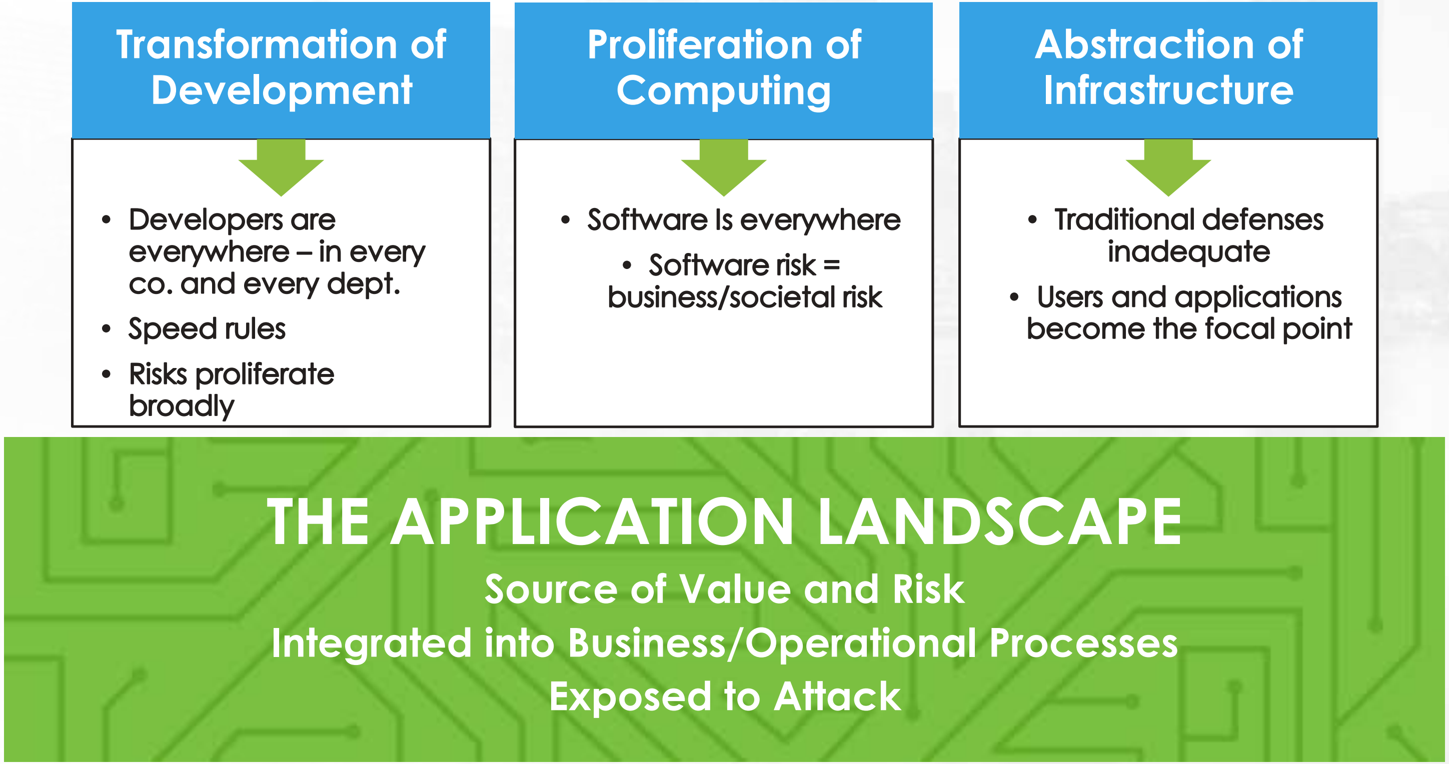
How to integrate application security into the development lifecycle and achieve a positive ROI

Julian Totzek-Hallhuber, Pricipal Solutions Architect

Market Trends Put Applications in the Crosshairs



Transformation of Development

- Developers are everywhere – in every co. and every dept.
- Speed rules
- Risks proliferate broadly

Proliferation of Computing

- Software Is everywhere
- Software risk = business/societal risk

Abstraction of Infrastructure

- Traditional defenses inadequate
- Users and applications become the focal point

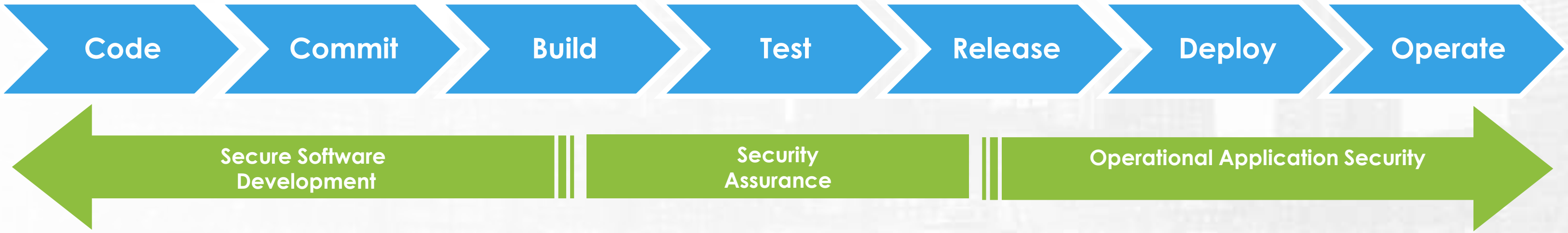
THE APPLICATION LANDSCAPE

Source of Value and Risk

Integrated into Business/Operational Processes

Exposed to Attack

Impact on Application Security: Shift Left and Shift Right



Code

Commit

Build

Test

Release

Deploy

Operate

Secure Software Development

Security Assurance

Operational Application Security

DEVELOPER- DRIVEN

- Emphasis on immediacy of results, automation and integrations

SECURITY-DRIVEN

- Emphasis on regulatory and compliance requirements
- Focus on internal and third-party risks

OPERATIONS_DRIVEN

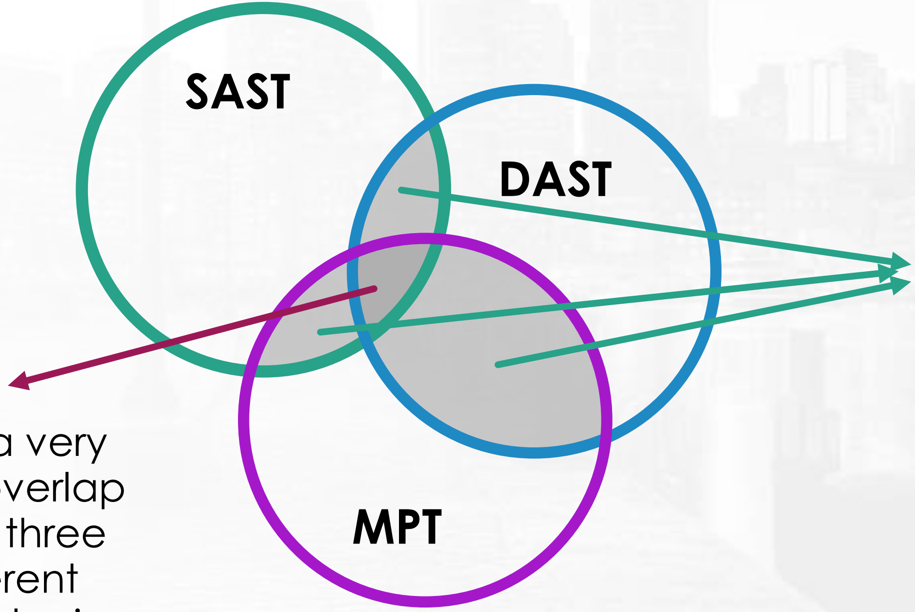
- Emphasis on vulnerability management and protection

Prevention

Governance

Protection

Differences manual and automated testing

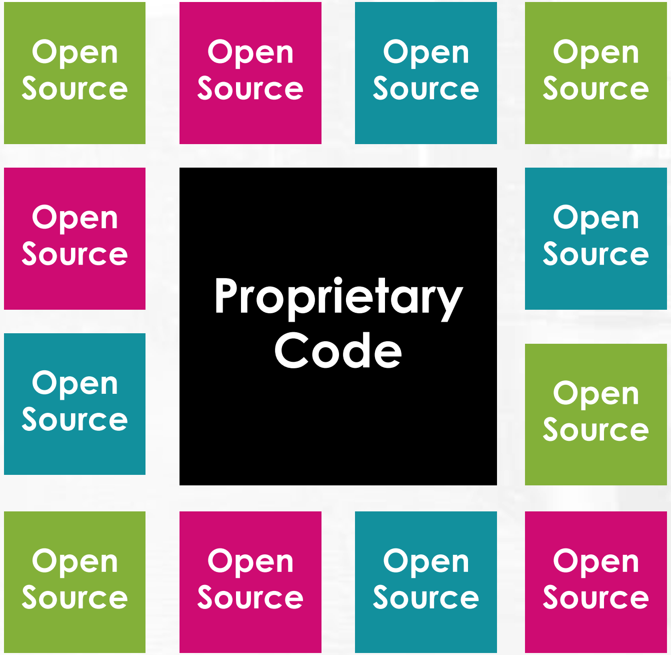


Only a very small overlap for all three different technologies

Overlap of the different technologies.

Each technology is able to identify different things

Today’s Applications Are Assembled



Open Source

Open Source

Open Source

Open Source

Open Source

Proprietary Code

Open Source

Open Source

Open Source

Open Source

Open Source

Open Source

Open Source

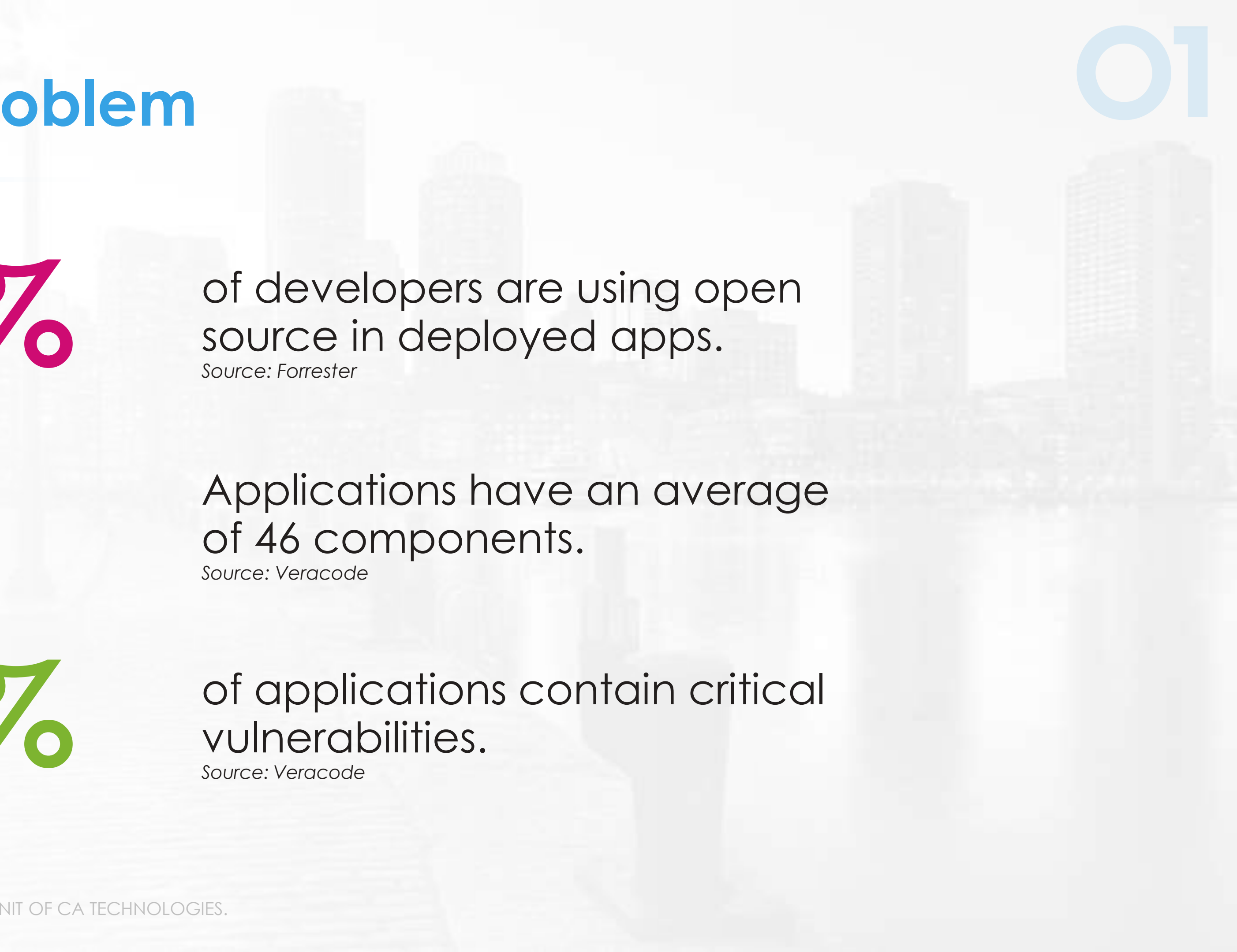
Food for Thought
How do you inventory open source libraries in your applications today?

Application Security Testing Methods

Capabilities	Static Analysis	Software Composition Analysis	Dynamic Analysis	Manual Penetration Testing
Flaws in Custom Web Apps (CWEs)	✓		✓	✓
Flaws in Custom non-Web Apps (CWEs)	✓			✓
Flaws in Custom Mobile Apps (CWEs)	✓			✓
Known Vulnerabilities in Open Source Components (CVEs)		✓		✓
Behavioral Issues (CWEs)	✓			✓
Configuration Errors (CWEs)			✓	✓
Business Logic Flaws (CWEs)				✓
Can be automated (scalability, cost, speed)	✓	✓	✓	

Sizing The Problem

01



80% of developers are using open source in deployed apps.

Source: Forrester

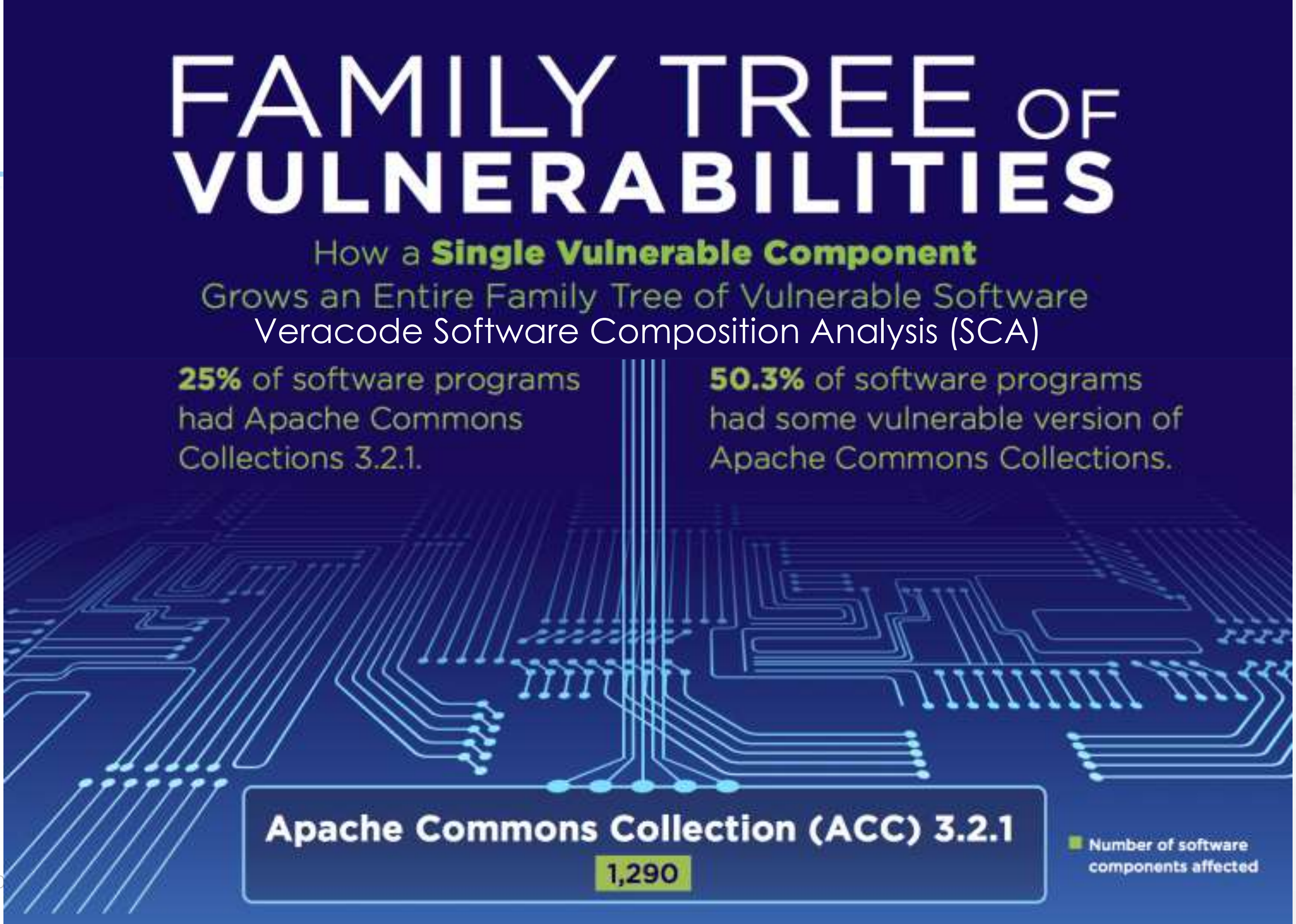
46 Applications have an average of 46 components.

Source: Veracode

44% of applications contain critical vulnerabilities.

Source: Veracode

Veracode Software Composition Analysis (SCA)



FAMILY TREE OF VULNERABILITIES

How a **Single Vulnerable Component** Grows an Entire Family Tree of Vulnerable Software

25% of software programs had Apache Commons Collections 3.2.1.

50.3% of software programs had some vulnerable version of Apache Commons Collections.

Apache Commons Collection (ACC) 3.2.1

1,290

🟩 Number of software components affected

Different Teams have Different AppSec Needs

DEV

- Time to Market
- Ease of Use
- Education

OPS

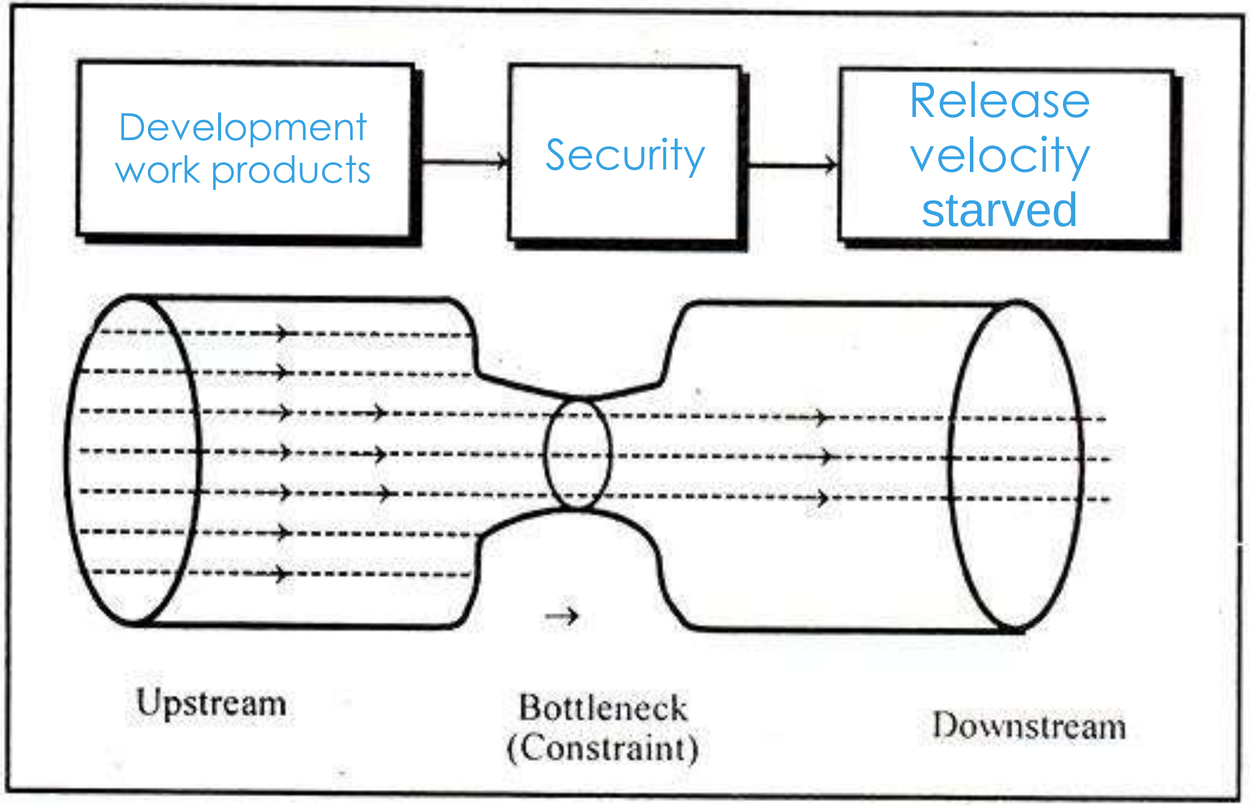
- Visibility
- Performance
- Protection

SEC

- Risk Reduction
- Compliance
- Scalability

Culture clash revisited

01

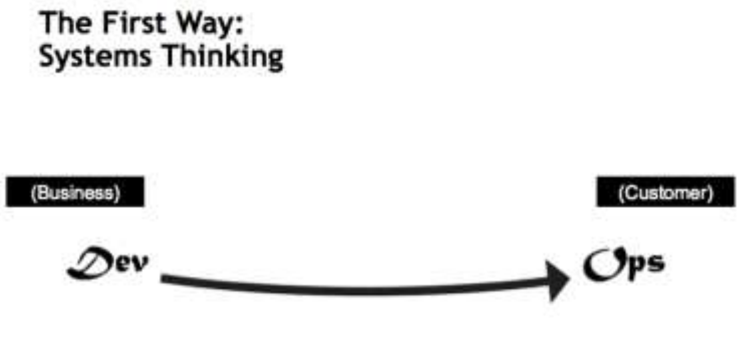


Development work products

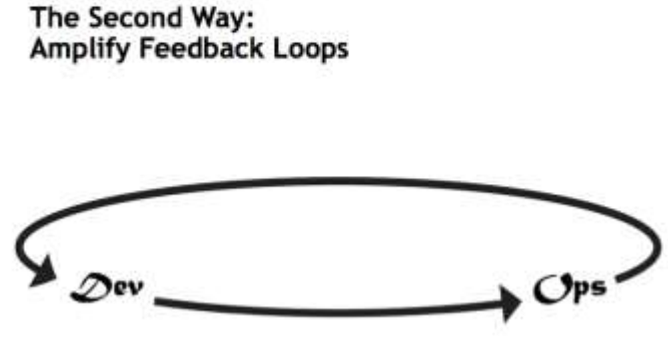
Security

Release velocity starved

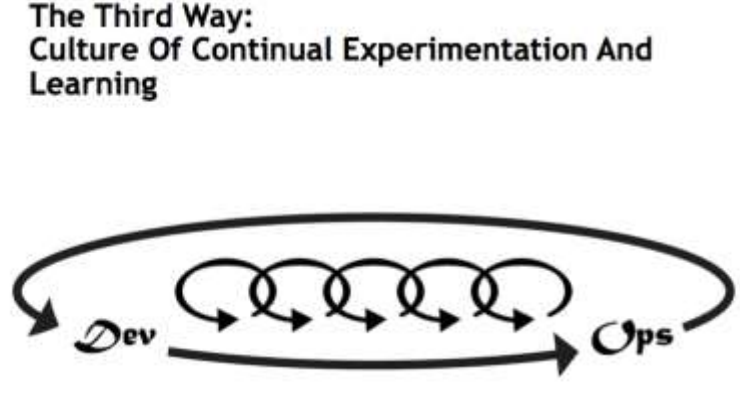
3 ways



The First Way:
Systems Thinking



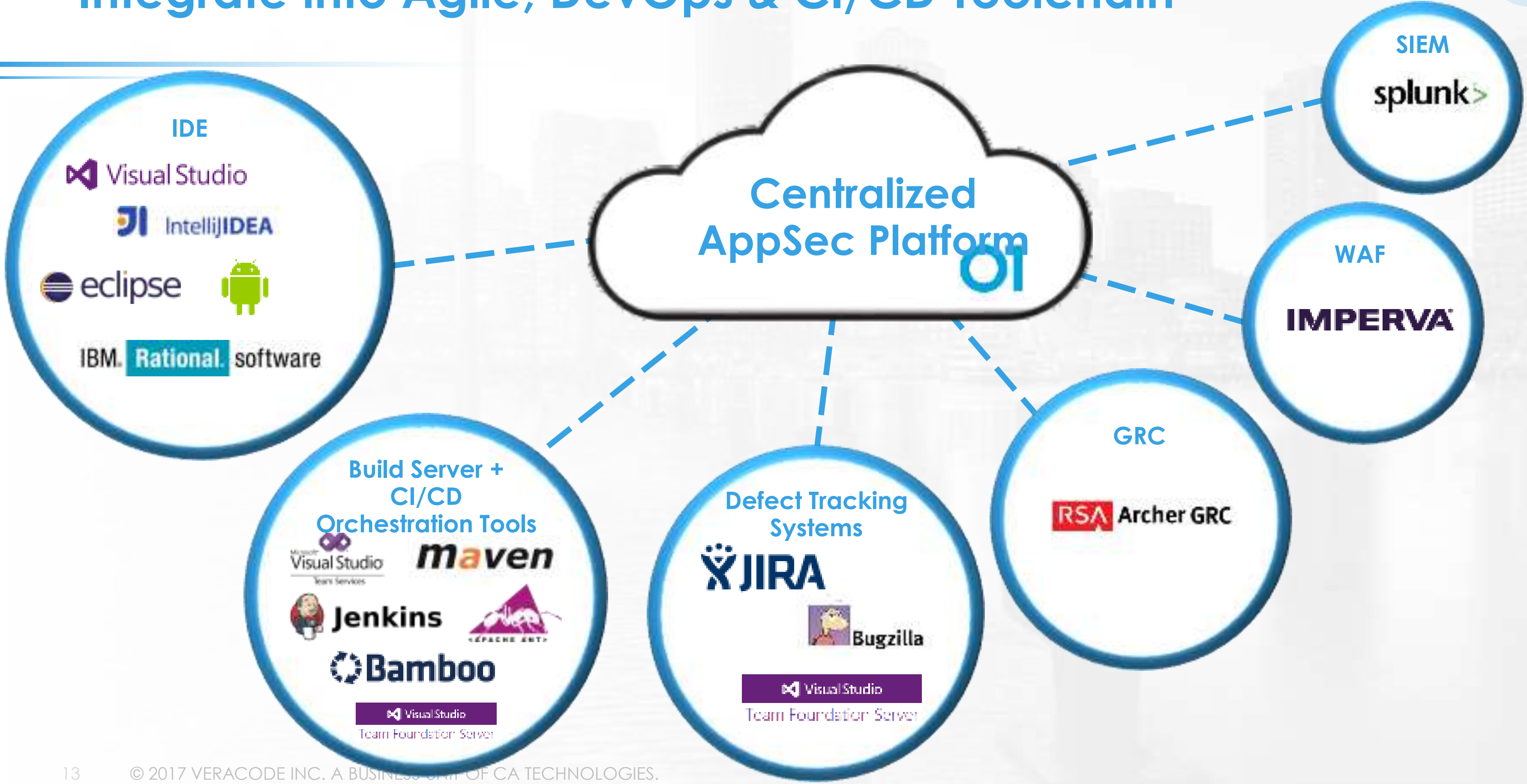
The Second Way:
Amplify Feedback Loops



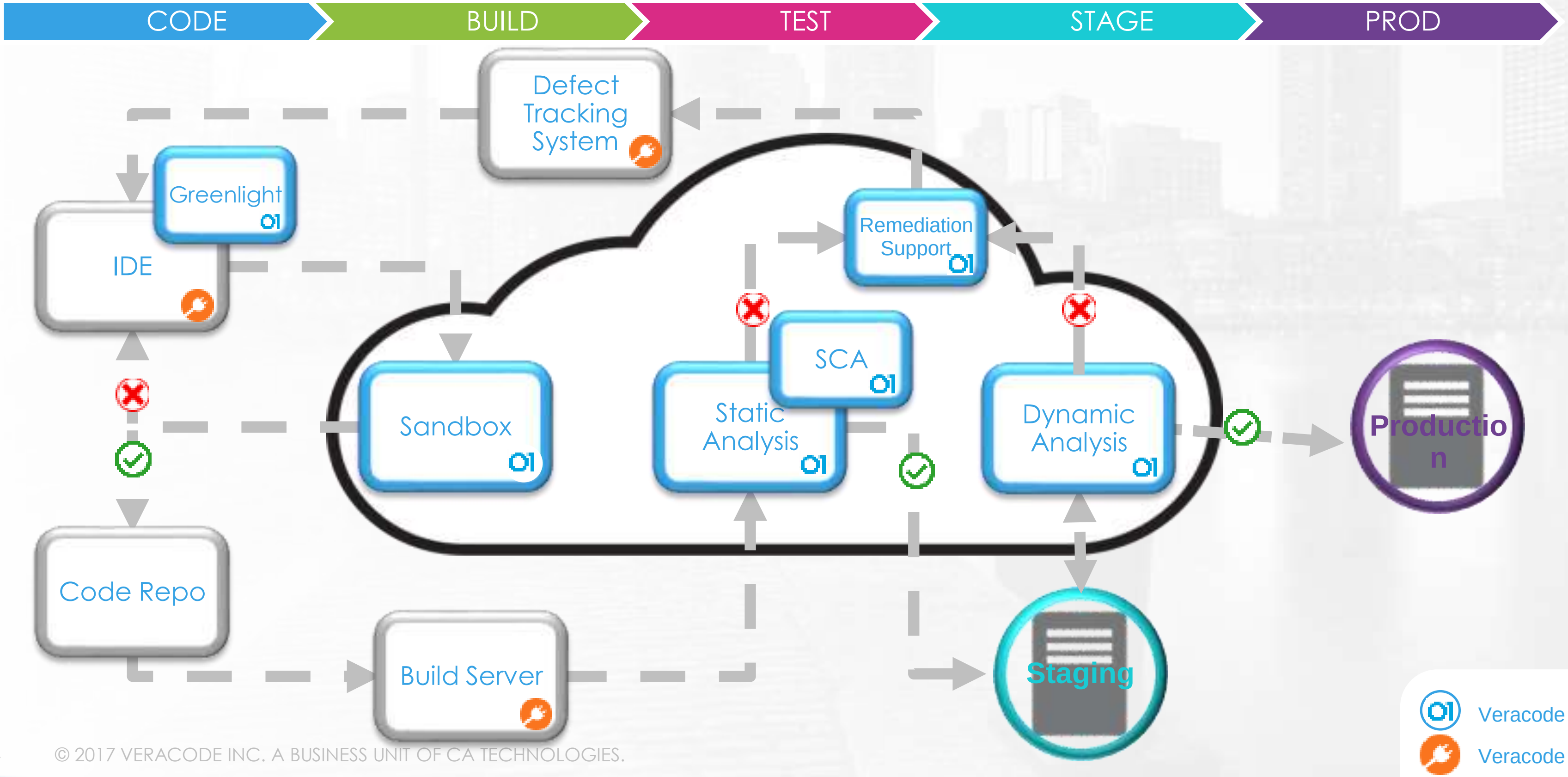
The Third Way:
Culture Of Continual Experimentation And Learning

Credit: Gene Kim, IT Revolution

Integrate into Agile, DevOps & CI/CD Toolchain


Centralized AppSec Platform
IDE
Visual Studio
IntelliJIDEA
eclipse
IBM. Rational. software
Build Server + CI/CD Orchestration Tools
Microsoft Visual Studio Team Services
maven
Jenkins
APACHE ANT
Bamboo
Visual Studio Team Foundation Server
Defect Tracking Systems
JIRA
Bugzilla
Visual Studio Team Foundation Server
GRC
RSA Archer GRC
WAF
IMPERVA
SIEM
splunk>

Automate Security into Existing SDLC



Cloud vs on premise

Trusted, Scalable, Capable, Automated & Fix-Rates

False Positives

Industry leading low FP Rates

Maintenance & Operations

Zero operational or maintenance cost, no HW needed

Scalability

Simple Scan & Fix scaling to 1,000's Apps

Integrations

Extensive API & Plugins into Dev Pipeline

Security

SOC 2 & 3 certified, encryption, HR security, data security

Reporting

Big Data analytics to improve and spot opportunity.

Cost Savings

Faster time to market, less flaws per MB

Continuous Improvement

Automated updates once a month

Being the CISO integrating security without blocking and huge cost savings

01

192% ROI using Veracode

FEWER VULNERABILITIES with LOWER REMEDIATION COST Per Vulnerability

BEFORE VERACODE

$70 per vulnerability, 50 vulnerabilities per megabyte (for outsourced code)

WITH VERACODE

$10 per vulnerability, 20 or less vulnerabilities per megabyte (for outsourced code)

GLOBAL 2000 FIRM ACHIEVES

192% ROI

SECURING CRITICAL FINANCIAL APPLICATIONS WITH VERACODE'S **CLOUD-BASED SERVICE**

BENEFITS: AVOIDED COST, REDUCED RISK, AND IMPROVED MARGINS

ROI	NPV (3 Years)	Application Vulnerabilities
192%	$11,522,027	↓ 60%

$1.98M per year

SAVINGS: OUTSOURCED CODE: Avoided costs of $1.98 million per year in identifying, tracking and mitigating vulnerabilities in applications developed by outsourced developers.

$3M per year

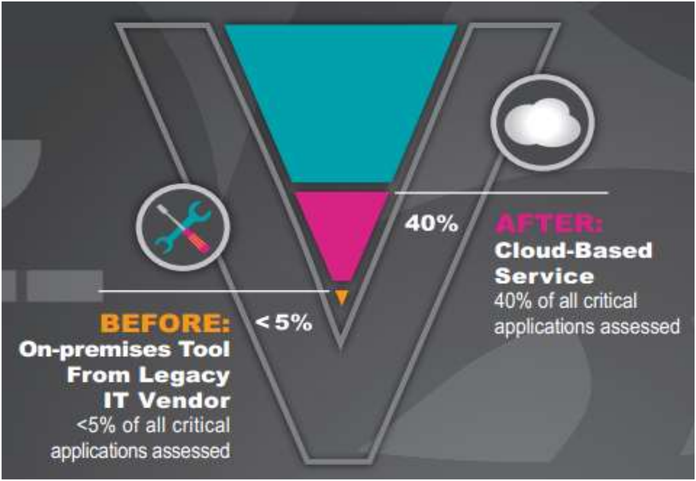
SAVINGS: INTERNALLY-DEVELOPED AND LEGACY CODE: Avoided costs of $3 million per year by remediating vulnerabilities earlier in the SDLC.

$630K per year

SAVINGS: REDUCED ENTERPRISE RISK: Avoided potential breach costs of $630,000 per year via reduced application-layer risk.

$1-2M per year

IMPROVED MARGINS: IMPROVED TIME-TO-MARKET: Improved development skill, speed, and best practices leading to reduced costs and improved margins totaling $1-2 million per year.



AFTER: Cloud-Based Service
40% of all critical applications assessed

BEFORE: On-premises Tool From Legacy IT Vendor
<5% of all critical applications assessed

01

EAT
SLEEP
IMPROVE
REPEAT
DanciaKS

Thank you