussing how Enterprises can secure DevOps, need to go back to the beginning
- How were Enterprises securing waterfall-based software development lifecycles?


# Secure SDLC Before Containerization

BC: Before Containerization, how did organizations secure the SDLC?

# Enter OWASP


- All started with web application security
- Founded in 2001, when web applications started being all the rage
- Famous for the *OWASP Top 10*
- OWASP Top 10 supported by MITRE, PCI DSS, DISA, FTC, etc.

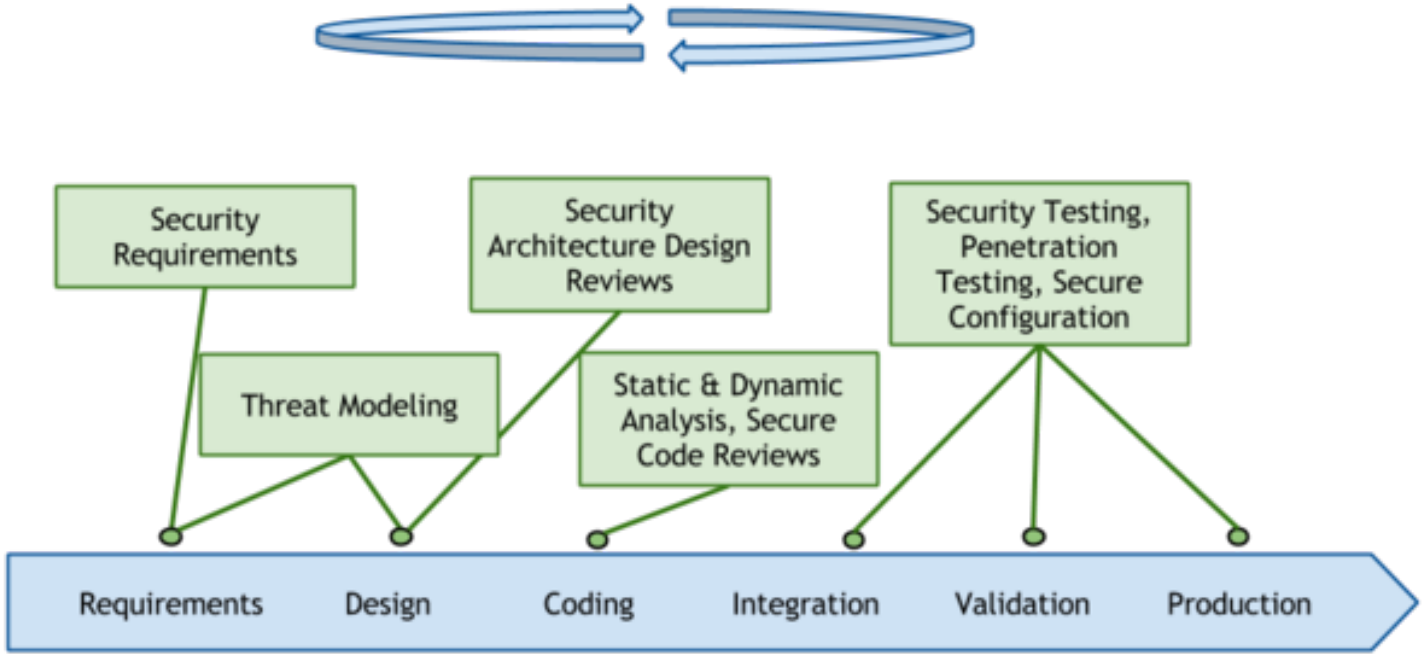
OWASP

The Open Web Application Security Project

# OWASP Top 10


| OWASP Top 10 – 2010 (Previous) | OWASP Top 10 – 2013 (New) |
|---|---|
| A1 – Injection | A1 – Injection |
| A3 – Broken Authentication and Session Management | A2 – Broken Authentication and Session Management |
| A2 – Cross-Site Scripting (XSS) | A3 – Cross-Site Scripting (XSS) |
| A4 – Insecure Direct Object References | A4 – Insecure Direct Object References |
| A6 – Security Misconfiguration | A5 – Security Misconfiguration |
| A7 – Insecure Cryptographic Storage – Merged with A9 → | A6 – Sensitive Data Exposure |
| A8 – Failure to Restrict URL Access – Broadened into → | A7 – Missing Function Level Access Control |
| A5 – Cross-Site Request Forgery (CSRF) | A8 – Cross-Site Request Forgery (CSRF) |
| <buried in A6: Security Misconfiguration> | A9 – Using Known Vulnerable Components |
| A10 – Unvalidated Redirects and Forwards | A10 – Unvalidated Redirects and Forwards |
| A9 – Insufficient Transport Layer Protection | Merged with 2010-A7 into new 2013-A6 |

## Security in the SDLC Process



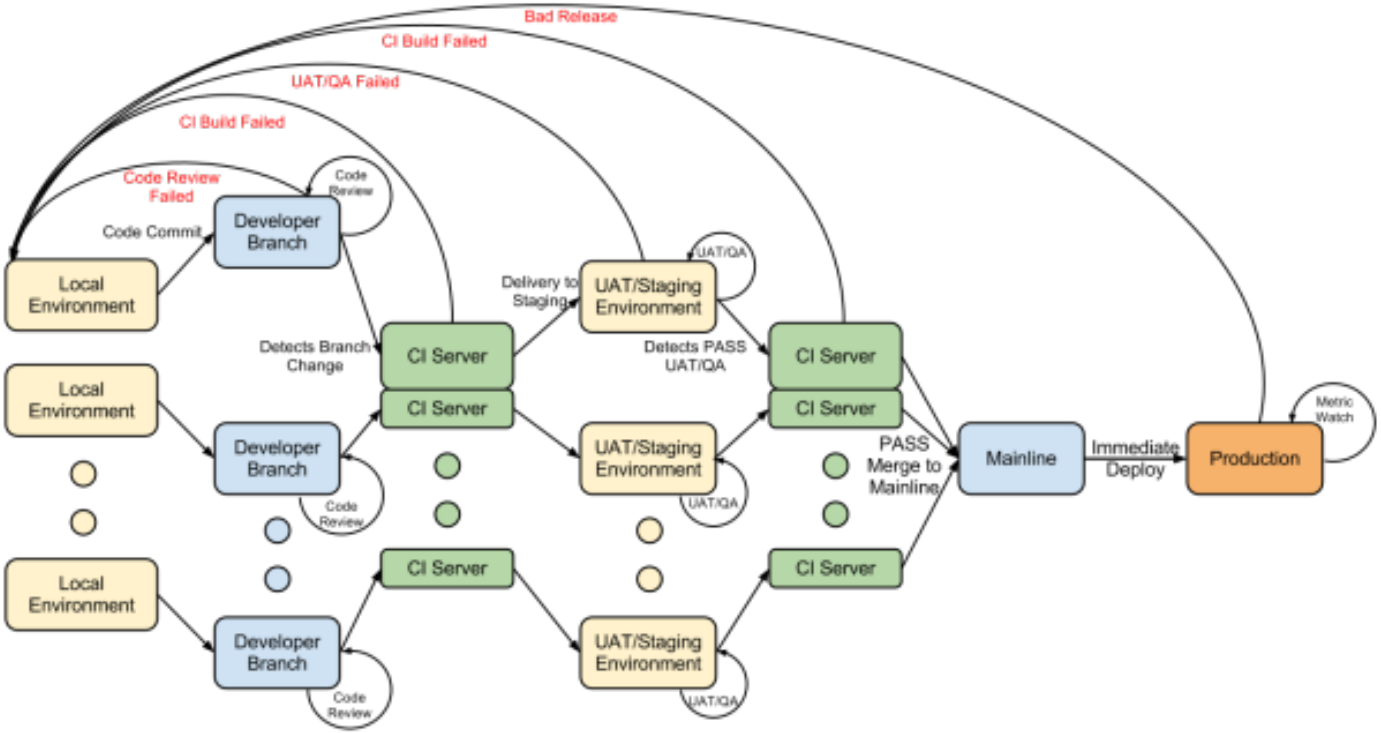
# The Carpet has been Pulled Out …


- The OWASP CISO AppSec Guide is still on the OWASP website
- But the “Security in the SDLC Process” is based on an SDLC from 10 years ago
- The SDLC has evolved, but security needs to be integrated into the newer SDLC (and move at the same speed as the SDLC)

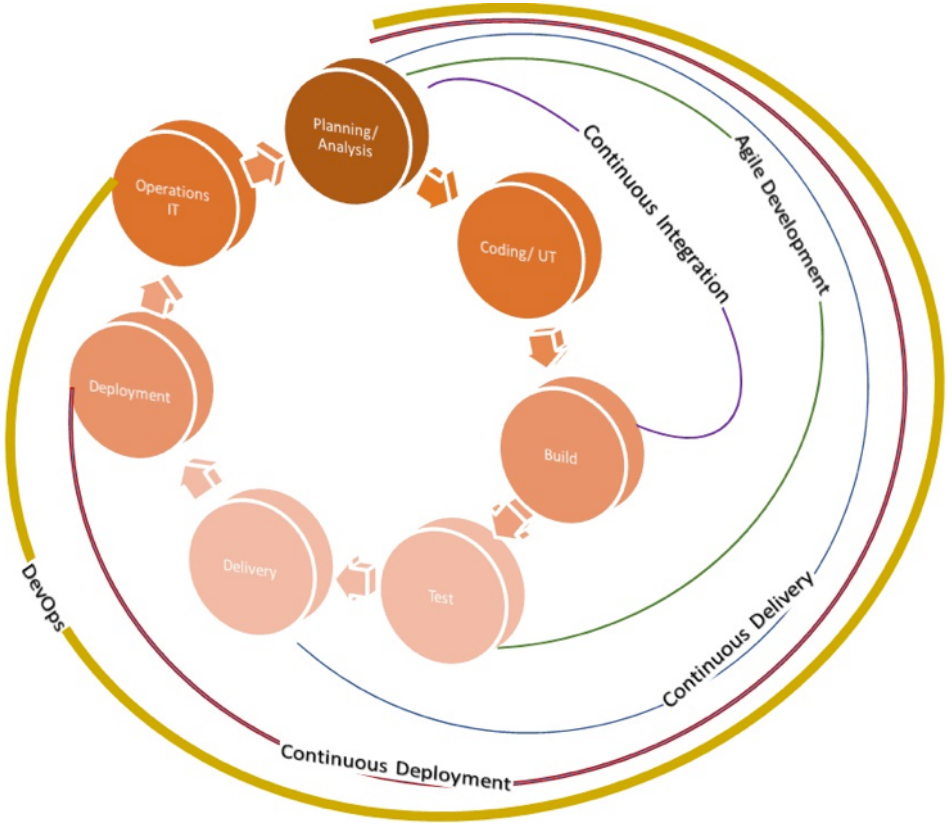

# High Stakes

Why this needs to be fixed?

# What's Missing?



# What's Still Missing?



# Security is Missing


- If the SDLC doesn't include Application Security Testing (AST), larger enterprises won't let applications reach production
- Even if the security operations team doesn't have the power (which is unlikely as they often have the power to say ***No***), regulatory compliance (auditors) will halt the applications from reaching productions
- This is something no one wants. Similarly, the old way of doing Application Security Testing (AST) was slow. It can't be shoved into the newer methodologies of doing fast software releases
- There needs to be a better way …


# Enterprise Surveys

Survey says …

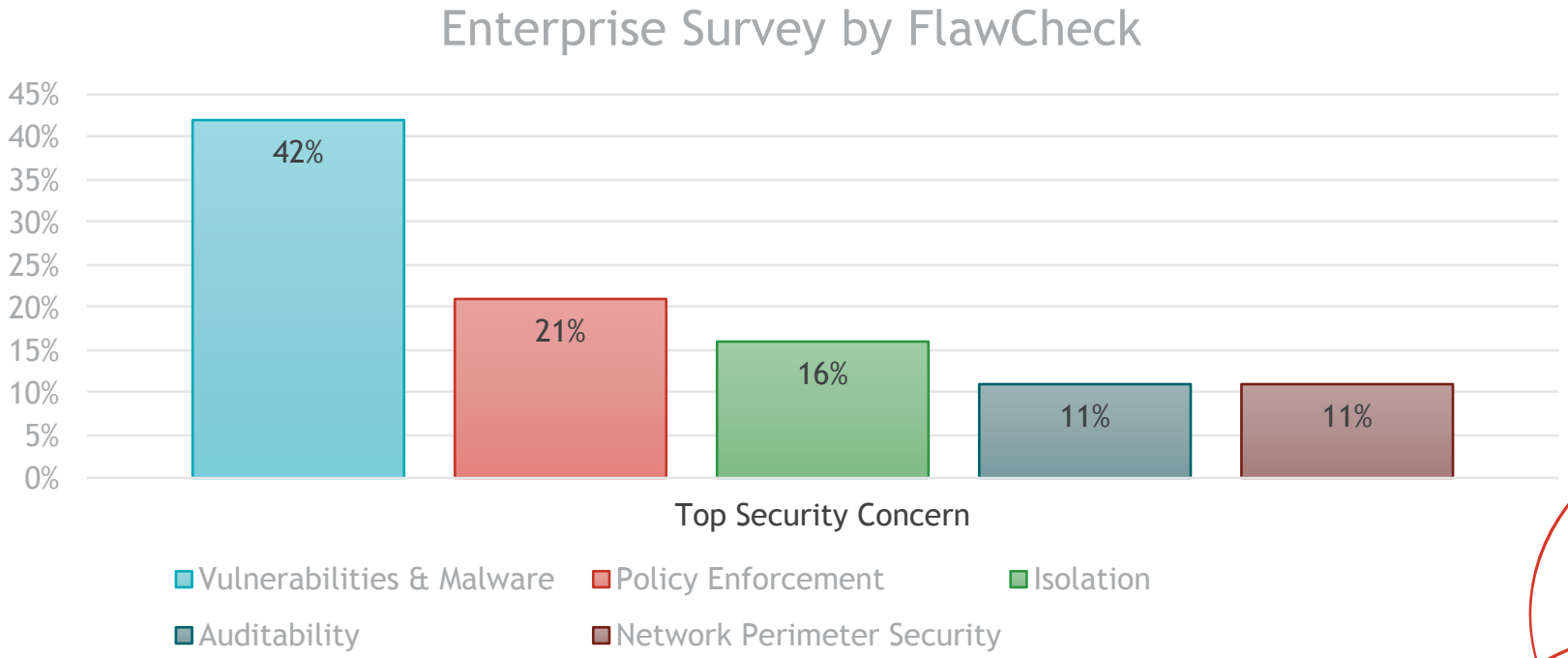
**53%** say **security**

is their biggest concern about containers.

Base: 194 IT operations and development decision-makers at enterprises in APAC, EMEA, and North America

Source: A commissioned study conducted by Forrester Consulting on behalf of Red Hat, January 2015

# Which Piece of the Security Puzzle?



# Application Security Testing (AST) is Critical


- Security concerns delaying container adoption in the data center
- Vulnerability & Malware affecting applications inside Docker containers is the top cybersecurity concern in the enterprise
- Security Operations holds back deployments of applications to production


# Security for DevOps

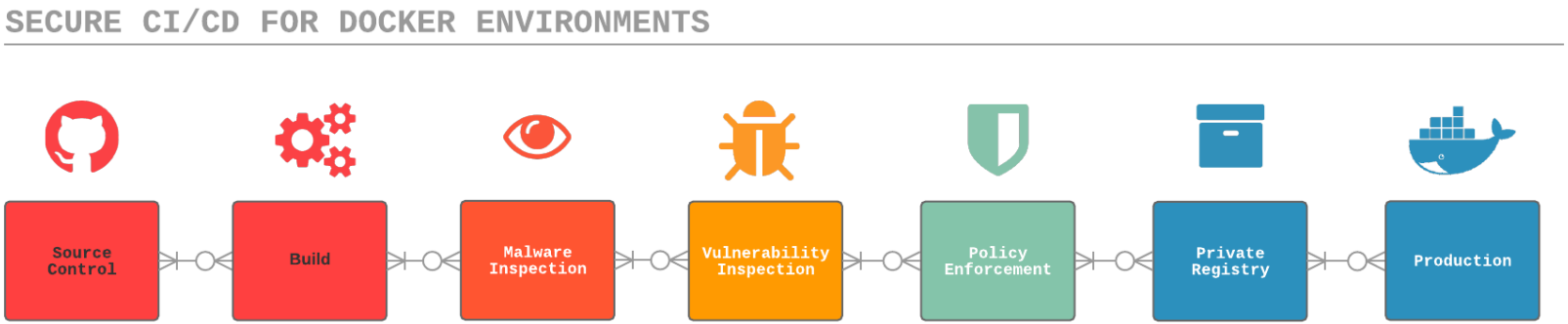
Security for Docker is Security for DevOps – and Jenkins is key

# Common Enterprise Questions


- How do we (the Enterprise) insert Application Security Testing (AST) into the build pipeline (powered by Jenkins), to ensure our applications are tested before they reach production (Docker)?
  - Without slowing down the developers?
  - While meeting regulatory compliance and standards controls?
- Oh, and what happens when we've approved it, but a new vulnerability is discovered, and production is affected?
  - And how will we know production is affected?

# Securing Docker in the SDLC


- As Enterprises begin coming to grasps with the changes to their SDLC, they begin trying to insert security into the pipeline



# How Our Enterprise Customers Solve This


**Source Control**

- GitLab
- GitHub Enterprise
- GitHub
- BitBucket Server (Stash)
- BitBucket

**Build**

- Jenkins
- CircleCI
- Shippable
- Bamboo
- Drone.io
- Travis CI
- Wercker
- Distelli
- Codeship
- Solano Labs

**Registry**

FlawCheck

- Container Registry
- Vulnerability Scanning
- Malware Detection
- Policy Enforcement
- Continuous Monitoring

**Container Host**

- Docker


# What's in a container? You don't know. And that's a problem

LARS HERRMANN, RED HAT

VentureBeat

TAGS: DOCKER, LARS HERRMANN, LINUX, LINUX CONTAINERS, RED HAT

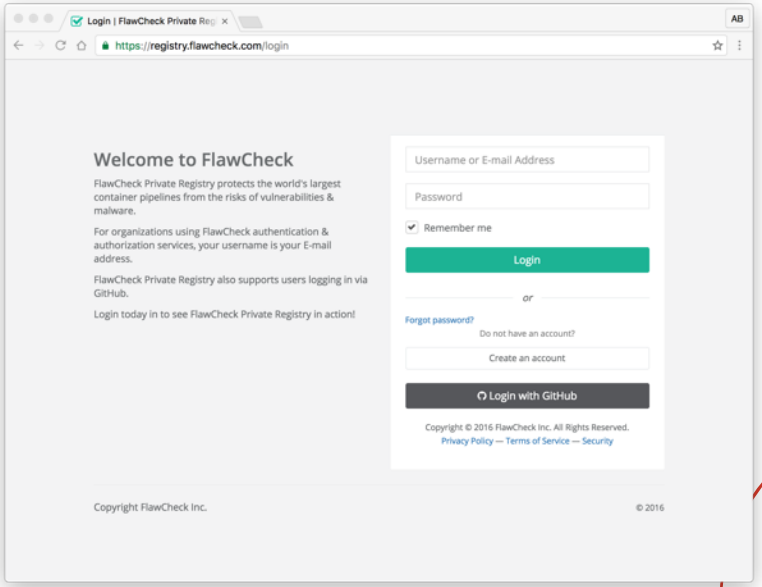
# Signup for Free


Already building Docker container images with Jenkins?

Concerned about the security of container images that could be pushed to production environments?

Register today for a free (for 1 private repository) hosted cloud account of FlawCheck Private Registry:

https://registry.flawcheck.com/register




# Plugins

Which Jenkins plugins are we seeing Enterprises use?

# Common Jenkins Plugins We See


- CloudBees Docker Build and Publish plugin
  - https://wiki.jenkins-ci.org/display/JENKINS/CloudBees+Docker+Build+and+Publish+plugin
  - (With the Docker daemon installed on the Jenkins hosts)
- GitHub plugin
  - https://wiki.jenkins-ci.org/display/JENKINS/GitHub+Plugin
- GitLab plugin *(seeing GitLab more and more …)*
  - https://wiki.jenkins-ci.org/display/JENKINS/GitLab+Plugin

Jenkins World
2016

# Conclusion

Lessons learned and takeaways

# Lessons Learned and Takeaways


- The stakeholders for Docker, Jenkins, and Application Security Testing (AST) are one-in-the-same: the largest enterprises of the world
- *Most* developers don't seem to care about security but *most* ops do … as DevOps converges, questions remain about how this divergence is handled
- Application Security Testing (AST), as it existed for waterfall environments, won't work (without substantial changes) in DevOps environments
- Application Security Testing (AST) needs to move at the same speed as the Software Development Lifecycle (SDLC)

# Q&A

Questions?

# Jenkins World

## 2016

#JenkinsWorld