

RSA[®]Conference2015

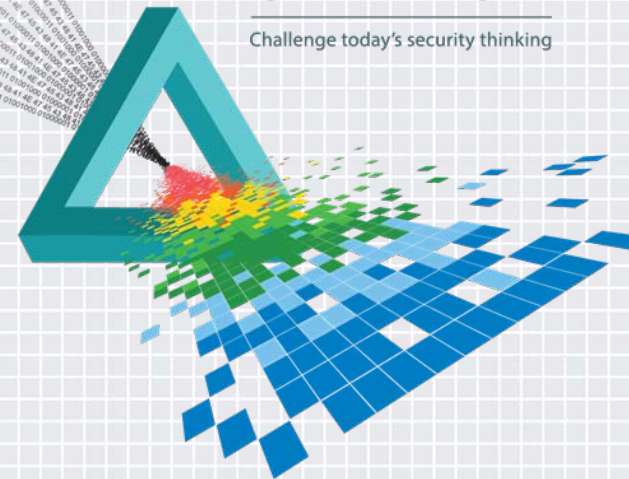
San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: SPO1-W04

Practical Advice for Embracing RASP - A New Kind of Defense



MODERATOR:

Jason Schmitt

VP and General Manager, Fortify
HP Enterprise Security Products
@raidschmitt

PANELISTS:

Tyler Shields

Senior Analyst
Forrester
@txs

Steve Dyer

Chief Technologist, Head of Research
HP Enterprise Security Products
@w1srd

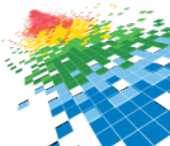
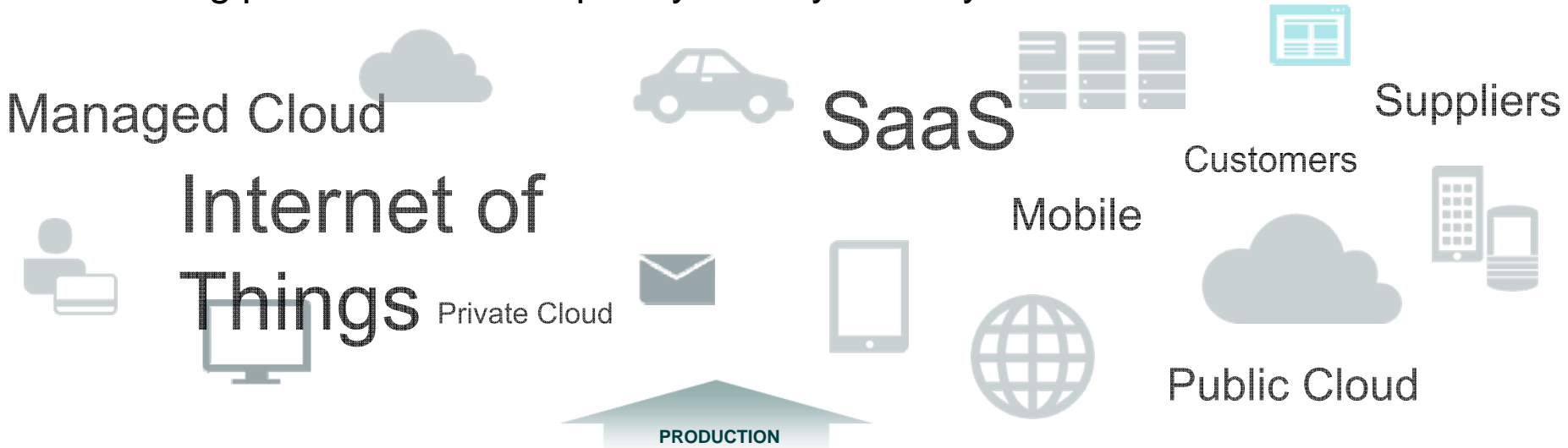
Joe Sechman

Director, Software Security Research
HP Security Research
@Inxkid

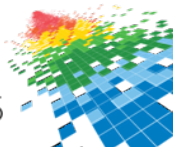
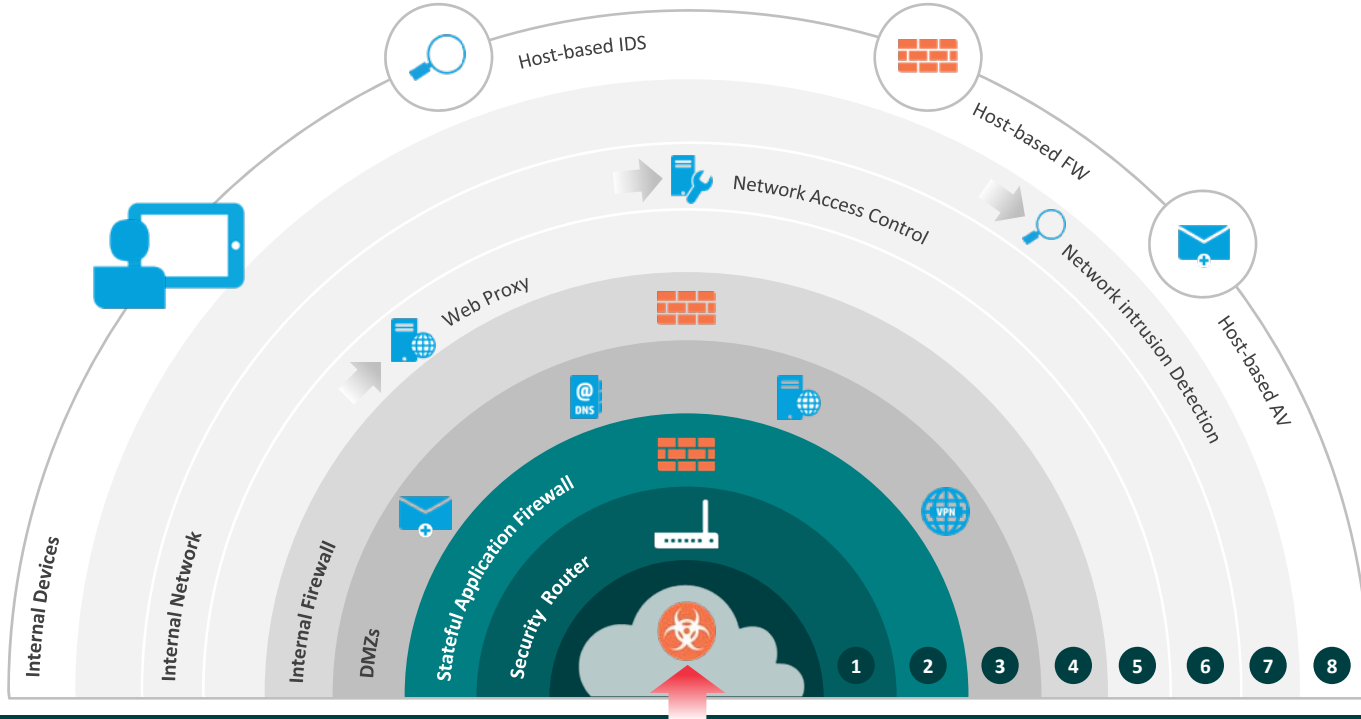


The number of apps is growing

Increasing platforms and complexity...many delivery models



Current solutions protect the perimeter



Application Security Testing

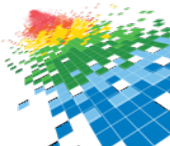
Application Security Testing is a best practice, but remediation before production is difficult to implement = 1-2 weeks to remediation



**Application Security
talent is very difficult
to find**

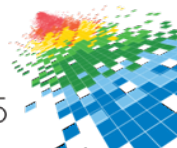
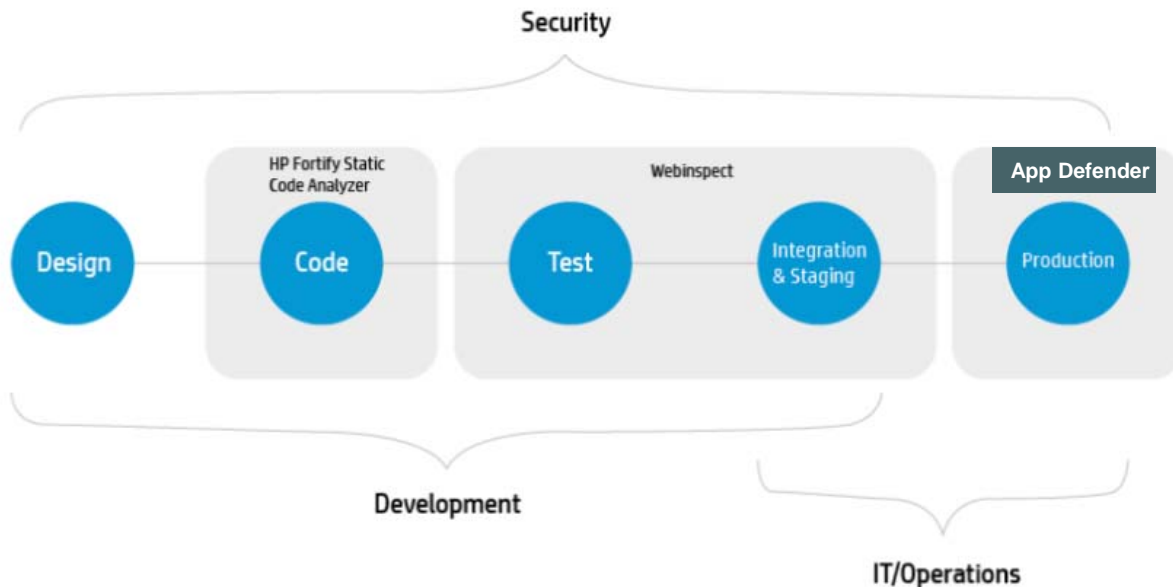
**Process need to be
defined so that
everything is
standardized and
efficient**

**Developers are not
measured to think about
security**



Software Security Assurance

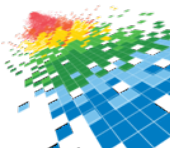
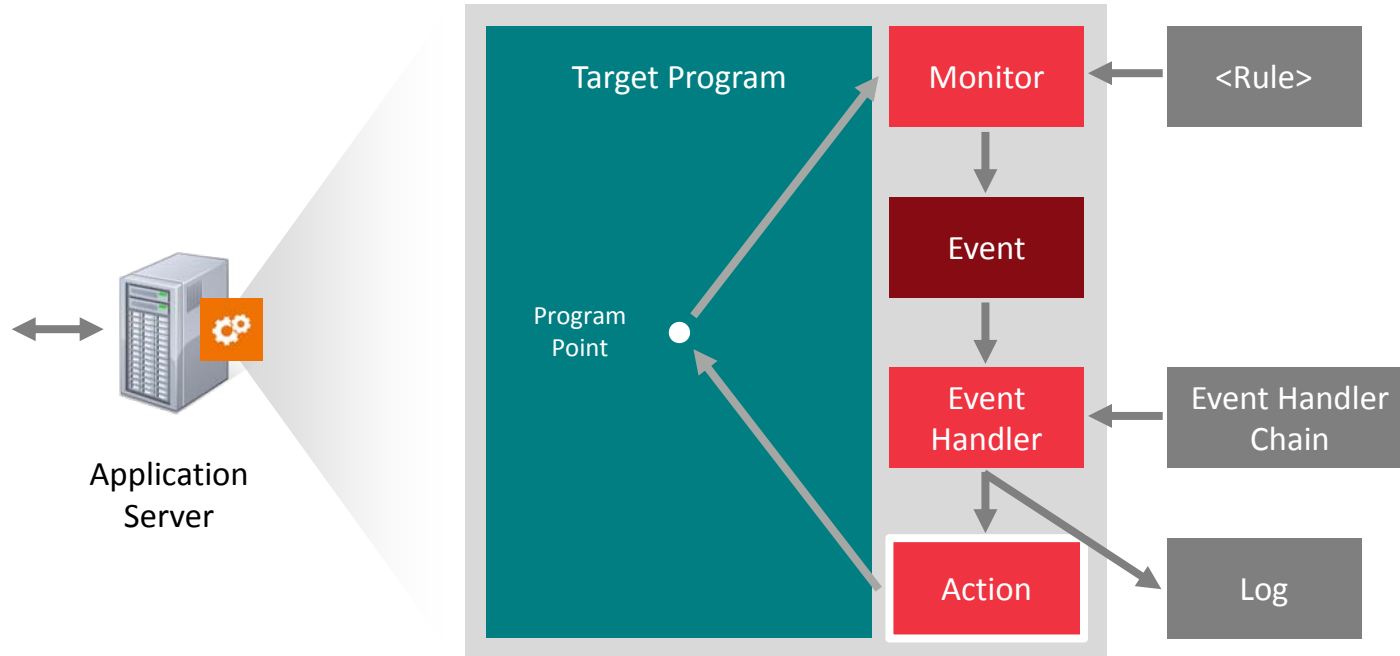
An HP Fortify example of protection across the SDLC



Runtime technology

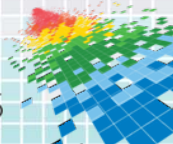
RSA Conference 2015

San Francisco | April 20-24 | Moscone Center



Practical advice for embracing RASP: A new kind of defense

- ◆ Is WAF dead?
- ◆ Which applications are ideal for RASP?
- ◆ Might RASP challenge traditional security roles?
- ◆ Is there a best practice for using RASP?
- ◆ What should I look for when considering RASP technologies?
- ◆ What is the best way to get started?



RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

Learn more at
www.hp-application-defender.com

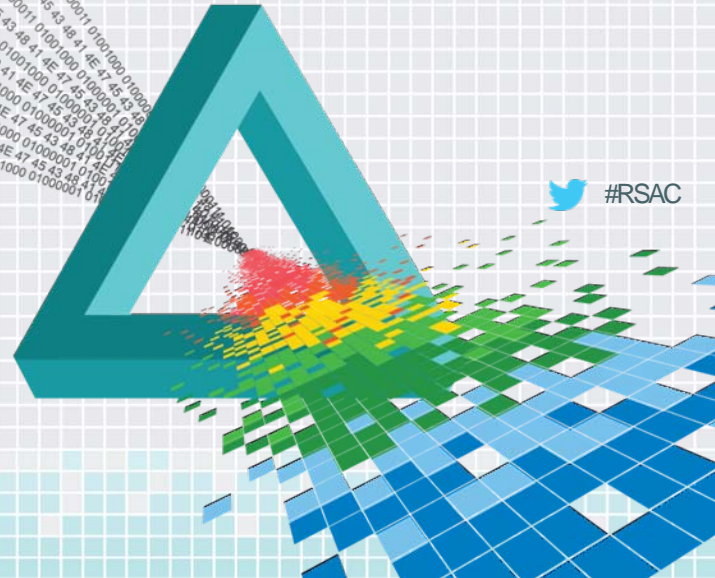


 #RSAC

RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

Thank you



 #RSAC

Back-up slides



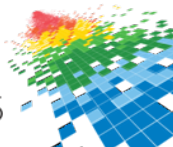
We stop what no one else can even see



HP Application Defender Solution

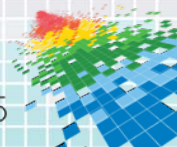
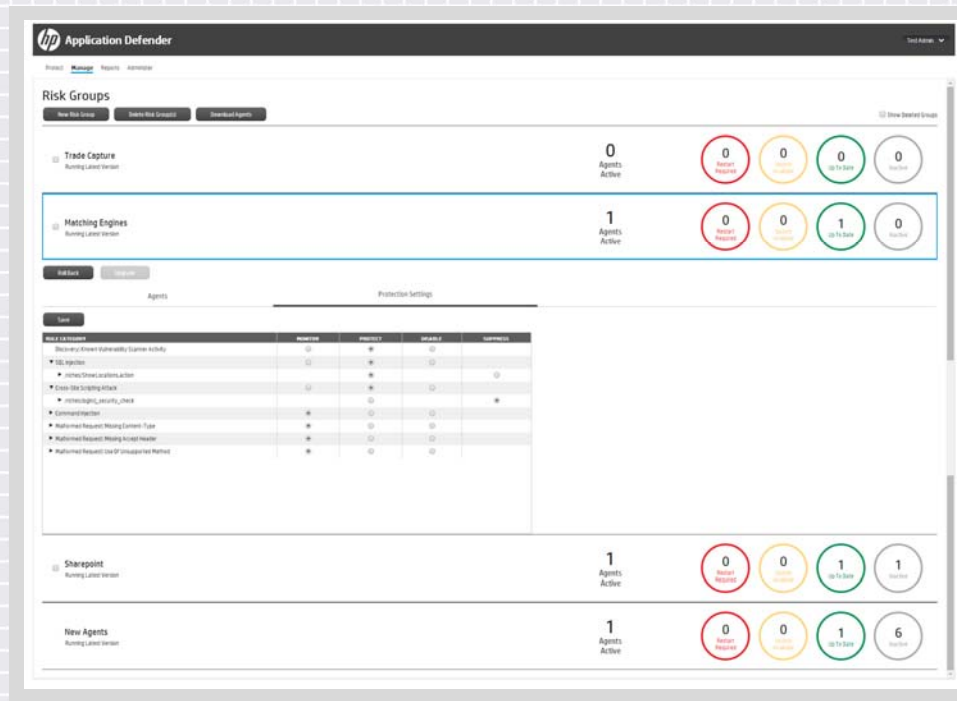


VERTICA Edge Cluster VERTICA VERTICA
 VERTICA VERTICA VERTICA
 VERTICA VERTICA VERTICA VERTICA
 VERTICA VERTICA VERTICA VERTICA



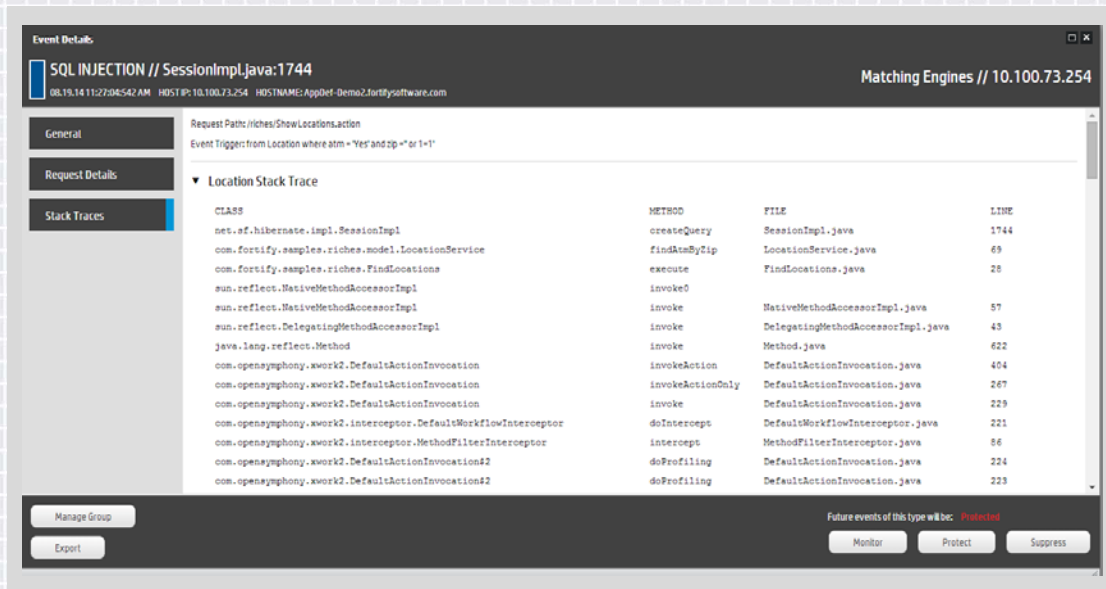
Simplicity

- ◆ **Quick Installation**
 - ◆ Up and running in less than 5 minutes
 - ◆ 3 easy steps
- ◆ **Easy “In Service” Updates**
 - ◆ Rulepack
 - ◆ Agent Binary
- ◆ **Accurate application protection and grouping**



Visibility

- **Quick** access to specific vulnerability events
- **Easy** filtering of real-time and historical data
- **Accurate** presentation of event trigger and stack trace detail



Event Details

SQL INJECTION // SessionImpl.java:1744

08.19.14 11:27:04:542 AM HOST IP: 10.100.73.254 HOSTNAME: AppDef-Demo2.fortifysoftware.com

Matching Engines // 10.100.73.254

General

Request Details

Stack Traces

Request Path: /riches/ShowLocations.action

Event Trigger: from Location where atm = 'Yes' and zip = '1-1'

Location Stack Trace

CLASS	METHOD	FILE	LINE
net.sf.hibernate.impl.SessionImpl	createQuery	SessionImpl.java	1744
com.fortify.samples.riches.model.LocationService	findDataByZip	LocationService.java	69
com.fortify.samples.riches.FindLocations	execute	FindLocations.java	28
sun.reflect.NativeMethodAccessorImpl	invoke0		
sun.reflect.NativeMethodAccessorImpl	invoke	NativeMethodAccessorImpl.java	57
sun.reflect.DelegatingMethodAccessorImpl	invoke	DelegatingMethodAccessorImpl.java	43
java.lang.reflect.Method	invoke	Method.java	622
com.opensymphony.xwork2.DefaultActionInvocation	invokeAction	DefaultActionInvocation.java	404
com.opensymphony.xwork2.DefaultActionInvocation	invokeActionOnly	DefaultActionInvocation.java	267
com.opensymphony.xwork2.DefaultActionInvocation	invoke	DefaultActionInvocation.java	229
com.opensymphony.xwork2.interceptor.DefaultWorkflowInterceptor	doIntercept	DefaultWorkflowInterceptor.java	221
com.opensymphony.xwork2.interceptor.MethodFilterInterceptor	intercept	MethodFilterInterceptor.java	86
com.opensymphony.xwork2.DefaultActionInvocation\$2	doProfiling	DefaultActionInvocation.java	224
com.opensymphony.xwork2.DefaultActionInvocation\$2	doProfiling	DefaultActionInvocation.java	223

Manage Group

Export

Future events of this type will be: **Protected**

Monitor Protect Suppress

Protection

- ◆ **Quick** protection against attacks from within your application
- ◆ **Easy** identification of top vulnerability events by criticality
- ◆ **Accurate** results from within application logic and data flows

