



# ***Information Security: Enabling the Business***

## **Developing an Effective Application Security Program**

Bruce C Jenkins (bcj@hp.com)

AppSec Program Strategist

04 April 2014

# About me

- **28 years US Air Force (SW dev, Ops, CISO, CSO, and CIO)**
- **4 ½ years software security pro services**
- **1+ years learning & development (PM)**
- **1 year in current role**



# About my motivation for developing secure systems...



- **2005:** US Air Force personnel system breached; 33K records exfiltrated
- **2006:** VA employee's personal external drive stolen; 26M VA records at risk
- **2012:** Thrift Saving Plan contractor's system attacked; 123K SSNs stolen
- **2013:** Target POS system compromised; up to 70M customers impacted
- **2014:** University of Maryland data breach; 309K records at risk

# About my motivation for developing secure systems...

**FOR IMMEDIATE RELEASE**

May 25, 2012

**FEDERAL RETIREMENT THRIFT INVESTMENT BOARD  
REPORTS A CYBER ATTACK ON A CONTRACTOR  
POTENTIALLY AFFECTING TSP PARTICIPANTS  
*No Indication of Any Improper Use of Data***



FEDERAL RETIREMENT THRIFT INVESTMENT BOARD  
775 Street, NE Washington, DC 20002

**FOR IMMEDIATE RELEASE**  
May 25, 2012

**FEDERAL RETIREMENT THRIFT INVESTMENT BOARD  
REPORTS A CYBER ATTACK ON A CONTRACTOR  
POTENTIALLY AFFECTING TSP PARTICIPANTS  
*No Indication of Any Improper Use of Data***

Washington, D.C. -- The Federal Retirement Thrift Investment Board (FRTIB) announced today that a contractor belonging to Serco Inc., a third party service provider, suffered a sophisticated cyber attack that resulted in unauthorized access of the personal information of approximately 123,000 Thrift Savings Plan (TSP) participants or other recipients of TSP payments. In April of 2012, the FRTIB and Serco were informed of the unauthorized access incident by the Federal Bureau of Investigation (FBI).

There is no indication that any of these data have been misused. In addition, there is no evidence that the network or its website, [www.tsp.gov](http://www.tsp.gov), were affected.

In addition to performing a forensic analysis, the FRTIB and Serco took the following steps: 1) an immediate shutdown of the compromised computer; 2) the formation of a response team that is conducting a systems-wide review of computer security procedures; and 3) enhanced information technology security.

Notification letters are being sent to all affected individuals offering them information on how to contact the call center that has been established to provide assistance and offer services such as credit monitoring. In addition, as a precautionary measure, the FRTIB will place the impacted TSP accounts to ensure that any account activity receives heightened scrutiny.

Washington, D.C. -- The Federal Retirement Thrift Investment Board (FRTIB) announced today that a computer belonging to Serco Inc., a third party service provider, suffered a sophisticated cyber attack that resulted in the unauthorized access of the personal information of approximately 123,000 Thrift Savings Plan (TSP) participants or other recipients of TSP payments. In April of 2012, the FRTIB and Serco were informed of the unauthorized access incident by the Federal Bureau of Investigation (FBI).



# Agenda

**Security Problem Level-set**

**What Matters Most in AppSec (Software Security Assurance) Program Dev**

**(Hint: It's NOT the technology!)**

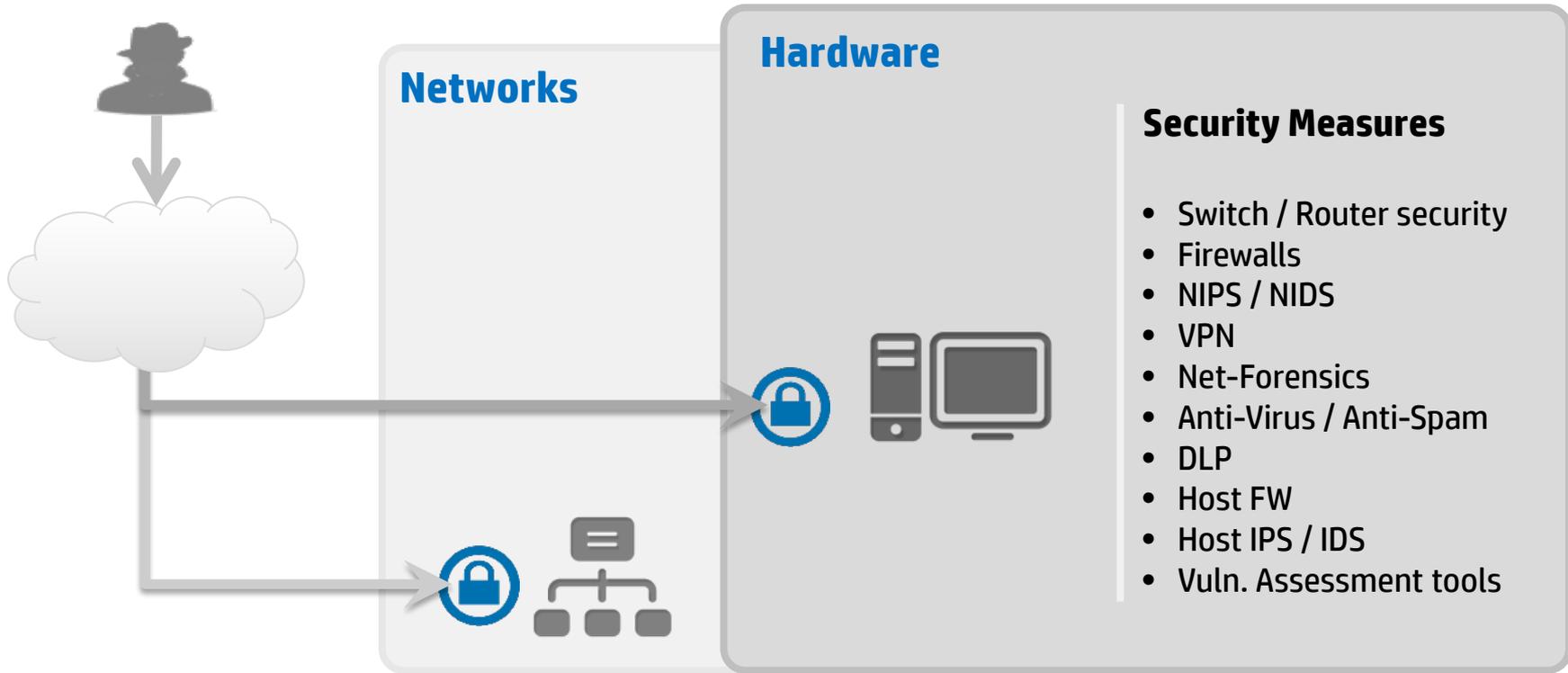
**HP Fortify Solution Overview**



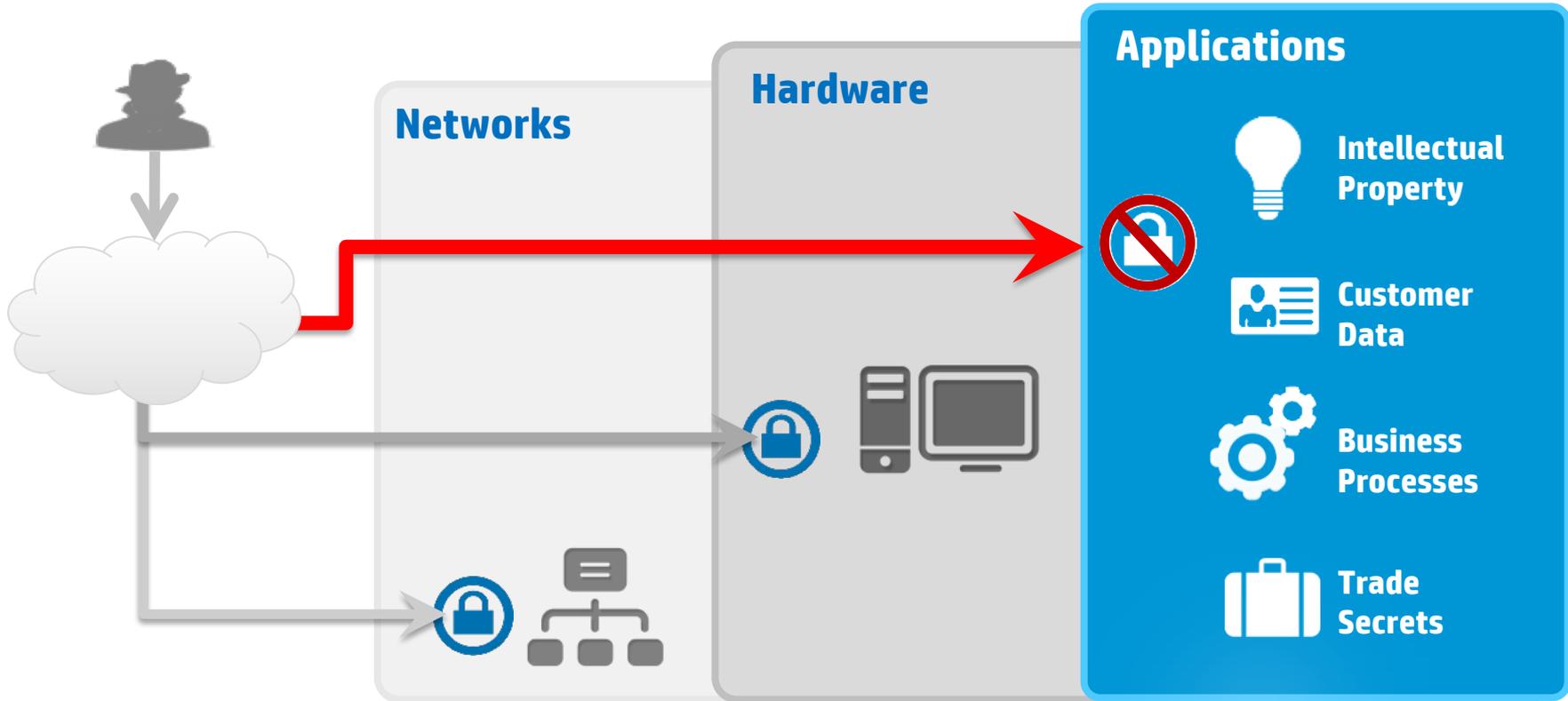
# Problem Level-set



# Cyber attackers are hitting network brick walls...



# So they are targeting applications for best ROI



# 84%

of breaches  
occur at the  
application layer

Gartner, 2013



# What's the worst that could happen?

# SONY®



## PLAYSTATION® Network

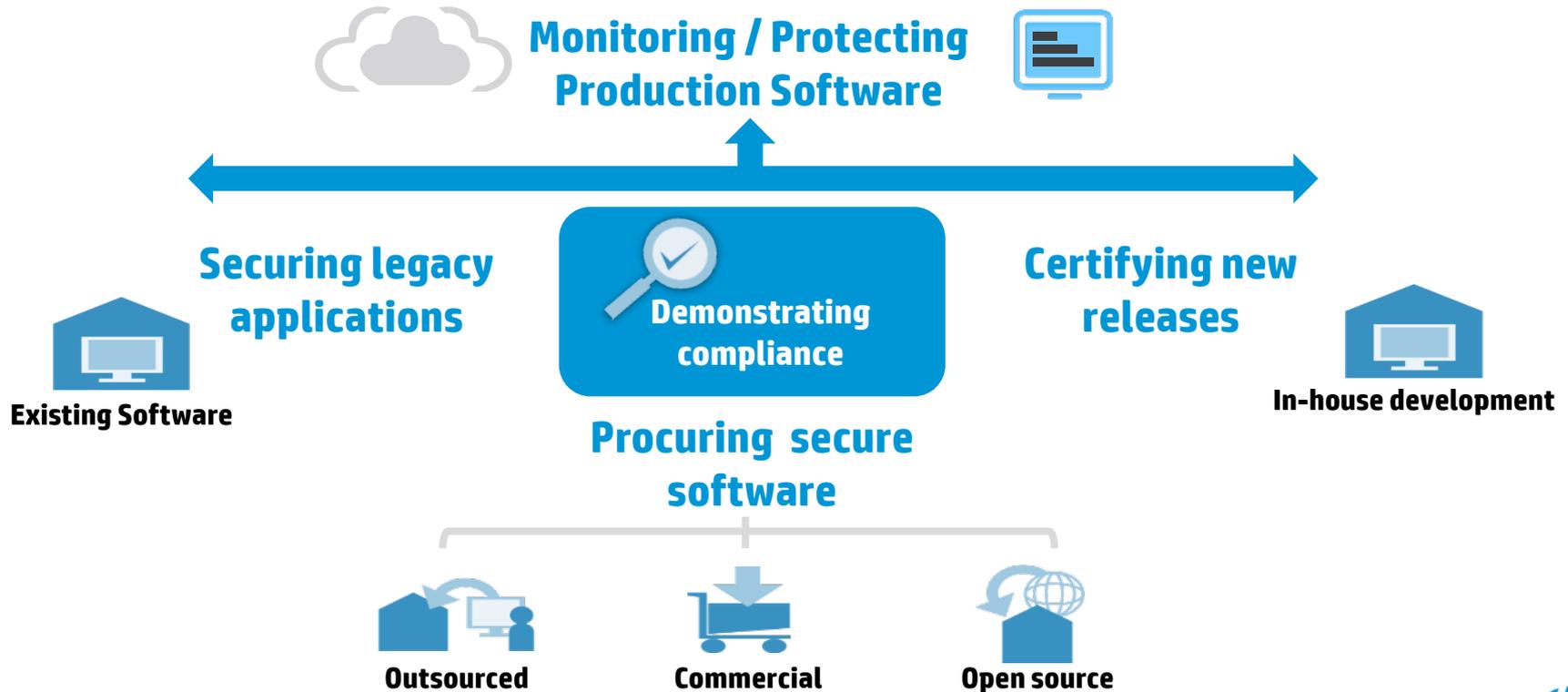
### The Incident

- PlayStation Network breach reported April 2011
- **77M** customer accounts compromised
- PS Network completely offline for **25 days**
- Total cost of damages / loss > **\$171M**  
(+ £250,000 as of Jan 2013)

### The Attack

- DDoS attack followed by **SQL Injection**
- 130+ servers completely compromised
- Account data, credit cards, email addresses stolen
- Required full network shutdown to contain
- More than just PlayStation Network...

# Application security challenges



# Security-related Business Drivers

## Why organizations get involved with application security

**Compliance**

**Third-party Demands (Risk Management)**

**Breach (Avoid Breach)**

**Proactive (Secure the SDLC)**



# Software Security Assurance (SSA): What Matters Most



# Thesis: Without a people-process plan, technology fails

Shelfware can be an expensive proposition

11% of \$325B

*2011 IDC Study*



# Addressing People-Process w/ SW Security Frameworks

A little background

**CLASP [2005]**



# Addressing People-Process w/ SW Security Frameworks

## A little background

CLASP [2005]

**Microsoft SDL [2006]**



# Addressing People-Process w/ SW Security Frameworks

## A little background

CLASP [2005]

Microsoft SDL [2006]

**Software Assurance Maturity Model (SAMM)** [[opensamm.org](https://opensamm.org)]

- Developed by Pravir Chandra, commissioned by then-Fortify Software
- First release: 2008 (Latest release: n/a)
- A prescriptive guide to what works in successful security organizations
  - ➔ *Create a map of where you want to go*



# Addressing People-Process w/ SW Security Frameworks

## A little background

CLASP [2005]

Microsoft SDL [2006]

Software Assurance Maturity Model (SAMM) [[opensamm.org](http://opensamm.org)]

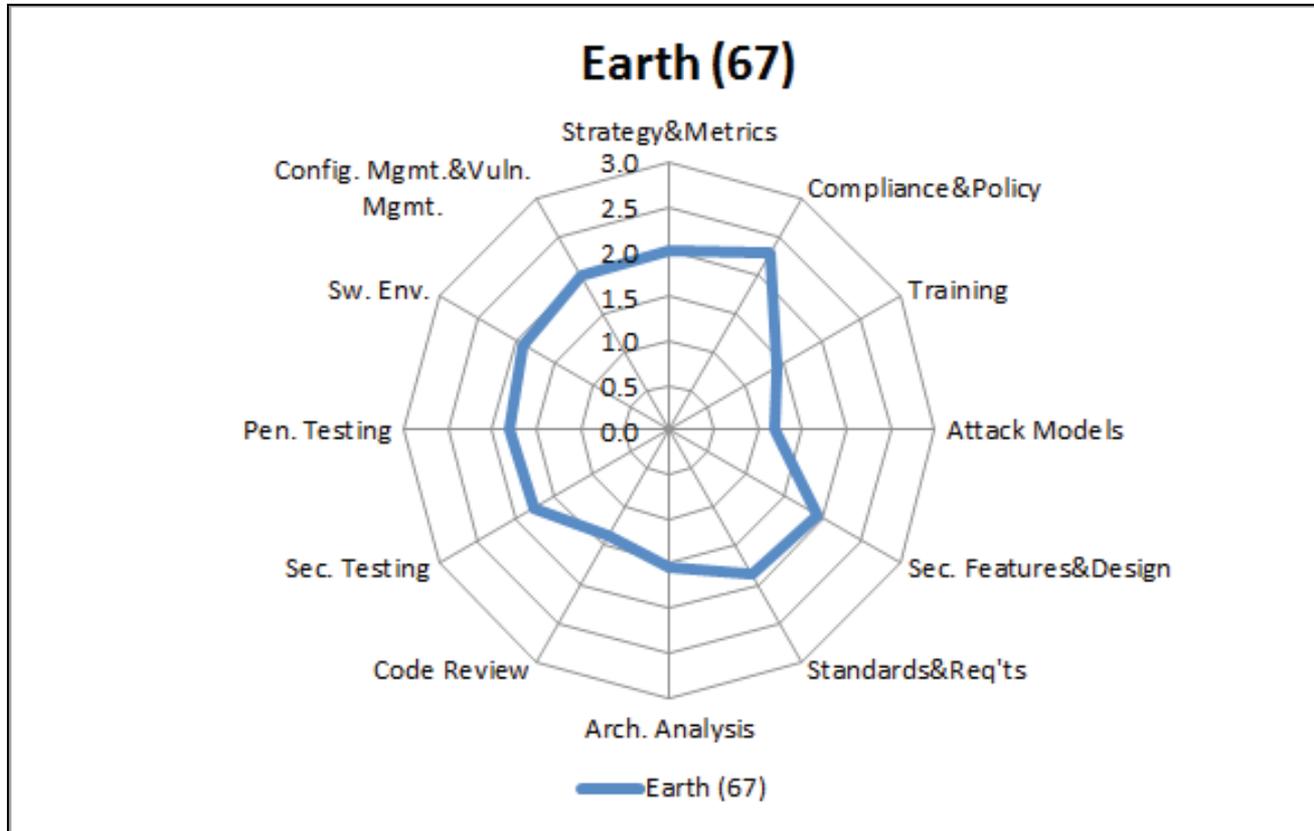
- Developed by Pravir Chandra, commissioned by then-Fortify Software
- First release: 2008 (Latest release: n/a)
- A prescriptive guide to what works in successful security organizations  
→ *Create a map of where you want to go*

Building Security In Maturity Model (BSIMM) [[bsimm.com](http://bsimm.com)]

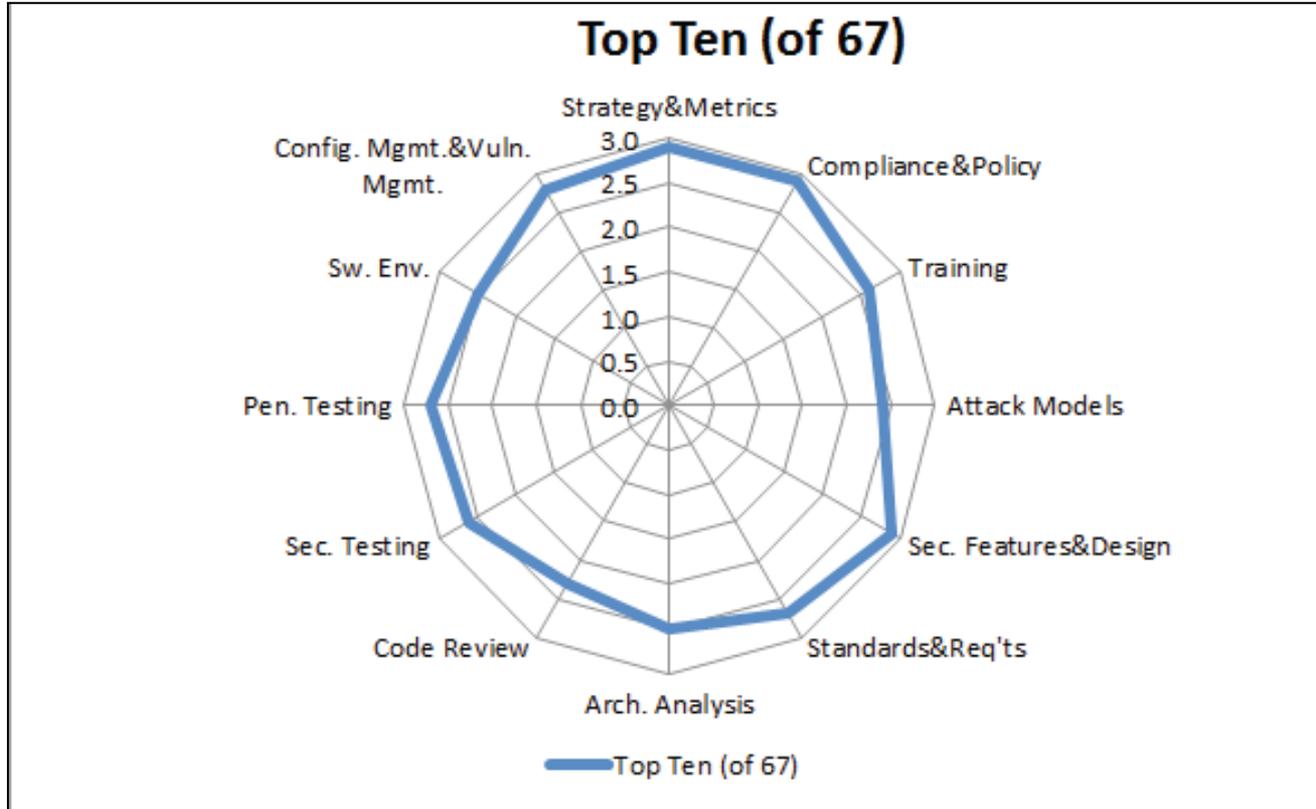
- Developed by Cigital and Fortify
- First release: 2009 (Latest release: 2013)
- A descriptive reference to what works in successful software security organizations  
→ *View a map of where everyone else is now*



# BSIMM-V Results: A map of where everyone else is now



# BSIMM-V Results: Top 10 BSIMM Member Organizations



# Introducing the BSIMM Software Security Framework

The Software Security Framework (SSF)			
Governance	Intelligence	SSDL Touchpoints	Deployment
Strategy and Metrics	Attack Models	Architecture Analysis	Penetration Testing
Compliance and Policy	Security Features and Design	Code Review	Software Environment
Training	Standards and Requirements	Security Testing	Configuration Management and Vulnerability Management



# Introducing the BSIMM Software Security Framework

## Governance

- Strategy and metrics
- Compliance and Policy
- Training

## SSDL Touchpoints

- Architecture Analysis
- Code review
- Security testing



## Intelligence

- Attack Models
- Security Features and Design
- Standards and Requirements

## Deployment

- Penetration Testing
- Software Environment
- Config Mgt and Vuln Mgt

# Introducing the BSIMM Software Security Framework

## Governance

- Strategy and metrics

## SSDL Touchpoints



## Intelligence

## Deployment



# Do you have software security-related goals?

With goals and objectives, you can set a direction and measure success in getting there



# Goals of a Software Security Assurance (SSA) Program



Reduce risk with minimal effort and operational costs



Deliver measurable business and strategic value



Comply with government and industry standards and regulations



Build a security culture throughout your organization

# Introducing the BSIMM Software Security Framework

## Governance

- Strategy and metrics

## SSDL Touchpoints



## Intelligence

## Deployment



# Introducing the BSIMM Software Security Framework

## Governance

- Strategy and metrics
- **Compliance and Policy**

## SSDL Touchpoints



## Intelligence

## Deployment



# Introducing the BSIMM Software Security Framework

## Governance

- Strategy and metrics
- Compliance and Policy
- **Training**

## SSDL Touchpoints



## Intelligence

## Deployment



# Introducing the BSIMM Software Security Framework

## Governance

- Strategy and metrics
- Compliance and Policy
- Training

## SSDL Touchpoints



## Intelligence

- **Attack Models**

## Deployment



# Introducing the BSIMM Software Security Framework

## Governance

- Strategy and metrics
- Compliance and Policy
- Training

## SSDL Touchpoints



## Intelligence

- Attack Models
- **Security Features and Design**

## Deployment



# Introducing the BSIMM Software Security Framework

## Governance

- Strategy and metrics
- Compliance and Policy
- Training

## SSDL Touchpoints



## Intelligence

- Attack Models
- Security Features and Design
- **Standards and Requirements**

## Deployment

# Introducing the BSIMM Software Security Framework

## Governance

- Strategy and metrics
- Compliance and Policy
- Training

## SSDL Touchpoints

- **Architecture Analysis**



## Intelligence

- Attack Models
- Security Features and Design
- Standards and Requirements

## Deployment

# Introducing the BSIMM Software Security Framework

## Governance

- Strategy and metrics
- Compliance and Policy
- Training

## SSDL Touchpoints

- Architecture Analysis
- **Code review**

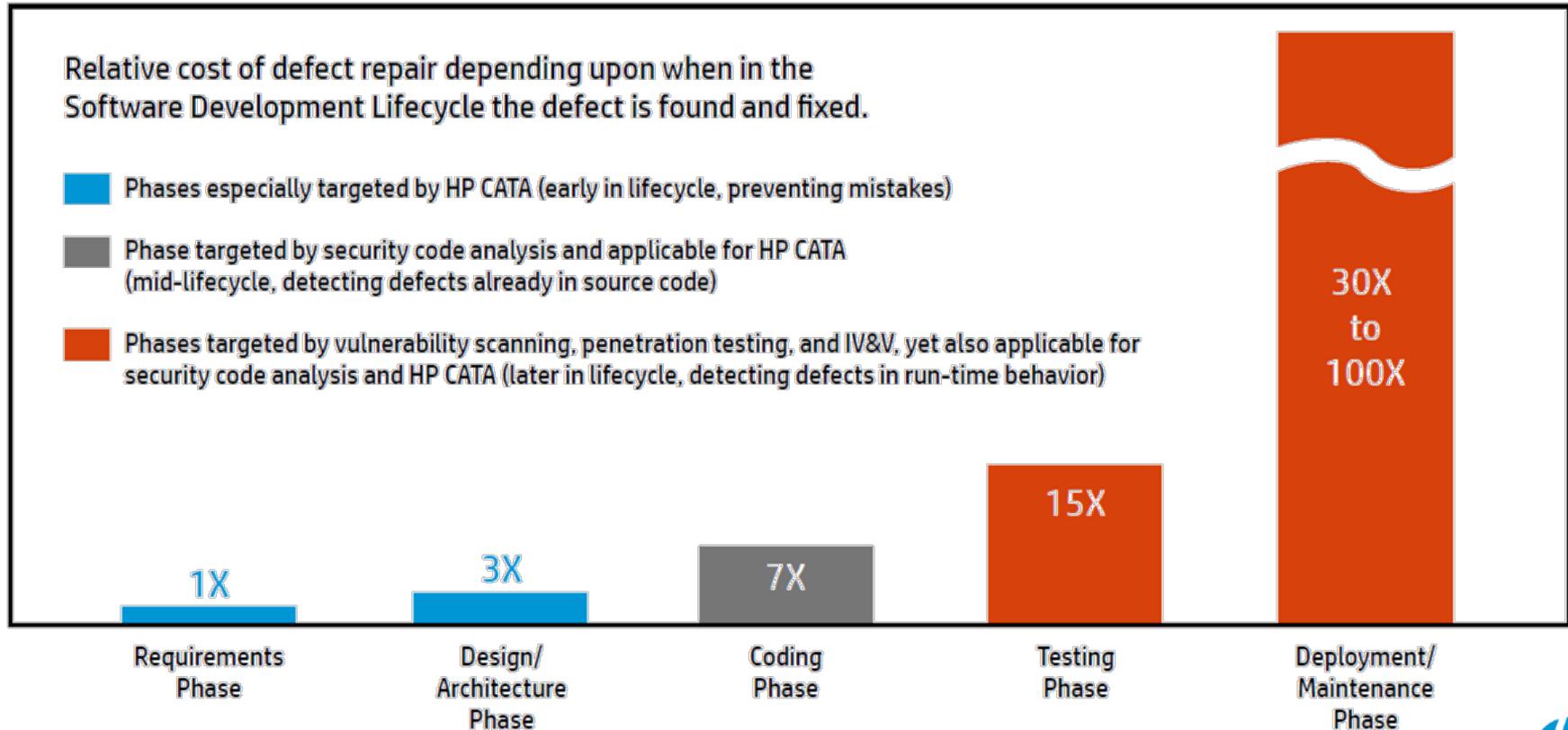


## Intelligence

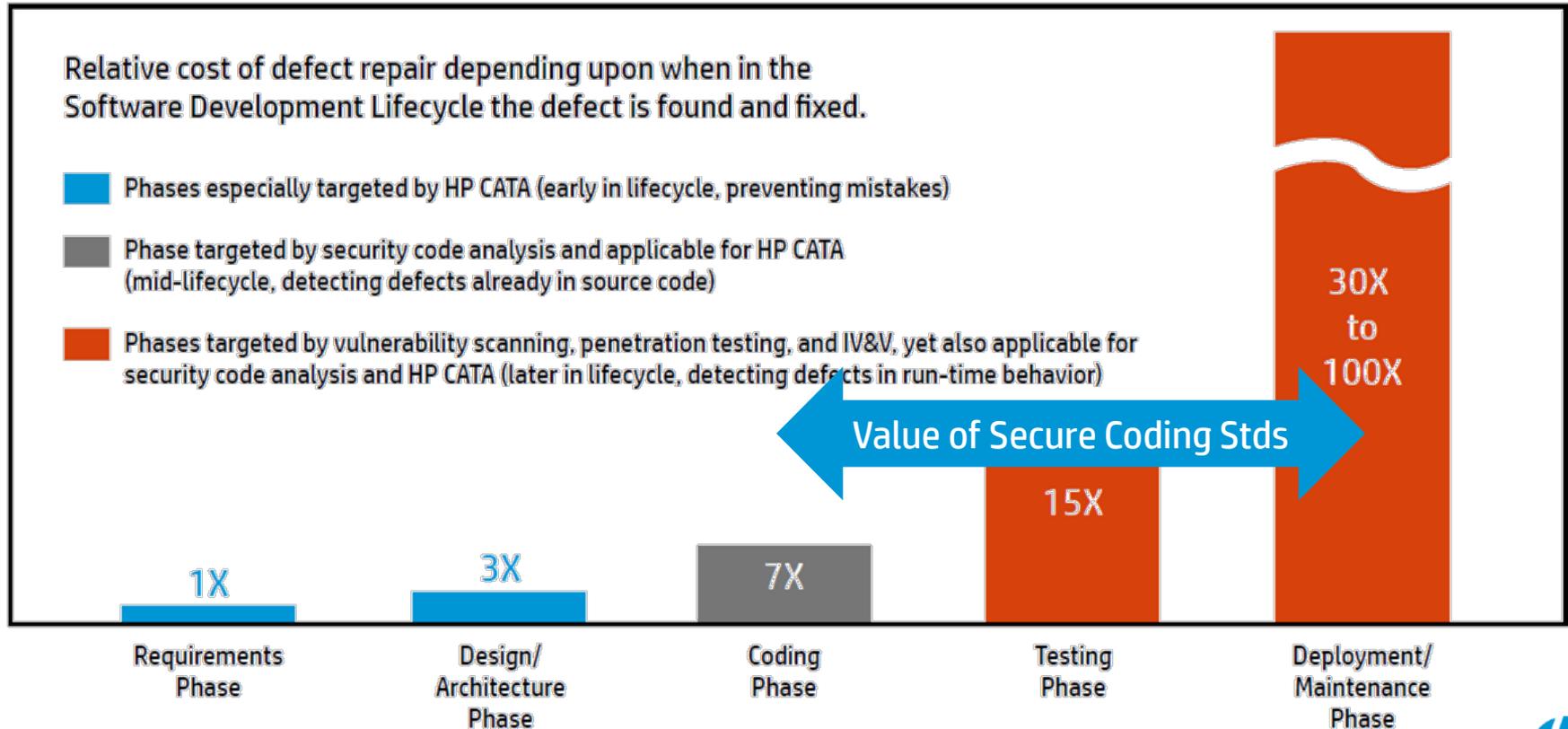
- Attack Models
- Security Features and Design
- Standards and Requirements

## Deployment

# Cost of Defect



# Cost of Defect



# Introducing the BSIMM Software Security Framework

## Governance

- Strategy and metrics
- Compliance and Policy
- Training

## SSDL Touchpoints

- Architecture Analysis
- Code review
- **Security testing**



## Intelligence

- Attack Models
- Security Features and Design
- Standards and Requirements

## Deployment

# Introducing the BSIMM Software Security Framework

## Governance

- Strategy and metrics
- Compliance and Policy
- Training

## SSDL Touchpoints

- Architecture Analysis
- Code review
- Security testing



## Intelligence

- Attack Models
- Security Features and Design
- Standards and Requirements

## Deployment

- **Penetration Testing**

# Introducing the BSIMM Software Security Framework

## Governance

- Strategy and metrics
- Compliance and Policy
- Training

## SSDL Touchpoints

- Architecture Analysis
- Code review
- Security testing



## Intelligence

- Attack Models
- Security Features and Design
- Standards and Requirements

## Deployment

- Penetration Testing
- **Software Environment**

# Introducing the BSIMM Software Security Framework

## Governance

- Strategy and metrics
- Compliance and Policy
- Training

## SSDL Touchpoints

- Architecture Analysis
- Code review
- Security testing



## Intelligence

- Attack Models
- Security Features and Design
- Standards and Requirements

## Deployment

- Penetration Testing
- Software Environment
- **Config Mgt and Vuln Mgt**

# Introducing the BSIMM Software Security Framework

## Governance

- Strategy and metrics
- Compliance and Policy
- Training

## SSDL Touchpoints

- Architecture Analysis
- Code review
- Security testing



## Intelligence

- Attack Models
- Security Features and Design
- Standards and Requirements

## Deployment

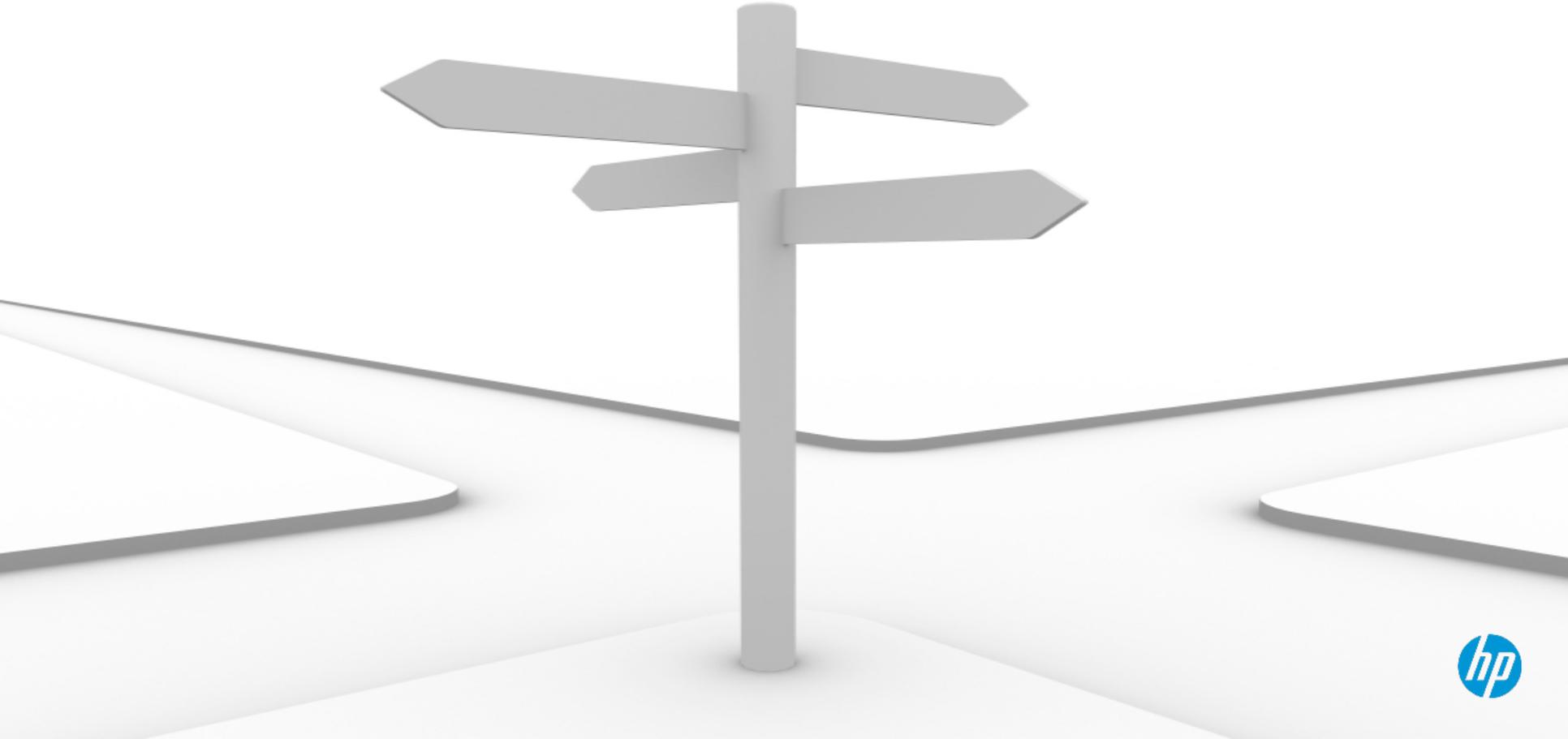
- Penetration Testing
- Software Environment
- Config Mgt and Vuln Mgt

# Why BSIMM?

- **Currently 67 firms participating in the BSIMM (and growing!)**  
For example: Adobe, Aetna, Bank of America, Box, Capital One, Comerica Bank, EMC, Intuit, JPMC, McAfee, Microsoft, Nokia, Salesforce, Symantec, Vmware, Zynga, *et al*
- **Measure your firm to see where you stand**
- **Compare your firm to others in your industry**
- **Systematically, measurably reduce business risk!**



# Where is application security going?



# Application / Information Security Trends

## Some thoughts on 2014

- **Mobile → Look for more malware and applications that misbehave**



# Application / Information Security Trends

## Some thoughts on 2014

- **Mobile** → Look for more malware and applications that misbehave
- **Cloud** → Infrastructure, Software and Security as a Service



# Application / Information Security Trends

## Some thoughts on 2014

- **Mobile** → Look for more malware and applications that misbehave
- **Cloud** → Infrastructure, Software and Security as a Service
- **Security Program Execution** → More outsourcing as SMEs become scarce



# Application / Information Security Trends

## Some thoughts on 2014 and beyond

- **Mobile** → Look for more malware and applications that misbehave
- **Cloud** → Infrastructure, Software and Security as a Service
- **Security Program Execution** → More outsourcing as SMEs become scarce
- **Encryption** → Snowden effect



# Summary

- **The risk is there and we are hearing about it daily**
- **Do *something* to reduce your exposure, but do it thoughtfully; get the people-process piece squared away *before* considering technology**
- **Implementing a security gate provides meaningful results with the least disruption when starting from zero or on constrained budget**
- **Put security flaws and bugs should into the same work stream that developers are used to; *training* your staff is not optional**
- **For legacy systems: Do Nothing, Fix, Enhance or Replace; identify the risk**
- **Measure and report progress against security goals and objectives**



# HP Fortify Solution Overview



# HP Fortify's Software Security Vision

1

## Application Assessment



### Assess

Find security vulnerabilities in any type of software

*Mobile, Web, Infrastructure*

2

## Software Security Assurance (SSA)



In-house



Outsourced



Commercial



Open source

### Assure

Fix security flaws in source code before it ships

*Secure SDLC*

3

## Application Protection



### Protect

Fortify applications against attack in production

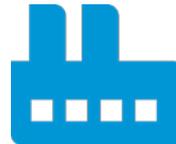
*Logging, Threat Protection*

# HP Fortify Solution from Process Viewpoint

*The HP Fortify solution is flexible enough to be delivered on demand...*



*...or on premise.*



# HP Fortify Solution from Process Viewpoint



**Education & Training**

Instructor-Led  
(On site or Public)

*Two courses, 8 days of training, for  
WebInspect and Fortify products*



# HP Fortify Solution from Process Viewpoint

**Education & Training  
Virtual & on Demand**

*Nearly 50 courses, 100+ hours of eLearning;  
2 courses, 8 days of Virtual Instructor Led Training*

<http://www.hpenterprisesecurity.com/university>

**Design**

**Build**

**Test**

**Deploy**

**Education & Training**



**Instructor-Led  
(On site or Public)**



# Train & Retain

*Our #1 goal is to **train**  
so you can **retain** your talent*



## HP Enterprise Security University Products

### HP Enterprise Security Products - Customer Course Catalogue

HP Enterprise Security Education offers role-based curriculum to ensure that you have the right skills and knowledge to maximize your company's investment in HP Enterprise Security solutions.

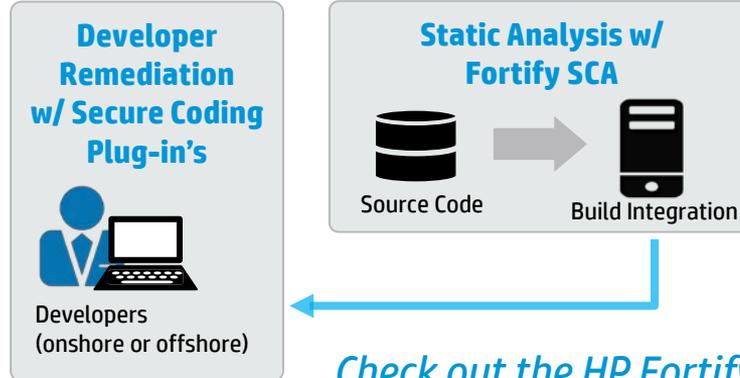
		ArcSight	Fortify	TippingPoint
		COURSE OFFERINGS		
Product Training	WebInspect	Dynamic Application Testing with HP WebInspect		
	Software Security Center	Securing Global IT Applications Using Static Code Analysis		
		Fortify Foundations		
		Developing with Fortify For Application Security (eLearning)		
		Working with Fortify SCA, Audit Work Bench & SSC		
	Architecture	<b>Architect Curriculum</b> (Subscription)		
Application Security Fundamentals				

# HP Fortify Solution from Process Viewpoint



*HP Fortify Static Code Analyzer may be integrated with developer IDEs and/or build systems. Fortify SCA detects:*

- 570+ unique categories of vulnerabilities across
- 21 programming languages and over
- 720,000 individual APIs



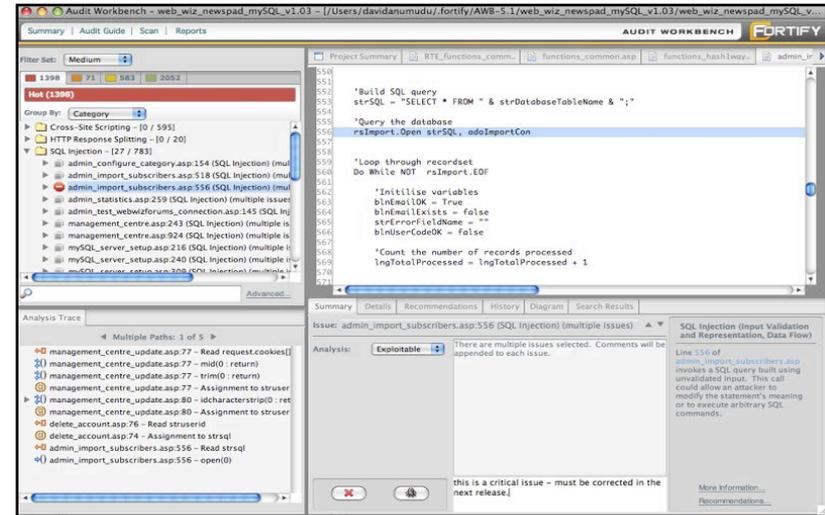
*Check out the HP Fortify taxonomy of security errors at <http://vulncat.fortify.com/>*

# HP Fortify Static Code Analyzer (SCA)

Static analysis – find and fix security issues in your code during development

## Features:

- Automate static application security testing to identify security vulnerabilities in application source code during development
- Pinpoint the root cause of vulnerabilities with line of code details and remediation guidance
- Prioritize all application vulnerabilities by severity and importance
- Supports 21 languages, 500+ vulnerability categories



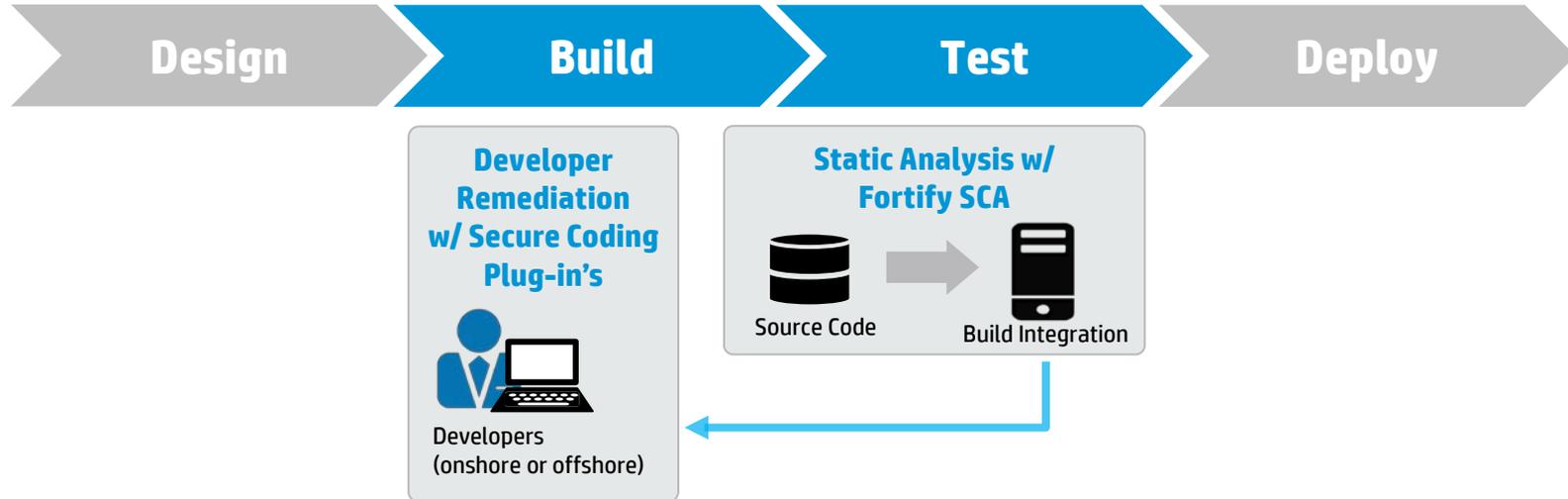
# HP Fortify Solution from Process Viewpoint

*HP Fortify SCA's security defect detection capabilities are available in SaaS format with a typical 24-hour response time.*

**Static Analysis w/  
Fortify on Demand**



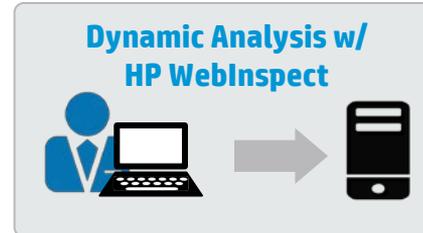
1. Upload code
2. Test code
3. Report & Review results



# HP Fortify Solution from Process Viewpoint



*HP WebInspect is the industry's premiere Dynamic Application Security Testing (DAST) solution. It is often used as a Security Gate to identify risk before applications are moved to production.*

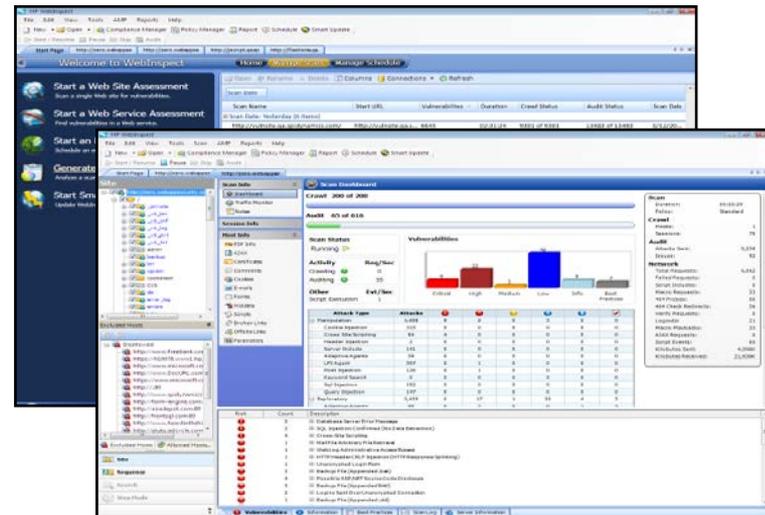


# HP WebInspect

Dynamics analysis – find critical security issues in running applications

## Features:

- Quickly identify risk in existing applications
- Automate dynamic application security testing of any technology, from development through production
- Validate vulnerabilities in running applications, prioritizing the most critical issues for root-cause analysis
- Streamline the process of remediating vulnerabilities



# HP Fortify Solution from Process Viewpoint

*The same great features of HP WebInspect are employed by the FoD Team to dynamically assess customer applications in pre-prod or production environments.*

**Dynamic Analysis w/  
Fortify on Demand**



**Dynamic Analysis w/  
HP WebInspect**



# HP Fortify on Demand at a glance

## Comprehensive and accurate

### Static Testing

HP Fortify  
SCA

### Dynamic Testing

HP  
WebInspect

### Audit & Analysis

Manual

## Powerful remediation

### Analysis & Reports



### Online Collaboration



## Broad support

- ABAP
- C/C++
- Cold Fusion
- Java
- Objective C
- Python
- VB6
- ASP.NET
- Classic ASP
- Flex
- JavaScript/AJAX
- PHP
- T-SQL
- VBScript
- C#
- COBOL
- HTML
- JSP
- PL/SQL
- VB.NET
- XML

## Fast, secure & scalable

### 1 Day Static Turnaround



### Virtual Scan Farm



### Encryption



### Third Party Reviews



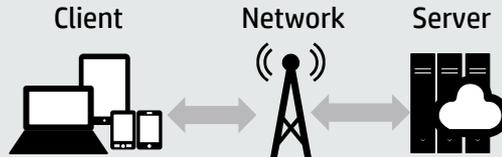
## Mobile Security Testing

### All platforms

- Apple iOS
- Android
- Windows, Blackberry

### Multiple analysis types

- Source Code
- Running Application
- Protocol Analysis



## Breadth of testing

- 10,000+ applications
- 18 different industries represented
- 5 Continents
- Civilian and Defense Agencies across US Government
- Vendor Management and Internal Management
- Development teams from 1 to 10,000s

# HP Fortify Solution from Process Viewpoint



*The HP Fortify Runtime™ platform provides two “flavors” for use in production: Runtime Application Logging (RTAL) and Runtime Application Protection (RTAP).*

*The Runtime platform supports both .NET and Java applications.*

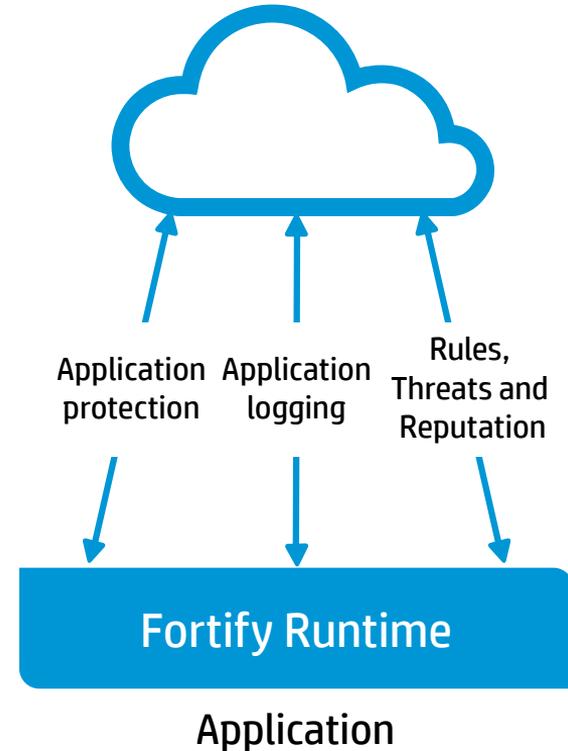
**Analysis, Logging &  
Application Defense w/  
Fortify Runtime  
Application Protection**



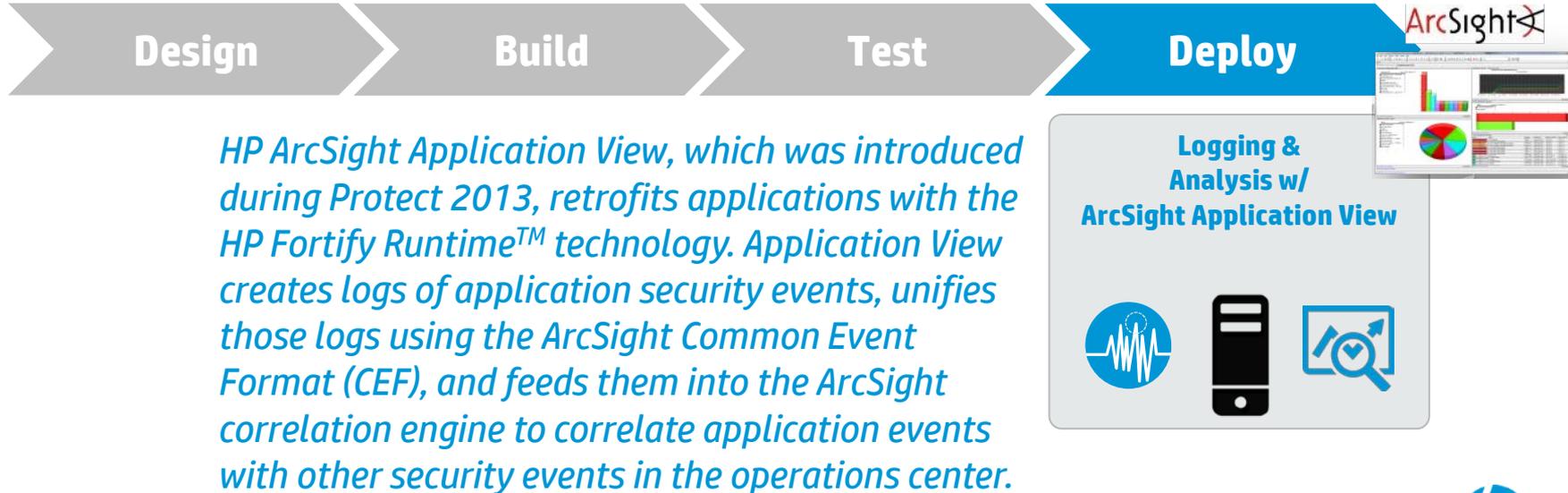
# HP Fortify Runtime Application Protection

## Detect, prevent and log application security threats

- Lightweight runtime analysis agent in production environment
- Instant application-layer security visibility
- Detects security threats and mitigates attacks
- Rules-based attack detection and prevention
- Live threat and reputation intelligence updates
- Active Application Logging – user, fraud, db activity
- Cloud management and reporting



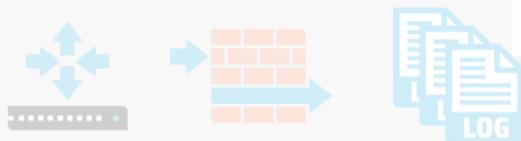
# HP Fortify Solution from Process Viewpoint



## Introducing Application View: Active Application Logging™



OS, databases, storage



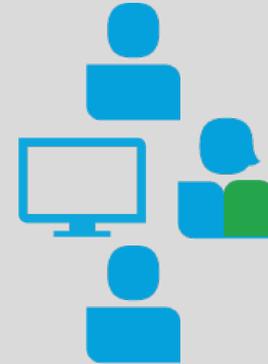
IPS, routers, switches, firewalls, DLP



Servers, IAM, networking



Applications



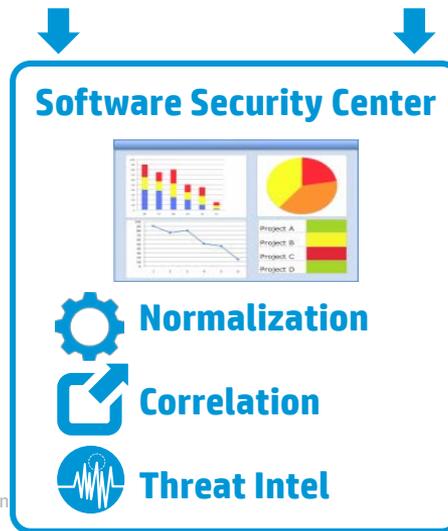
- Retrofits applications with security event logs
- No change to application required
- Out-of-box ready for ArcSight ESM



# HP Fortify Solution from Process Viewpoint



*HP Fortify Software Security Center (SSC) Server is a central security dashboard that allows security and development teams to triage and fix vulnerabilities identified by HP static, dynamic, and runtime analyzers. A collaborative web-based workspace and repository lets teams work together using role-specific interfaces.*



# HP Fortify Software Security Center server

Management, tracking and remediation of enterprise software risk

## Features:

- Specify, communicate and track security activities on software projects
- Role-based, process-driven management of software security program
- Integrations into key development environments
  - Build integration, defect tracking, source control, 3rd party analysis engines
- Flexible repository and reporting platform for security status, trending and compliance
  - Normalized, correlated vulnerability repository
  - Aggregated risk metrics



# Thank you

[hp.com/go/fortify](http://hp.com/go/fortify)

