

# **Immutable Awesomeness?**

## **Where Containers Collide with SW Supply Chains**

Joshua Corman - @joshcorman

John Willis - @botchagalupe

#DOES15



IMMUTABLE  
AWESOMENESS

# @joshcorman

- 20 Years in SW & Security
- IBM ISS, The 451 Group, Akamai, Sonatype
- Founder, Rugged Software
- Founder, I Am the Cavalry
- Adjunct Professor, Carnegie Mellon University Heinz College



# @botchagalupe

- a.k.a. John Willis
- 35 Years in IT Operations
- Exxon, Canonical, Chef, Enstratus, Socketplane
- Devopsdays Core Organizer
- Devopscafe on iTunes









h/t @petecheslock DevOpsDays Austin 2015

# Security is Dead. Long Live Rugged DevOps: IT at Ludicrous Speed...

*Josh Corman, Gene Kim*  
VERY ROUGH 1<sup>ST</sup> Draft



Session ID: CLD-106

Session Classification: Intermediate

RSACONFERENCE2012



SOURCEfire



CORETRACE

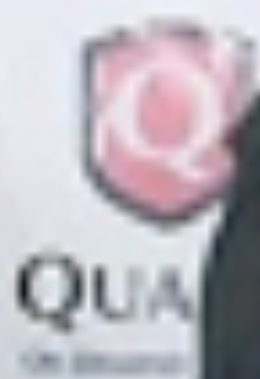
FORTINE

Akamai  
FASTER FORWARD



CONFERENCE | Where The Pros  
Talk Security

SOURCEfire



FORTINE

Akamai  
FASTER FORWARD

CONFERENCE | Where The Pros  
Talk Security





DevOps.com  
Share the world with DevOps

Sonatype

puppet  
labs

DevOps.com  
Share the world with DevOps









**SOFTWARE IS EATING THE WORLD**





Thu Jul 19 12:15:00 2004 (UTC)  
Visitors: 134181

<http://www.aids.org/>  
Copyright (C) 2004 UC Regents, Jeff Brown for UNAIDS/WHO

# Beyond **Heartbleed**: OpenSSL in 2014

(31 in NIST's NVD thru December)

CVE-2014-3470	6/5/2014	CVSS Severity: 4.3 MEDIUM ← <b>SIEMENS</b> *
CVE-2014-0224	6/5/2014	CVSS Severity: 6.8 MEDIUM ← <b>SIEMENS</b> *
CVE-2014-0221	6/5/2014	CVSS Severity: 4.3 MEDIUM
CVE-2014-0195	6/5/2014	CVSS Severity: 6.8 MEDIUM
CVE-2014-0198	5/6/2014	CVSS Severity: 4.3 MEDIUM ← <b>SIEMENS</b> *
CVE-2013-7373	4/29/2014	CVSS Severity: 7.5 HIGH
CVE-2014-2734	4/24/2014	CVSS Severity: 5.8 MEDIUM ** DISPUTED **
CVE-2014-0139	4/15/2014	CVSS Severity: 5.8 MEDIUM
CVE-2010-5298	4/14/2014	CVSS Severity: 4.0 MEDIUM
<b>CVE-2014-0160</b>	<b>4/7/2014</b>	<b>CVSS Severity: 5.0 MEDIUM</b> ← <b>HeartBleed</b>
CVE-2014-0076	3/25/2014	CVSS Severity: 4.3 MEDIUM
CVE-2014-0016	3/24/2014	CVSS Severity: 4.3 MEDIUM
CVE-2014-0017	3/14/2014	CVSS Severity: 1.9 LOW
CVE-2014-2234	3/5/2014	CVSS Severity: 6.4 MEDIUM
CVE-2013-7295	1/17/2014	CVSS Severity: 4.0 MEDIUM
CVE-2013-4353	1/8/2014	CVSS Severity: 4.3 MEDIUM
CVE-2013-6450	1/1/2014	CVSS Severity: 5.8 MEDIUM

...

As of today, internet scans by MassScan reveal 300,000 of original 600,000 remain unpatched or unpatchable



# MODIFIED MERCALLI INTENSITY SCALE

	Shaking	Structural Damage to Resistant Buildings	Structural Damage to Vulnerable Buildings
X	EXTREME		
IX	VERY STRONG		
VIII	STRONG		
VII	VERY STRONG		
VI	STRONG		
V	MODERATE		
IV	LIGHT		
III-III	WEAK		
I	NOT FELT		

## A TALE OF TWO QUAKES

In the span of two months, two massive earthquakes struck in Haiti and Chile. But while the tremor in Chile registered much higher on the Richter scale, the loss of life and damage in Haiti was far more severe. Why is that? Chile—which has experienced serious earthquakes in recent decades—has a robust building code to make sure buildings are earthquake resistant; Haiti has no code to speak of. And a look at both quake's scores on the Modified Mercalli Intensity Scale—which is used to measure how earthquakes affect those experiencing them—shows that while Chile's quake may have been stronger overall, Haiti had a larger population and more urban areas hit by more intense and damaging shaking.

### HAITI

January 12, 2010  
16:53 Local Time  
7.0 Richter Scale  
Estimated Fatalities:  
230,000



### POPULATION AFFECTED (percentage)



### CHILE

February 27, 2010  
03:34 Local Time  
8.8 Richter Scale  
Estimated Fatalities:  
279



Source: U.S. Geological Survey  
A collaboration between USGS and local authorities



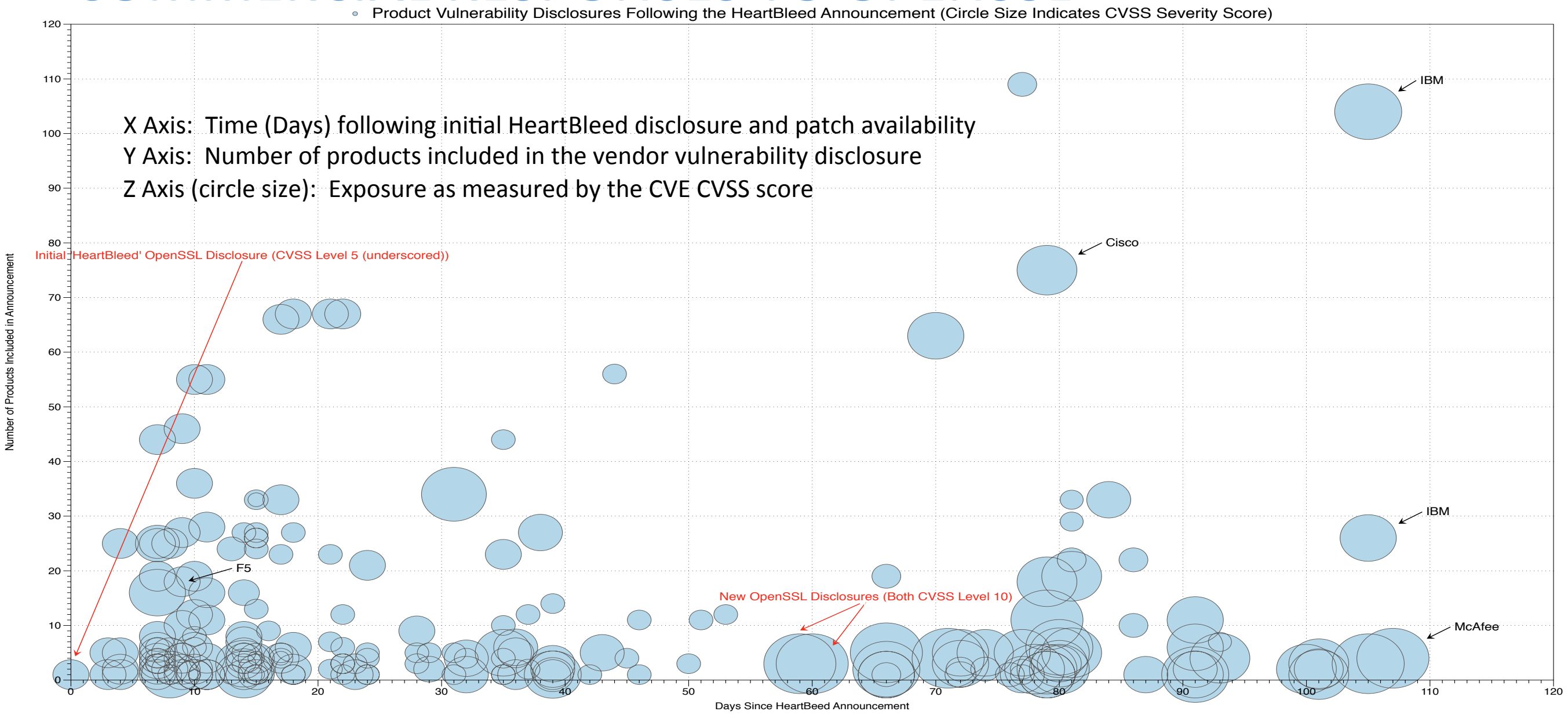


**"It is not enough to do your best;  
you must know what to do,  
and then do your best"**

*- W. Edwards Deming*

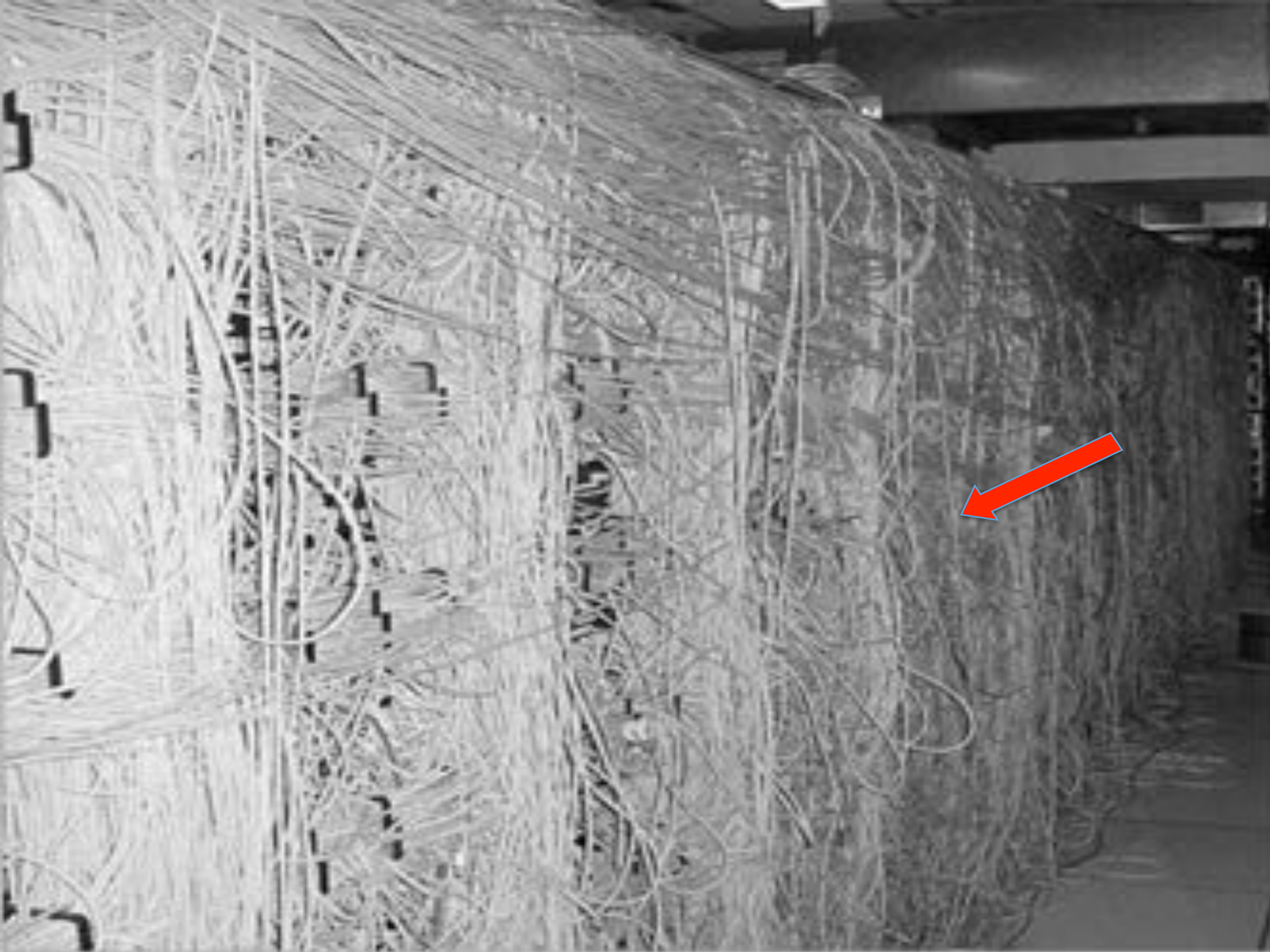
[LeadershipQuotes.org](http://LeadershipQuotes.org)

# COMMERCIAL RESPONSES TO OPENSSEL

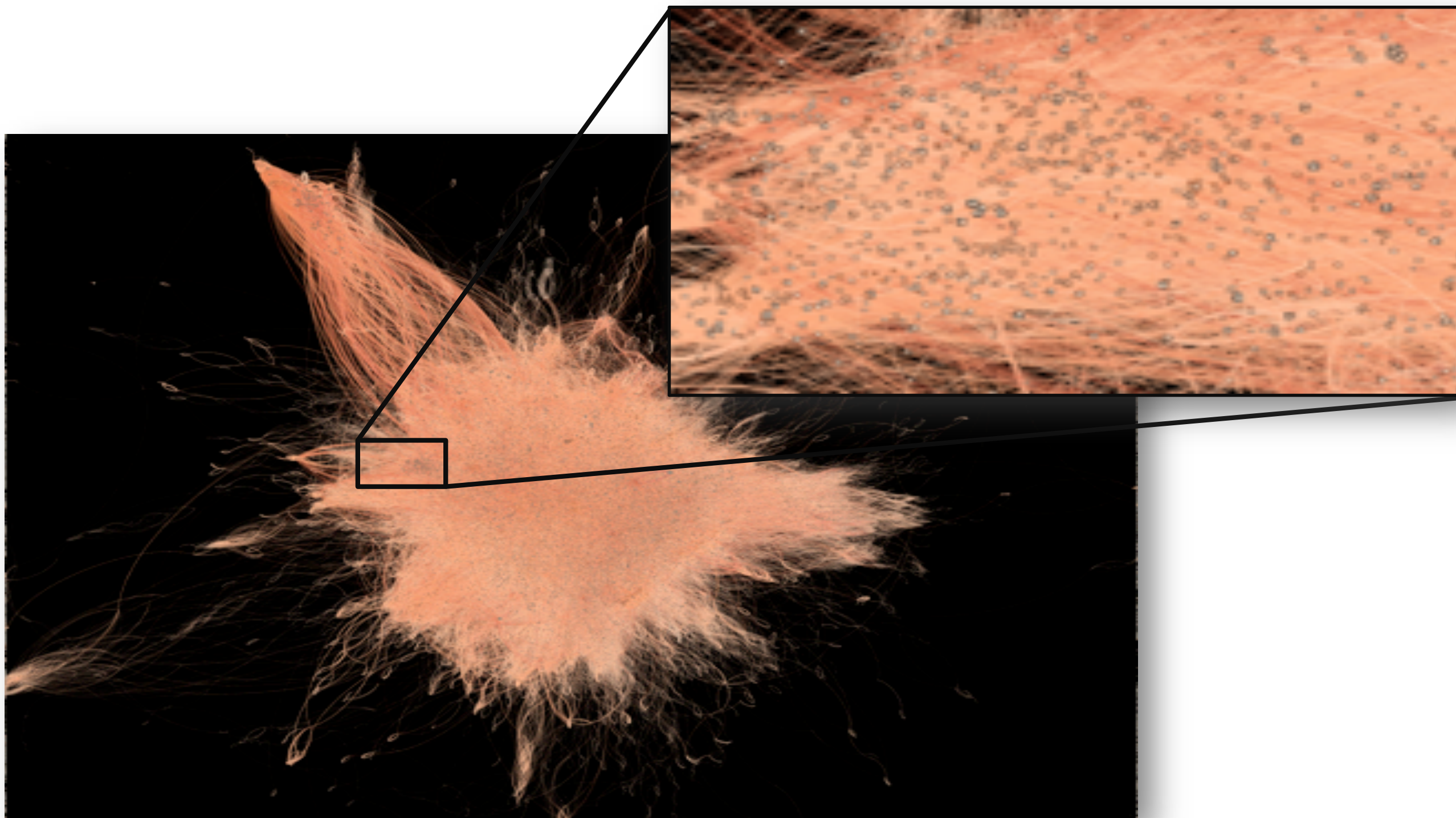








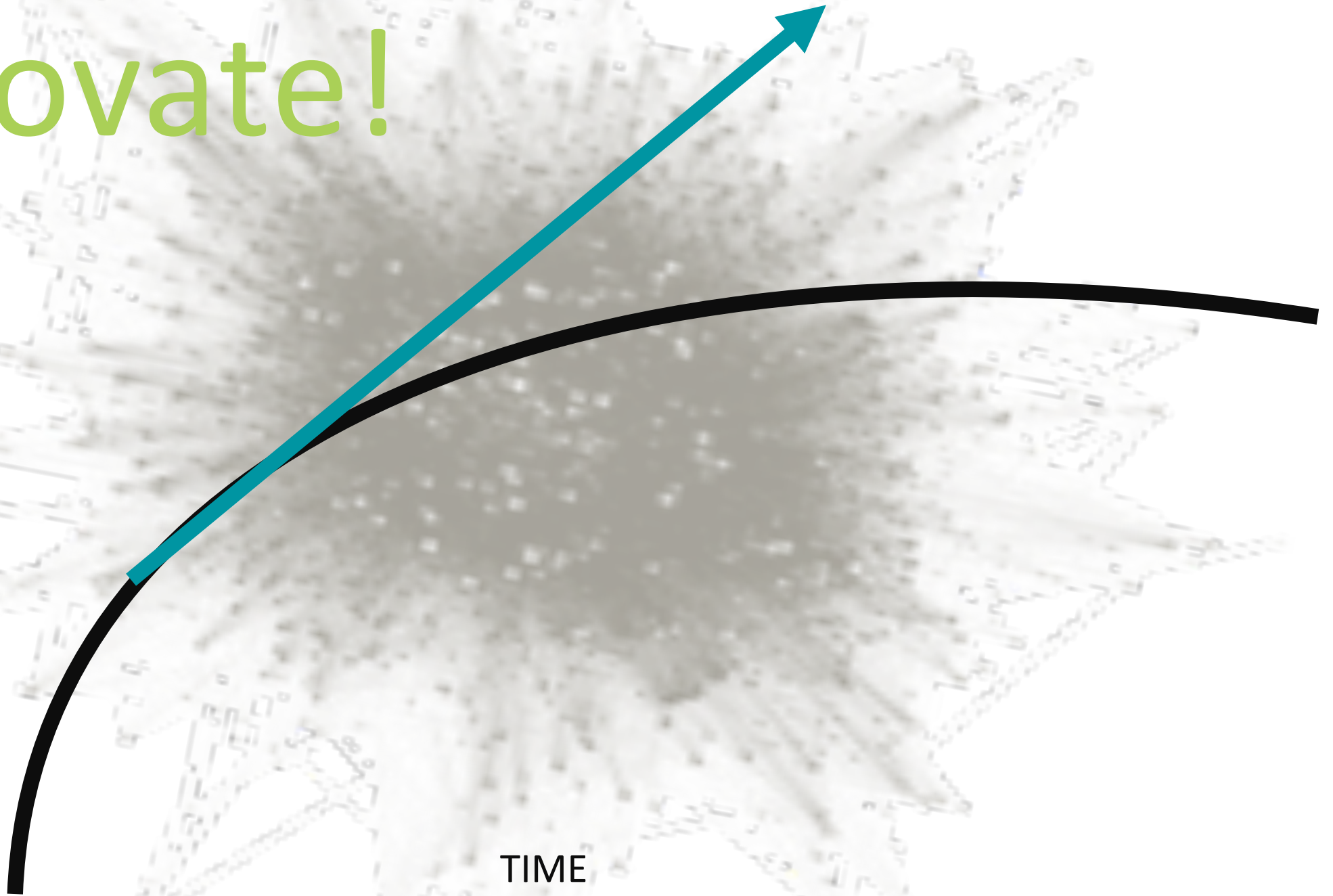




# Innovate!

PRODUCTIVITY

TIME





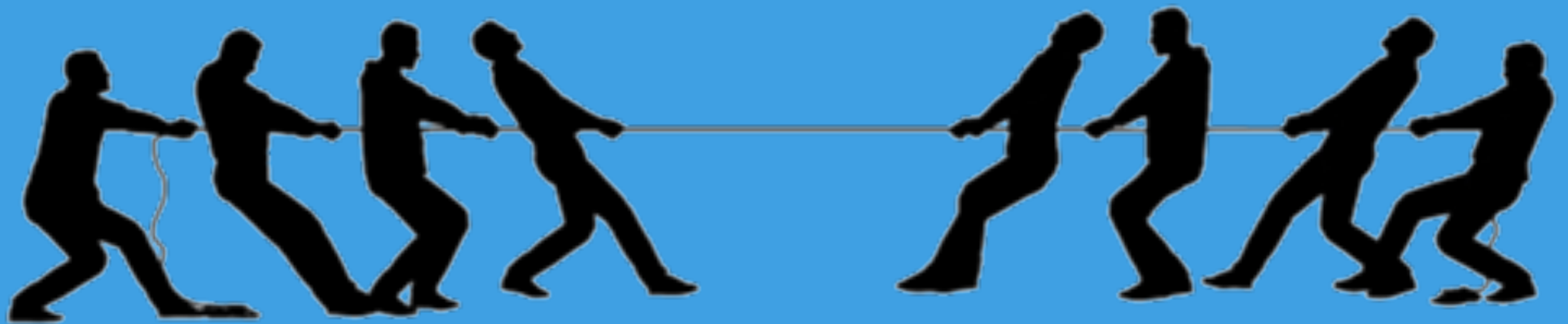
**Raw innovation**  
Innovation at  
any cost

**Quality?**  
**Security?**

**Net innovation**  
Net value to the  
organization

**Maintainability?**

**Repeatability?**

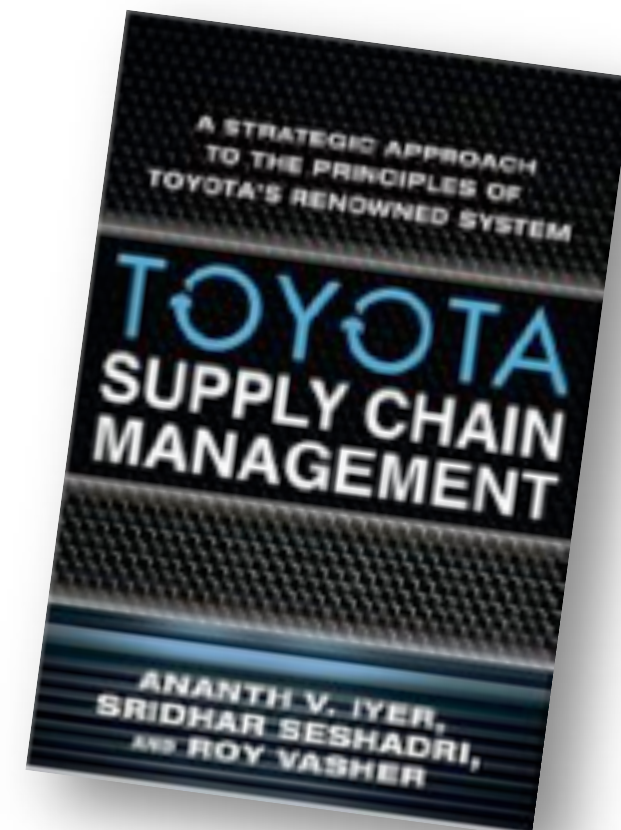




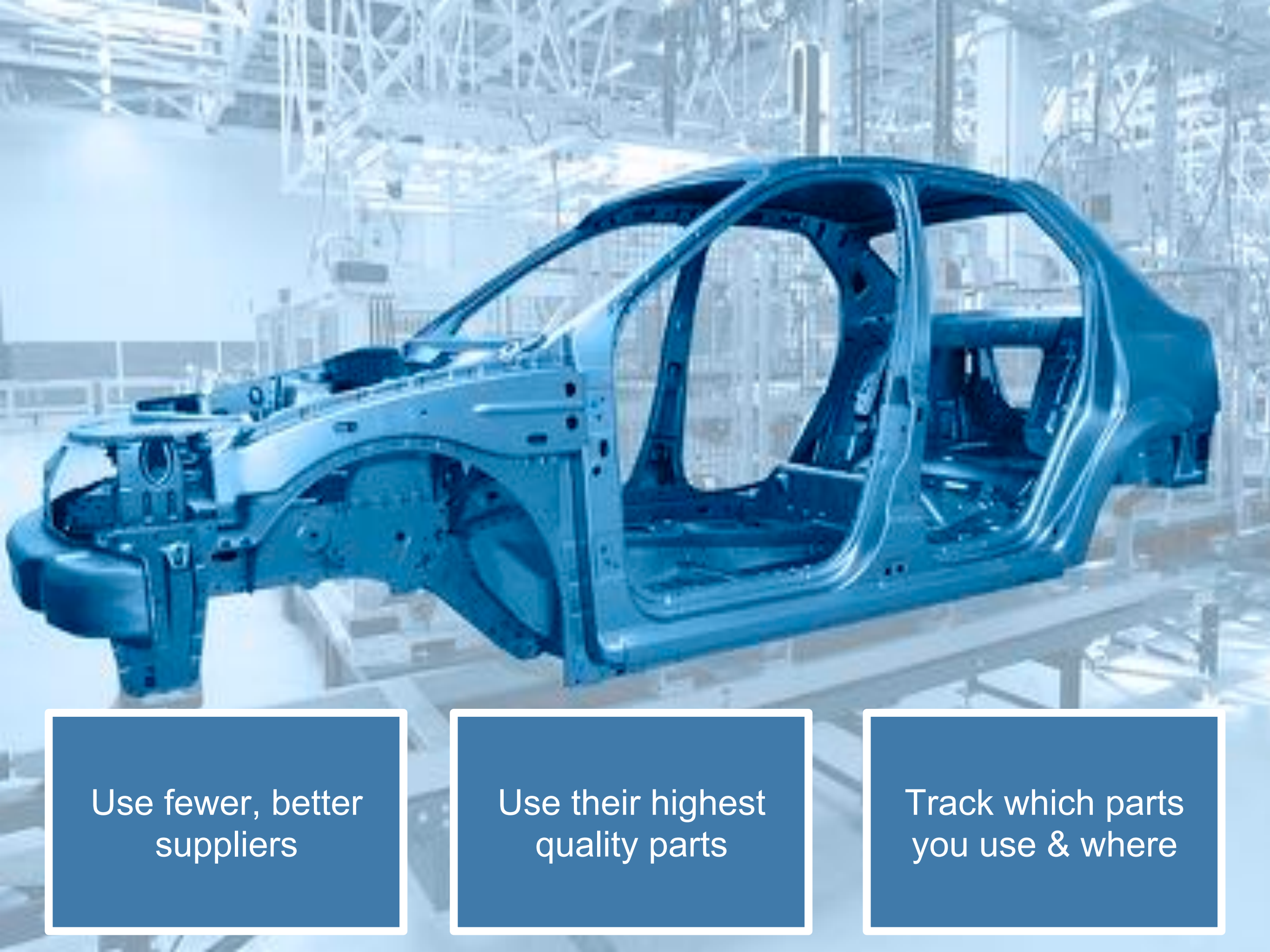


# Supply chain advantage

	Toyota Advantage	Toyota Prius	Chevy Volt
Unit Retail Price	<b>61%</b>	\$24,200	\$39,900
Units Sold/Month	<b>13x</b>	23,294	1,788
In-House Production	<b>50%</b>	27%	54%
Plant Suppliers	<b>16%</b>	125	800
<i>Firm-Wide Suppliers</i>	<b>4%</b>	224	5,500



Source: Toyota Supply Chain Management: A Strategic Approach to Toyota's Renowned System, by Ananth Iyer and Sridhar Seshadri



Use fewer, better  
suppliers

Use their highest  
quality parts

Track which parts  
you use & where



# Demo?

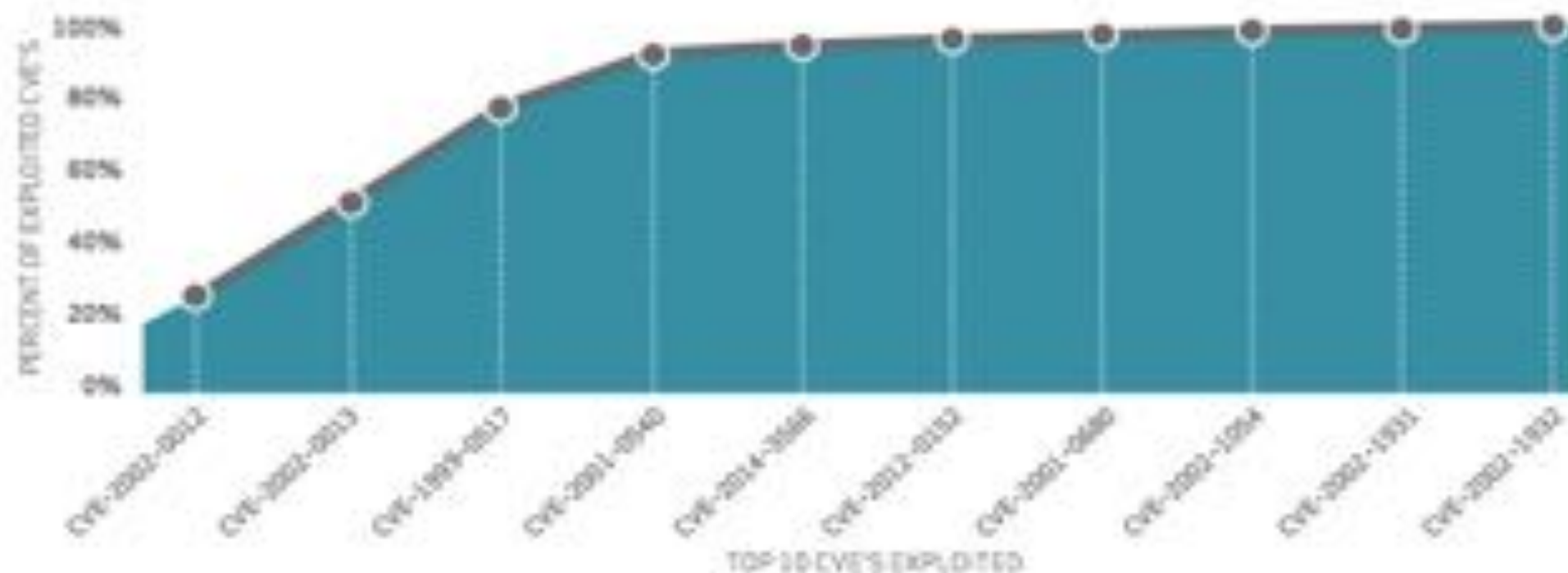
#DOES15

# Actual Exploitation 2015 VZ DBIR

## NOT ALL CVEs ARE CREATED EQUAL.

If we look at the frequency of exploitation in Figure 11, we see a much different picture than what's shown by the raw vulnerability count of Figure 12. **Ten CVEs account for almost 97%** of the exploits observed in 2014. While that's a pretty amazing statistic, don't be lulled into thinking you've found an easy way out of the vulnerability remediation rodeo. Prioritization will definitely help from a risk-cutting perspective, but beyond the top 10 are 7 million other exploited vulnerabilities that may need to be ridden down. And therein, of course, lies the challenge: once the "mega-vulns" are roped in (assuming you could identify them ahead of time), how do you approach addressing the rest of the horde in an orderly, comprehensive, and continuous manner over time?

*About half of the CVEs exploited in 2014 went from publish to pwn in less than a month.*



**Figure 11.**

Cumulative percentage of exploited vulnerabilities by top 10 CVEs



Less unplanned,  
unscheduled work

Fewer service  
interruptions

Faster MTTD &  
MTTR













*“Operational pain can neither  
be created nor destroyed -  
only moved to someone else”*

*-Nick Galbreath*

*“Well... you can create it... :)”*

*-Joshua Corman*



# **Immutable Awesomeness?: Where Containers Collide with SW Supply Chains**

John Willis

Director of Ecosystem Development

# Guns Germs and Microservices

## The New Guns, Germs and Steel





# Immutable Infrastructure

**NETFLIX**

The Netflix Tech Blog

Saturday, August 13, 2011

## Building with Legos

In the six years that I have been involved in building and releasing software I evolved and improved significantly. When I started, we would build a WAR, deploy it to a production host, and then run a script that would stop tomcat on the host, backup the structure and then start tomcat again. Each host would be manually pushed with very few hosts this took quite some time and a lot of human interaction.

Our next iteration was an improvement in automation, but not really in architecture. We built a tool that would handle the process of stopping and starting things as well as extracting the new code. This meant that people could push to a number of hosts with a few check boxes. The tests to make sure that the servers were back up before pushing were automated and have failsafes in the tool.

Links

[Netflix US & Canada Blog](#)

MARTIN FOWLER

[Intro](#) [Videos](#) [Design](#) [Agile](#) [Refactoring](#) [NoSQL](#) [DSL](#) [Continuous Delivery](#) [Microservices](#)

## ImmutableServer



Kief Morris

13 June 2013

Automated configuration tools (such as [CFEngine](#), [Puppet](#), or [Chef](#)) allow you to specify how servers should be configured, and bring new and existing machines into compliance. This helps to avoid the problem of fragile [SnowflakeServers](#). Such tools can create [PhoenixServers](#) that can be torn down and rebuilt at will. An Immutable Server is the logical conclusion of this approach, a server that once deployed, is never modified, merely replaced with a new updated instance.

@bg1pe

# Immutable Matters

## **Why Order Matters: Turing Equivalence in Automated Systems Administration**

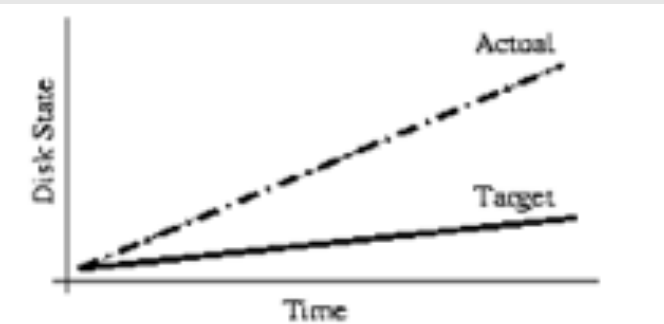
*Steve Traugott - TerraLuna, LLC  
Lance Brown - National Institute of Environmental Health Sciences*

*Pp. 99-120 of the **Proceedings of LISA '02: Sixteenth Systems Administration Conference**,  
(Berkeley, CA: USENIX Association, 2002).*

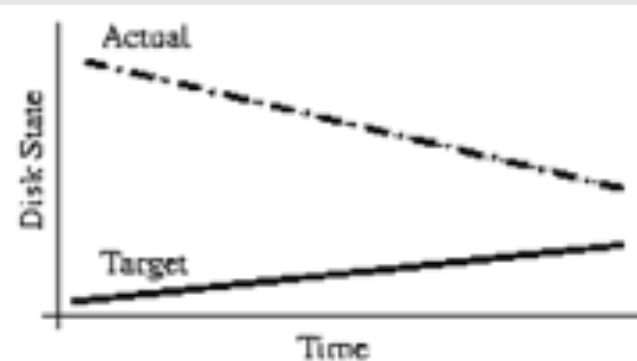
“The least-cost way to ensure that the behavior of any two hosts will remain completely identical is always to implement the same changes in the same order on both hosts.”

# Management Methods

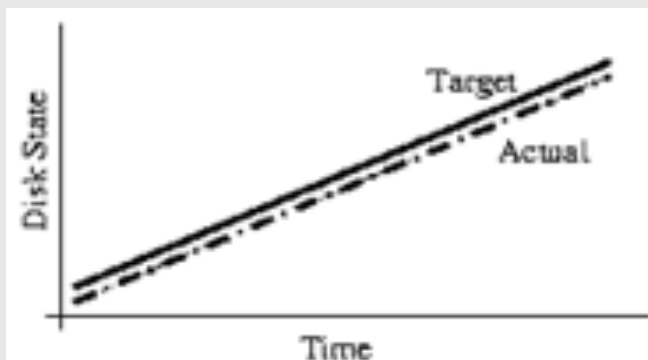
- Divergence
- Convergence
- Congruence



**Figure 1: Divergence.**



**Figure 2: Convergence.**



**Figure 3: Congruence.**



# Immutable Delivery

**Gartner.**

WHY GARTNER ANALYSTS RESEARCH EVENTS CONSULTING ABOUT

## Assessing Docker and Containers for Five Software Delivery Use Cases

🕒 27 April 2015 📄 G00275476

Analyst(s): [Richard Watson](#)

### Summary

Docker offers application-focused, container-based virtualization to DevOps-minded developers and administrators. This document assesses Docker for use cases spanning development and test, continuous integration (CI), production deployment, and building private PaaS.

Already have an account?

Sign in to view this document

Enter Username

Enter Password

**SIGN IN**

Forgot your password?



What is Docker?

Use Cases

Try It

Install & Docs

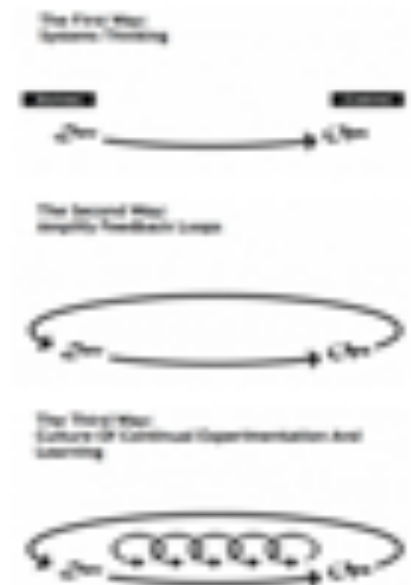
Blog

May 26, 2015

## DOCKER AND THE THREE WAYS OF DEVOPS

written by John Willis, Evangelist at Docker

Have you read [Gene Kim's The Phoenix Project](#)? Some of the principles behind the Phoenix Project and an upcoming book I am co-authoring with Gene (The DevOps Cookbook) have been referred to as the "Three Ways of DevOps". These are particular patterns of applying DevOps principles in a way that yields high performance outcomes.



We assert that the Three Ways describe the values and philosophies that frame the processes, procedures, practices of DevOps, as well as the prescriptive steps.

Gene Kim

Immutable  
Infrastructure  
Myth

Lead Time

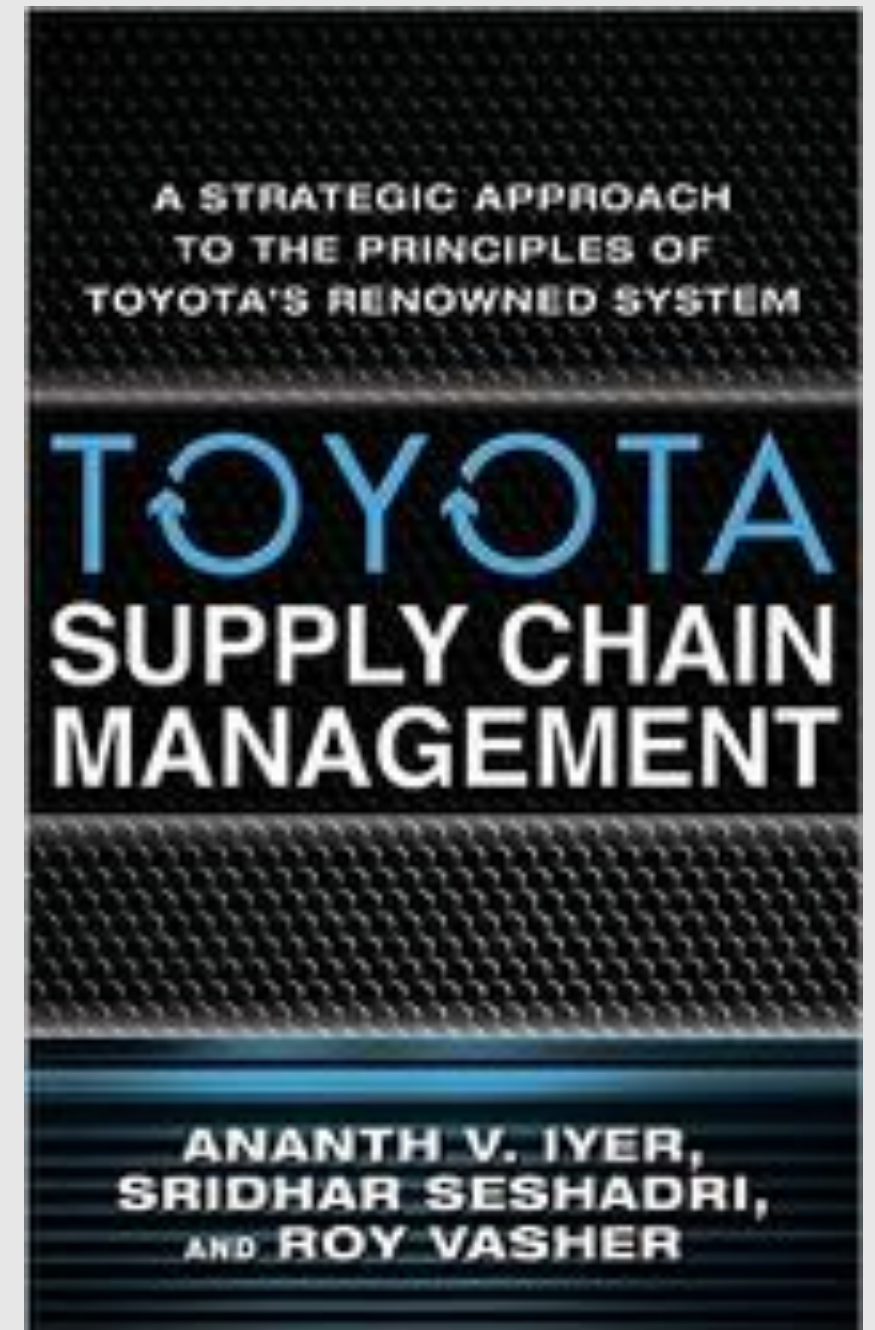
Shorten





# V4L : Left to Right Flow

- ↑ • **Variety**
  - Determine your variety of offerings based on operational efficiency and market demand
- ↑ • **Velocity**
  - Maintain a steady flow through all processes of the supply chain
- ↓ • **Variability**
  - Manage inconsistencies carefully to reduce cost and improve quality
- ↑ • **Visibility**
  - Ensure the transparency of all processes to enable continuous learning and improvement



# Left to Right Flow

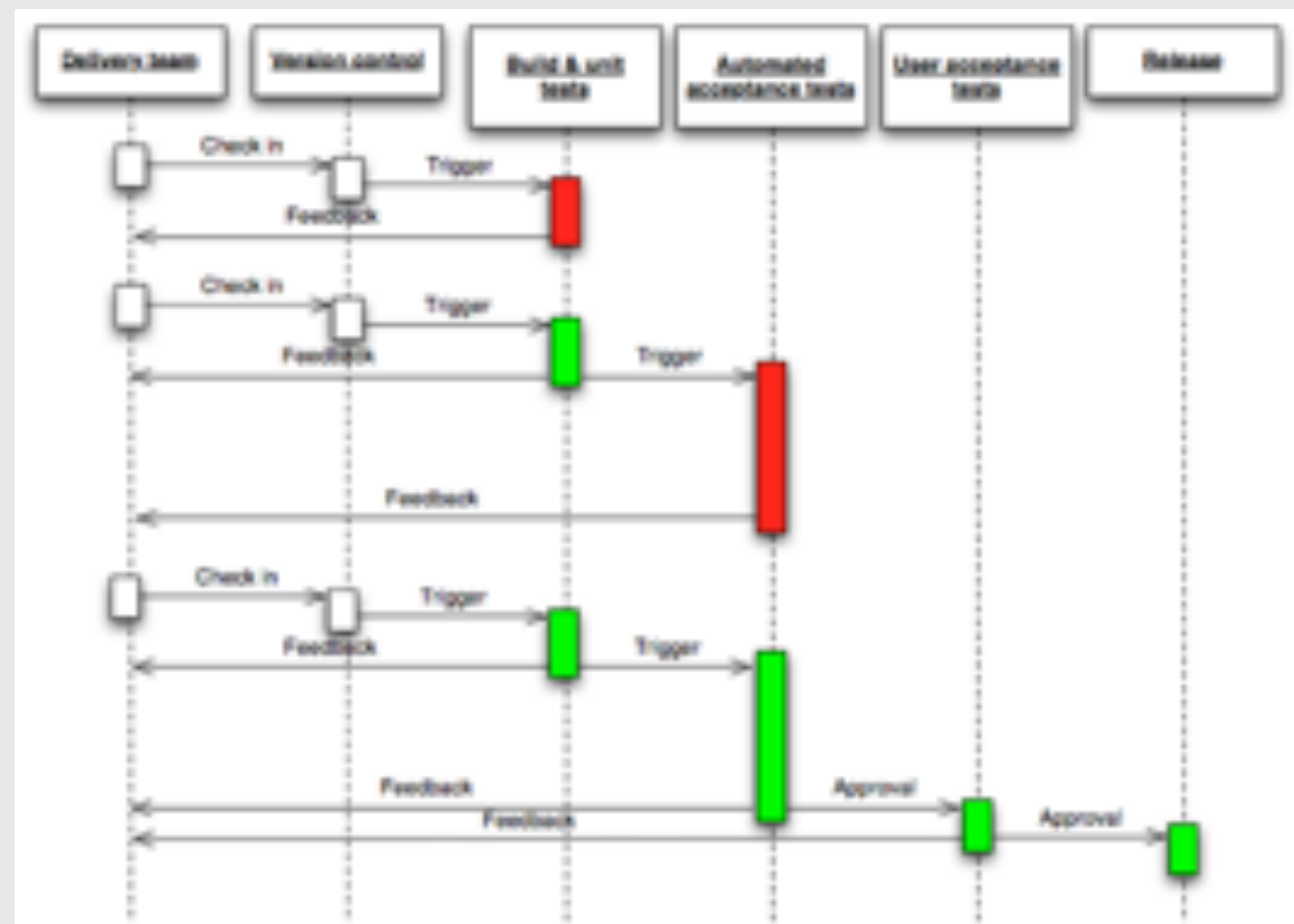
- **Variety**

- **Lean Startup**
- **Minimal Viable Product**
- **Pivot**
- **Build Measure Learn**
- **Customer Development Methodology**



# Left to Right Flow

- **Velocity**
- Developer Flow
- Integration Flow
- Deployment Flow

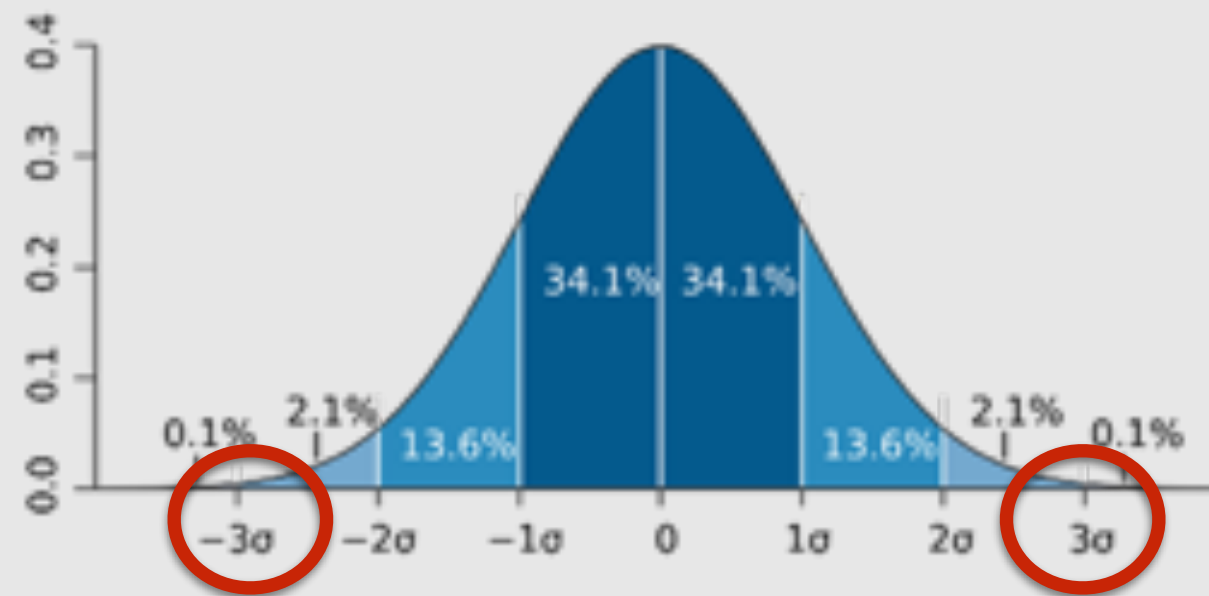


[https://upload.wikimedia.org/wikipedia/commons/7/74/Continuous\\_Delivery\\_process\\_diagram.png](https://upload.wikimedia.org/wikipedia/commons/7/74/Continuous_Delivery_process_diagram.png)



# Left to Right Flow

- **Variation**
  - Converged Isolation
  - Immutable Infrastructure
  - Immutable Delivery



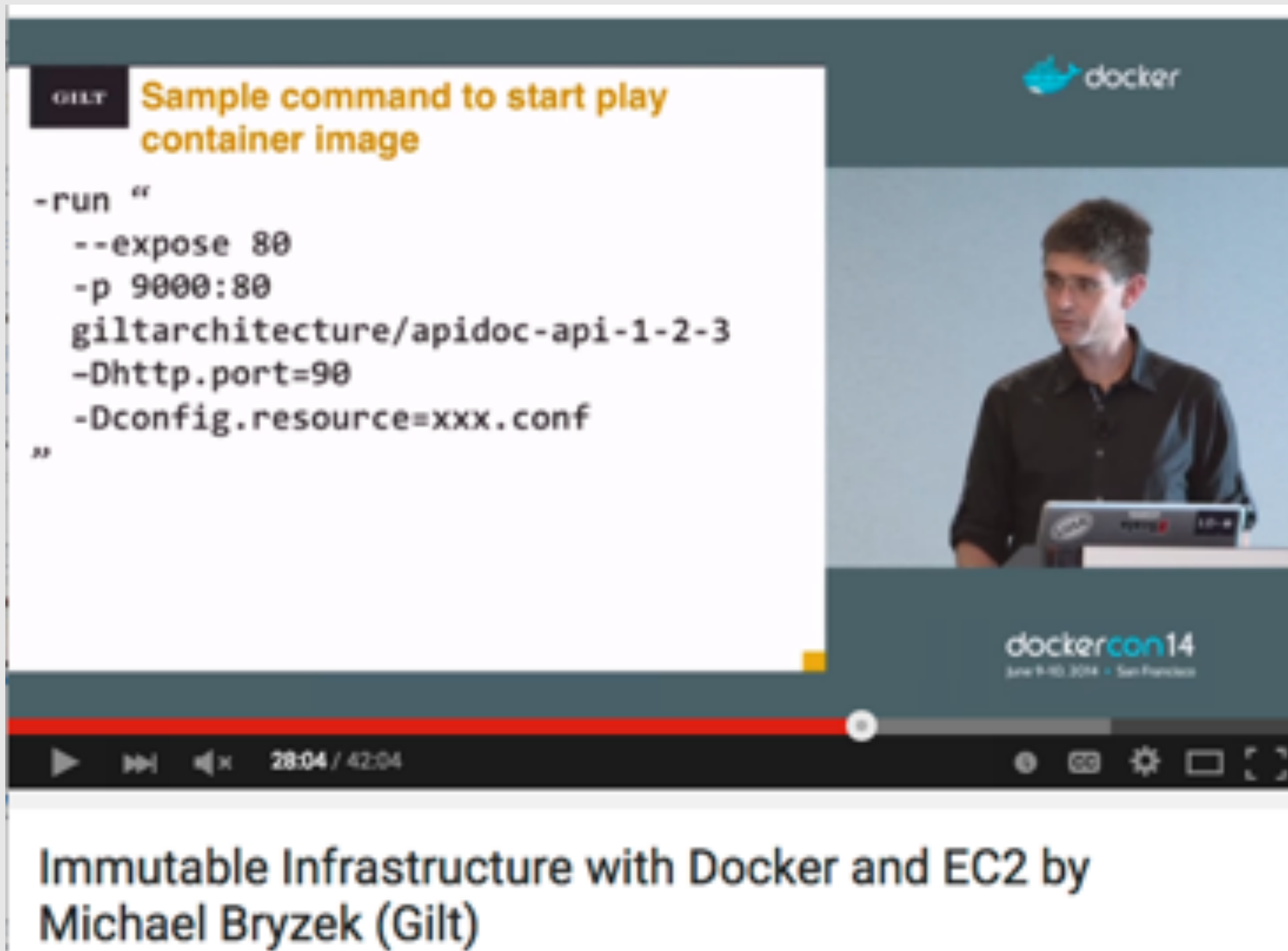
[https://en.wikipedia.org/wiki/Standard\\_deviation](https://en.wikipedia.org/wiki/Standard_deviation)

# Left to Right Flow

- **Visibility**
  - Containerization
  - Microservices
  - Data Gravity



# Case Studies



The image shows a video player interface for a presentation. The main content area is a slide with a dark blue header and a white code block. The slide header includes the Docker logo and the text 'dockercon14 June 9-10, 2014 - San Francisco'. The code block contains a sample command to start a Play container image. The video player controls at the bottom show a progress bar at 28:04 / 42:04 and various playback icons.

**GILT** Sample command to start play container image

```
-run "  
  --expose 80  
  -p 9000:80  
  giltarchitecture/apidoc-api-1-2-3  
  -Dhttp.port=90  
  -Dconfig.resource=xxx.conf  
"
```

dockercon14  
June 9-10, 2014 - San Francisco

28:04 / 42:04

Immutable Infrastructure with Docker and EC2 by Michael Bryzek (Gilt)







# References

**DOCKER AND THE THREE WAYS OF DEVOPS PART 1: THE FIRST WAY – SYSTEMS THINKING**  
<https://blog.docker.com/2015/05/docker-three-ways-devops/>

**DevOpsDays Chicago Sept 2015 - State of the DevOps by John Willis**  
<https://www.youtube.com/watch?t=16&v=319wlaAiaHM>

**Guns Germs and Microservices**  
<https://vimeo.com/129822162>

**Become More Agile and Get Ready for DevOps by Using Docker in Your Continuous Integration Environments**  
<https://www.gartner.com/doc/3016317/agile-ready-devops-using-docker>

**The Phoenix Project: A Novel about IT, DevOps, and Helping Your Business Win**  
<http://www.amazon.com/The-Phoenix-Project-Helping-Business/dp/0988262592>

**Immutable Infrastructure with Docker and EC2 by Michael Bryzek (Gilt)**  
<https://www.youtube.com/watch?v=GaHzdqFithc>

**Toyota Kata: Managing People for Improvement, Adaptiveness and Superior Results**  
<http://www.amazon.com/Toyota-Kata-Managing-Improvement-Adaptiveness/dp/0071635238>





[jcorman@sonatype.com](mailto:jcorman@sonatype.com)  
[@joshcorman](#)



[john.willis@docker.com](mailto:john.willis@docker.com)  
[@botchagalupe](#)