

March 1, 2011 | Westin Huntsville | Huntsville, AL



presented by



Accelerating Software Security With HP

Rob Roy
Federal CTO
HP Software

“If we were in a cyberwar today, the **United States** would lose.”



Mike McConnell
Former DNI, NSA.
Head of Booz Allen Hamilton
National Security Business

SECURITY SPENDING CONTINUES TO CLIMB...



\$79 Billion

U.S. IT Security spend, 2007¹

\$7.3 Billion

IT security allocation in
2009 U.S. Federal Budget²

\$288 Billion

Global IT Security spend, 2007³

¹Info-Tech Research Group , November 15, 2006 baseline, 30% growth in 2007

²U.S. Office of Management & Budget, March 11, 2008

³Gartner Symposium/ITxpo, October 10, 2007



...BUT THE BAD NEWS PILES UP EVEN FASTER



sponsored by



Cost of data breach at TJX soars to \$256m

The Boston Globe

Suits, computer fix add t

By Ross Kerber, Globe Staff |

Shoe Company Loses Credit Card Info

A subsidiary of credit card acc

November 8, 2007, 7:22 pm

Hackers Infect Alicia Keys's MySpace Page

By BRAD STONE

Shell, Rolls-Royce reportedly hacked by Chinese spies

MI5 has warned some 300 banks and accounting and legal firms to guard data

Jeremy Kirk Today's Top Stories > or Other Cybercrime and Hack

Comments (4) Recommendations: 108 — Recomm

December 03, 2007 (IDG News Service) — Britain's domestic intelligence

Military to boost cyber-protections

RELATED VIDEO



» All news video

By LOLITA C. BALDOR, Associated
Wed Mar 19, 2:50 AM ET

WASHINGTON - The military is b
and improve relations with other n
fighting two wars, according to a

Monster Investigated by FTC Conceals Data Security

The Federal Trade Commission has launched

Data Leak in Britain

By ERIC PFANNER
Published: November 22, 2007

LONDON, Nov. 21 — The British g

Four Million Credit, Debit Cards Exposed in Data Breach

Tuesday, March 18, 2008

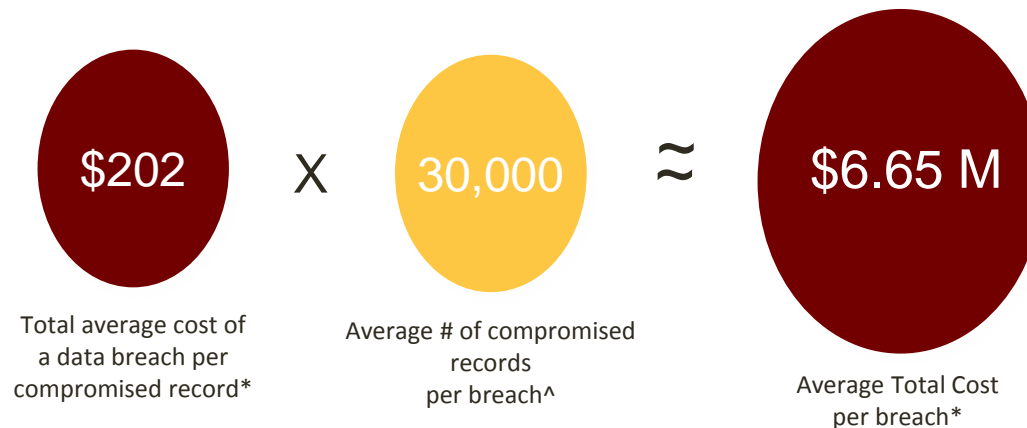
Associated Press

PORTLAND, Maine — A security breach at an East Coast supermarket chain exposed more than 4 million card numbers and led to 1,800 cases of fraud, the Hannaford Bros. grocery chain announced Monday.



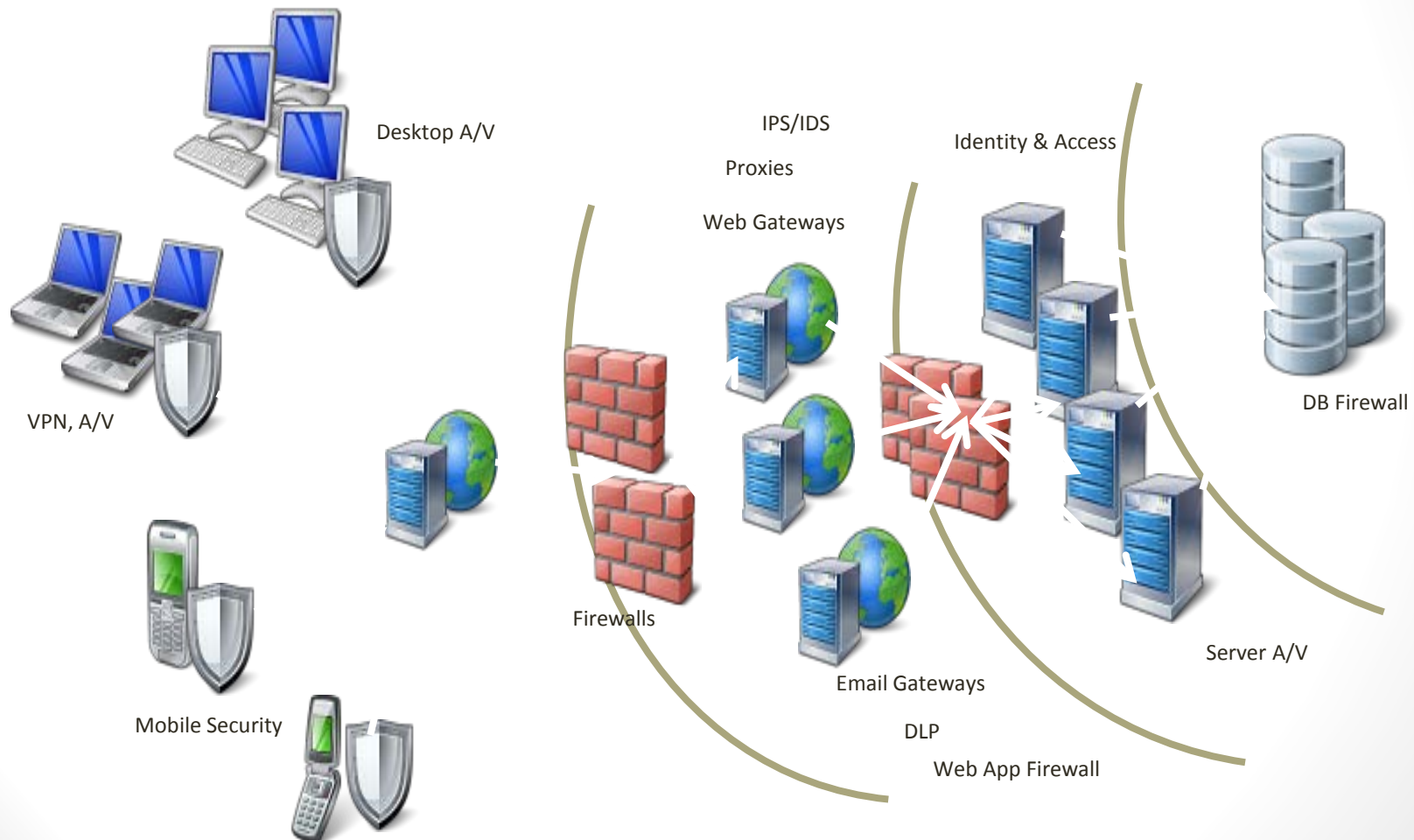
Applications are the focus...

- The number and costs of breaches continue to rise
- 80% of successful attacks target the application layer (Gartner)
- 86% of applications are in trouble
 - Web App Security Consortium studied security tests across 12,186 applications
 - 13% of applications could be compromised completely automatically
 - 86% had vulnerabilities of medium or higher severity found by completely automated scanning



...Yet WE HAVE A false sense of security

- Walls don't work. They protect the network, not the assets



Cybercrime case study



3rd largest US payment processor

The Incident

- Breach reported Jan 2009
- 94M credit records stolen
- Fines levied to banks > \$6M
- Total cost of damages / loss > \$140M

The Attack

- Personnel application attacked by SQL Injection
- Attackers inject code into data processing network
- Credit card transactions stolen



The Conclusion



- Time to Reprioritize
 - 80% of Attacks are at the Software layer
 - 0.6% of IT Security Spend is on Software Security

The Spend must be re-allocated to favor Software Security

- Software Security is a Cross Functional Problem
 - Security Must Provide Assurance
 - Vulnerabilities Must be Addressed in Development
 - Operations involved with Deployment Solutions

Today, Software is Everywhere

Users demand their applications anywhere, anytime



On Premise: desktops and servers

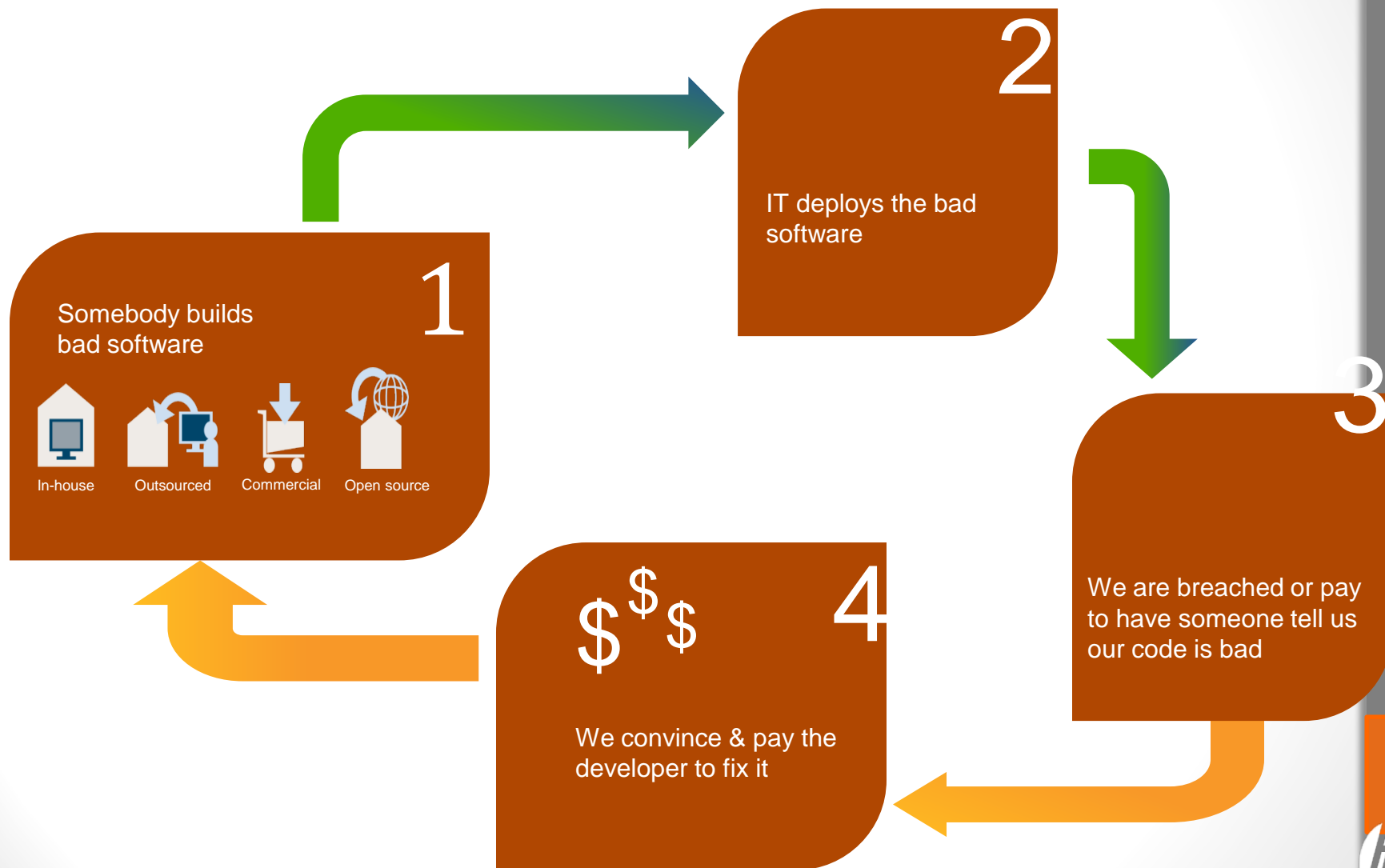


On Demand: cloud and hosted

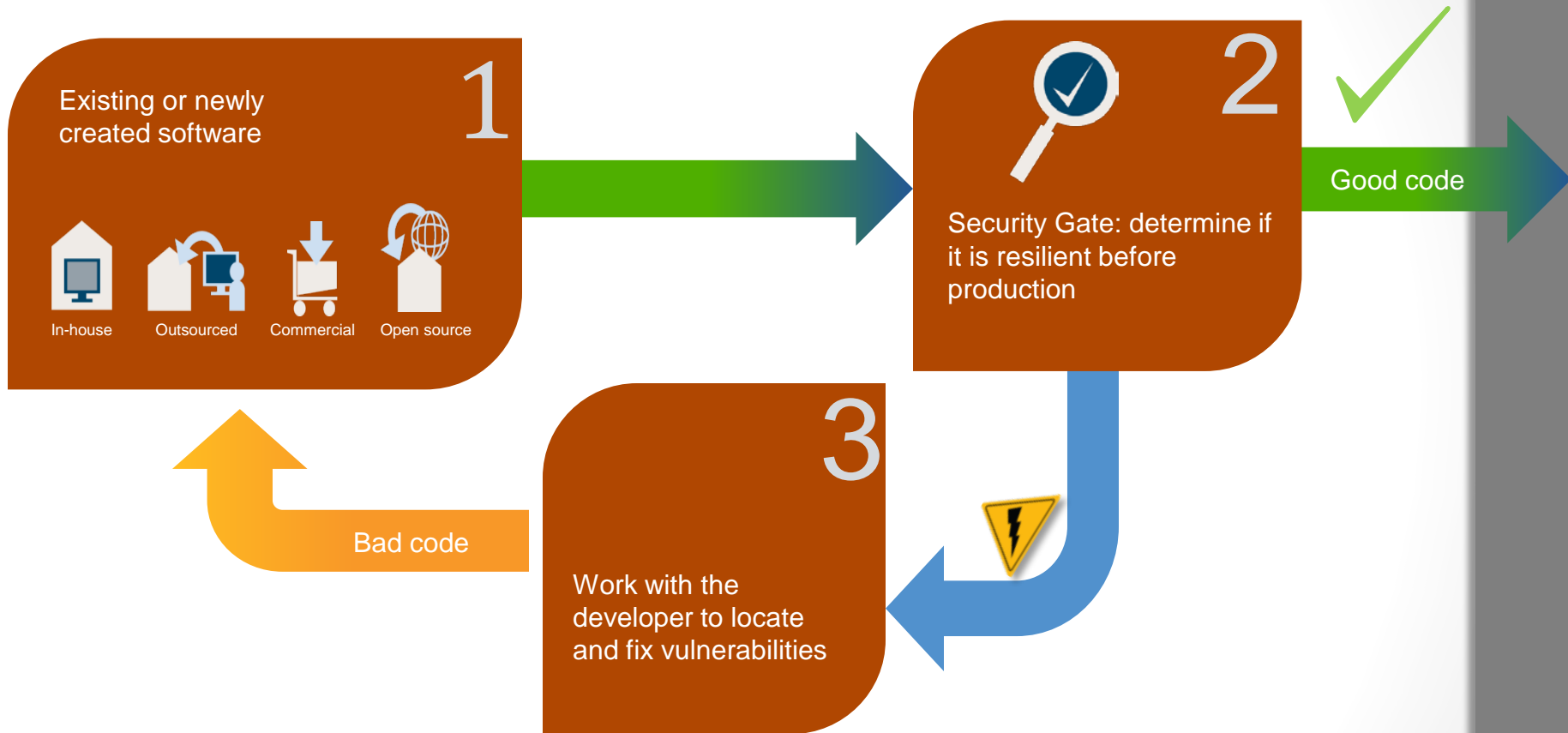


On The Go: laptops and mobile devices

Today's Approach > Expensive, Reactive



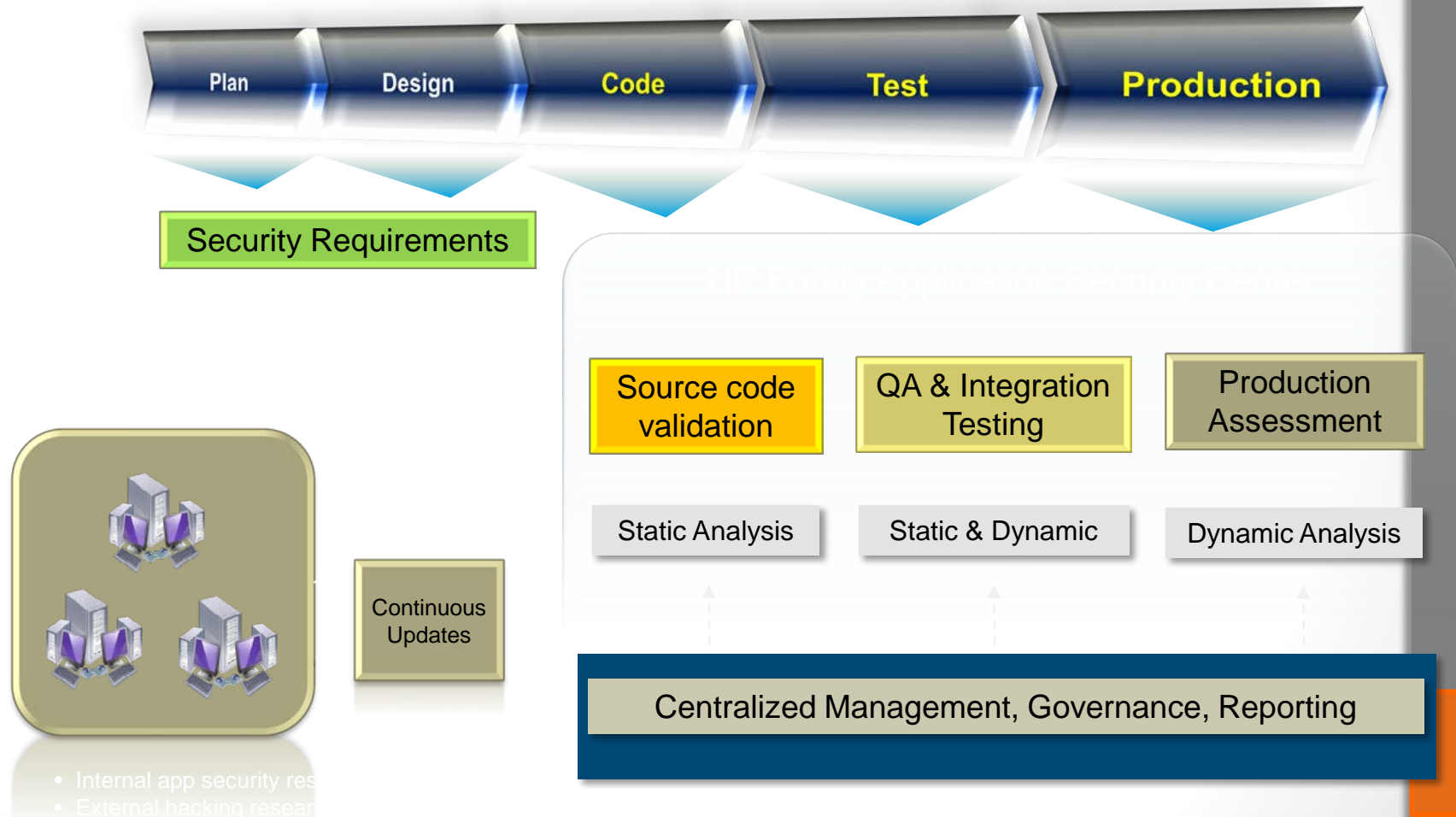
A Safer, More Cost Effective Approach



This is Software Security Assurance

Security in the lifecycle

- Making security a part of everything that you do

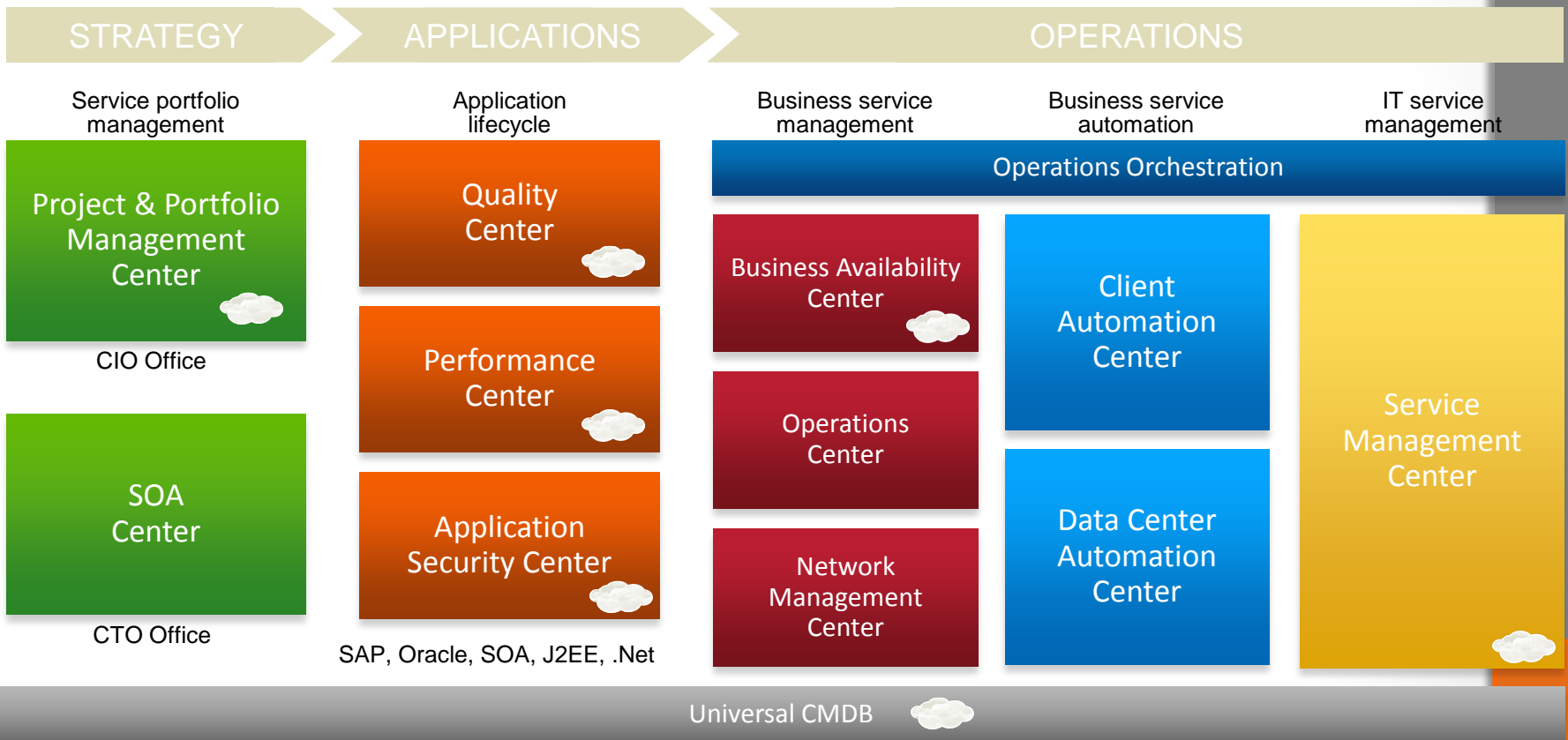


HP Software BTO portfolio

Industry's most comprehensive IT management portfolio



Business outcomes



Software-as-a-Service



presented by



Managing Application Security Risk

Through powerful automation and flexible management tools

Proactive Management

HP Fortify 360 Server

| **HP Assessment Management Platform** |

HP Fortify Governance module

Collaborative Remediation

IDE Plugins

| HP Fortify Collaboration module |

HP Fortify Audit Workbench

Security Testing

HP Fortify SCA | HP Fortify PTA | **HP WebInspect** | **HP QAInspect**

Monitoring and Defense

HP Fortify RTA

Threat Intelligence

HP Fortify Secure Coding Rulepacks

| **HP SecureBase**

Pillars for Success



Requirements for transformative changes throughout the organization

A light teal rounded square representing the 'Software' pillar.

Software

A dark blue rounded square representing the 'Services' pillar.

Services

Fortify Services



Industry-tested methodology to help you meet your SSA goals

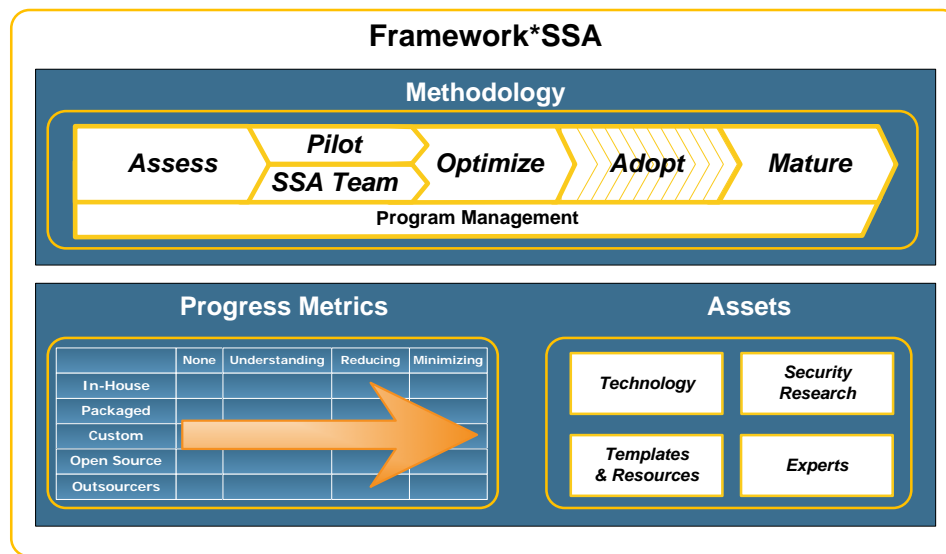
Services

Assessments

Software Security Strategy and Planning

SSA Pilot and Implementation

SSA Center of Excellence



HP Fortify on Demand

Hosted security testing solution for all software

The fastest, easiest way to quickly assess software risk

Protect your investment - integrates with Fortify360 as your software security program expands

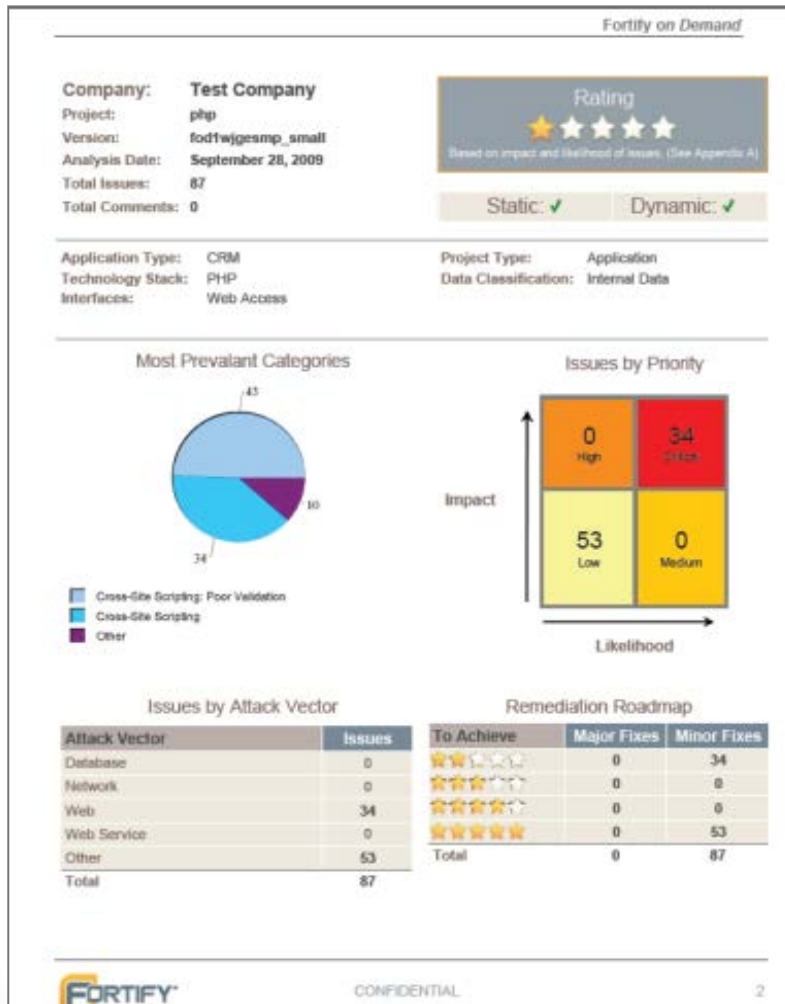
Greatly reduces time to meet compliance with government and industry regulations

Features

Fast, accurate results without hardware or software set up

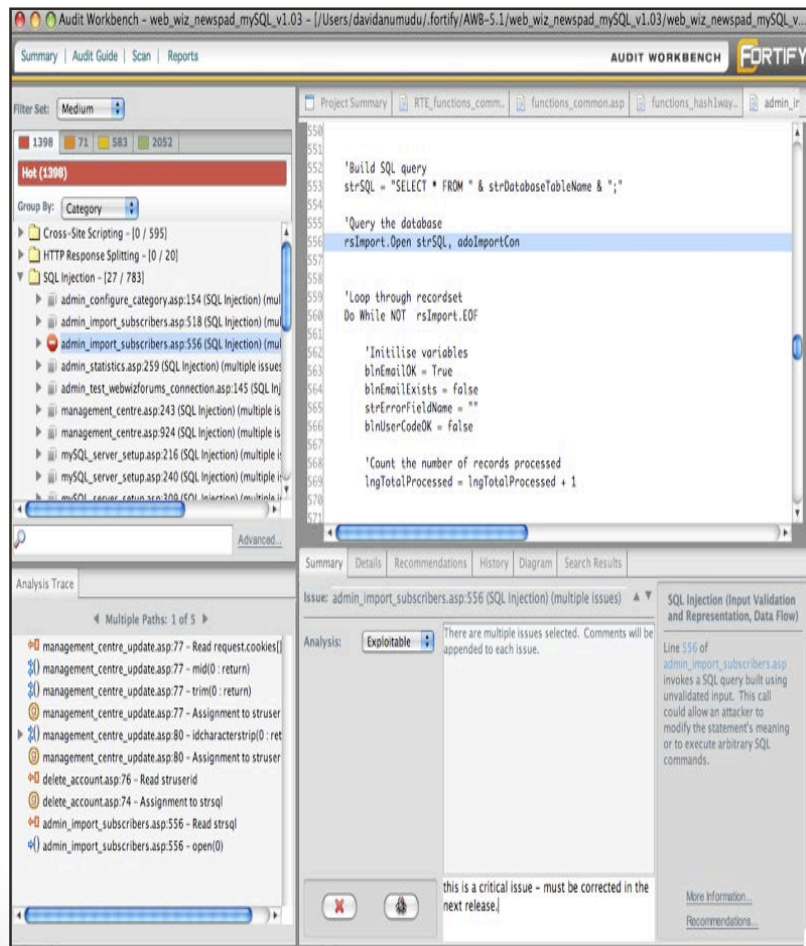
Prioritized, correlated static and dynamic results with remediation guidance

Can be used standalone or with F360



HP Fortify SCA

Security Analysis for Development



Saves valuable development time and costs by pinpointing vulnerabilities during development

Developers spend more time on innovation rather than patches after code is deployed

Increases organization efficiency and improve communication


Features


- Pinpoint root cause of vulnerabilities – line of code detail
- Prioritize fixes sorted by risk severity
- Detailed “fix” instruction -- in the development language


HP Fortify PTA

Security Analysis for Quality Assurance

RESULTS OVERVIEW	FPR GENERATION	CONFIGURATION	ERRORS
The information below is live runtime data calculated only for this instance of the application server			
Number of Issues Found: 3			
Security Code Coverage: 109 hits of 1502 total (92% not covered).			
Category	Total Found		
SQL Injection	1		
Log Forging	1		
Cross-Site Scripting	1		

SQL Injection				
Source	Sink	URL	Verified	Verification Steps
org.apache.struts.util.RequestUtils:1246 -> String[] javax.servlet.http.HttpServletRequest.getParameterValues(String)	com.order.spic.ItemService:201 -> ResultSet java.sql.Statement.executeQuery(String)	http://localhost:8380/spic/listMyItems.do		view

Log Forging				
Source	Sink	URL	Verified	Verification Steps
org.apache.struts.util.RequestUtils:1246 -> String[] javax.servlet.http.HttpServletRequest.getParameterValues(String)	org.apache.commons.beanutils.BeanUtils:873 -> void org.apache.commons.logging.Log.trace(Object)	http://localhost:8380/spic/listMyItems.do		view

Cross-Site Scripting				
Source	Sink	URL	Verified	Verification Steps
com.order.spic.ItemService:205 -> String java.sql.ResultSet.getString(int)	org.apache.jsp.pages.content.myListItems_jsp:127 -> void javax.servlet.jsp.JspWriter.print(String)	http://localhost:8380/spic/listMyItems.do		view

Find more security issues faster during current QA processes

Simplifies remediation and associated costs with IDE integration

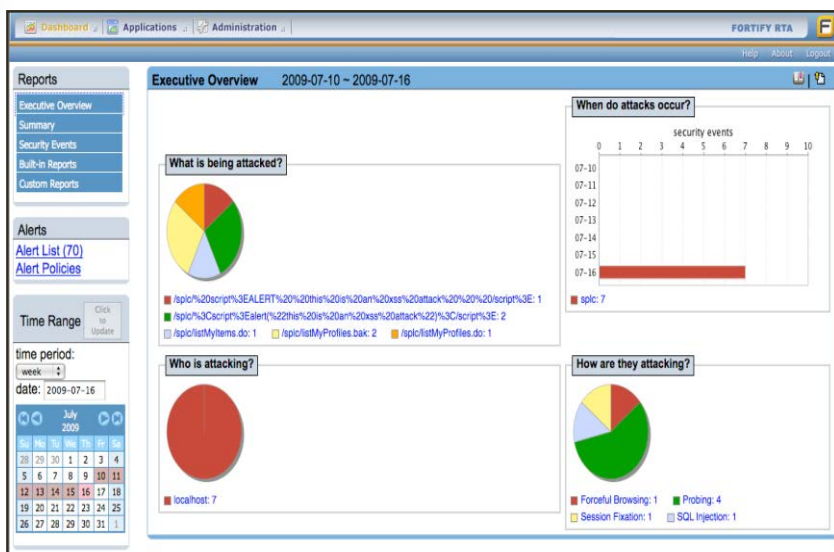
Lowers risk with correlated results from static and dynamic analysis

Features

- Works within existing QA test suite -- no disruption to current processes
- Provides precise results -- exact line of code
- Easy deployment -- no customization or expertise required

HP Fortify RTA

Security Analysis for Production Software



Blocks attacks to minimize security risks in deployed applications

Provides an immediate solution to help meet PCI, DIACAP, OWASP and HIPAA compliance

Protects while providing vulnerabilities root cause in a real-world context.

Features

- Accurate responses to attacks – automatically – and without tuning
- Extensive rules for common vulnerabilities
- Simple and easy set up -- no training, modeling or coding required

HP Fortify Governance

Security Management for Policy and Compliance

Summary

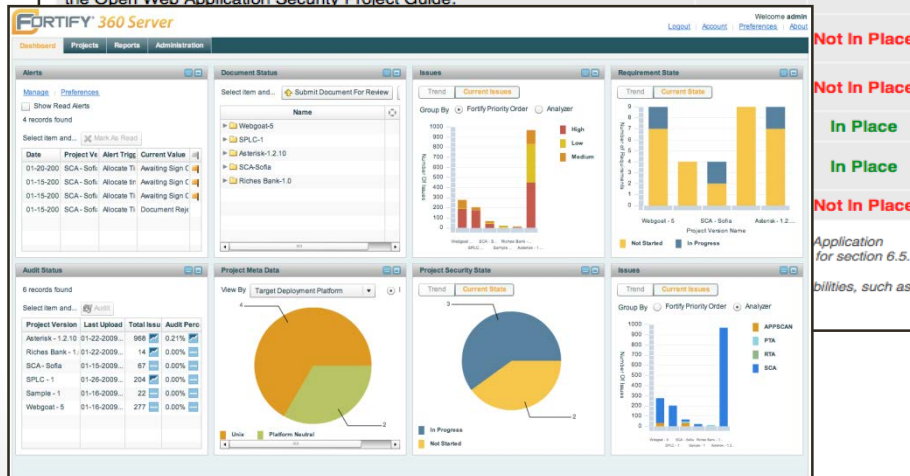
The following is a summary of the application security portions of PCI DSS v1.2. Fortify 360 tests for 10 application security specific requirements across sections 3,4,6,8 and 10, and reports whether each requirement is "In Place" or "Not In Place". Fortify assigns a "Fail" rating for the application if one or more requirements are "Not In Place".

Project Version: 1.0
Last Analysis Date: Mar 6, 2009 11:24 AM
Methodology: SCA
Lines of Code: 4,524
Number of Files: 98

PCI Compliance: Application Security Requirements

Fail

PCI Requirement	Findings	Status
3.2: Do not store sensitive authentication data after authorization.	1	Not In Place
3.4: Render PAN, at minimum, unreadable anywhere it is stored.	2	Not In Place
3.6: Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data.	0	In Place
4.2: Never send unencrypted PANs by end-user messaging technologies.	1	Not In Place
*6.5: Develop all web applications based on secure coding guidelines such as the Open Web Application Security Project Guide.	39	Not In Place



Reduces the costs of managing security programs

Optimizes the investment in SDLC program by automatically generating requirements based on software profile risk

Keeps developers focused on innovation and time to market vs. "managing" security

Features

- Web-based SSA dashboard with project and program level visibility
- Centralized risk profile manager maintains complete application inventory
- Automated assignment of the correct risk-mitigation activities based on risk profiles



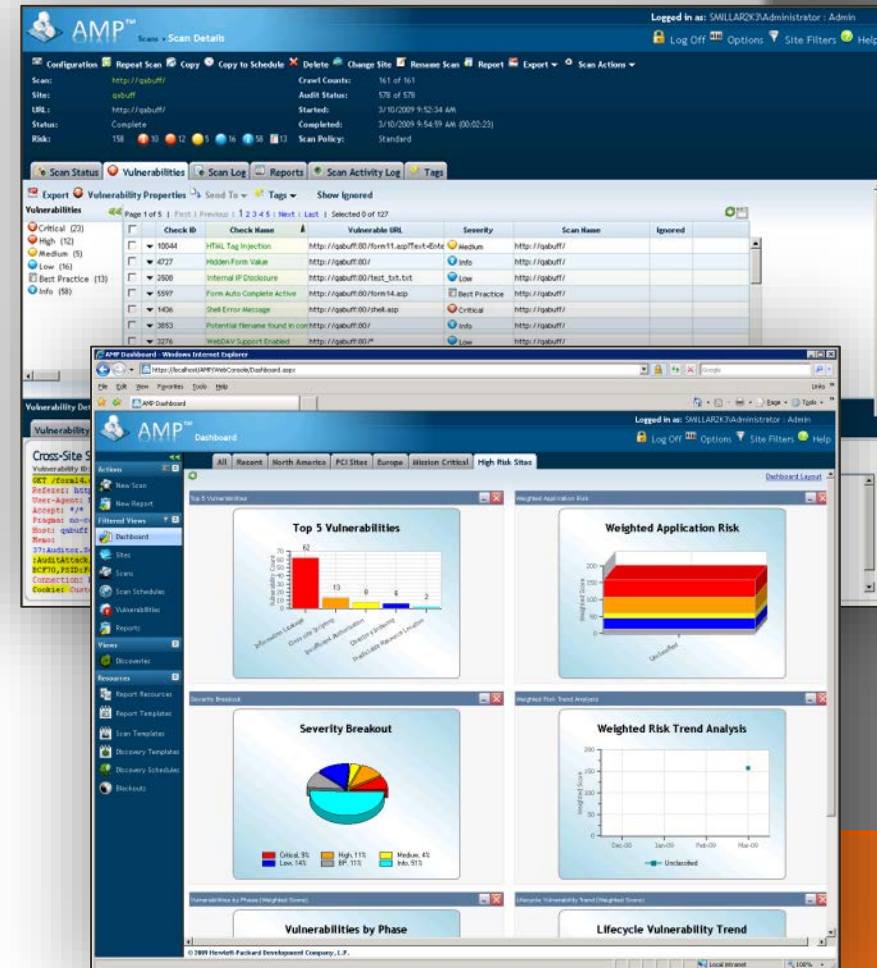
presented by



HP Assessment Management Platform

Control application security risk across the enterprise

- Scale application security
 - Manage application security programs
 - Enable Security Center of Excellence
- Extend security across the application lifecycle
 - Share knowledge and best practices
- Increase visibility and control
 - Quantify application security risk
 - Add asset, data and business context to security
- Trend reporting and analysis
- Govern compliance/policies across the enterprise
- Available as SaaS





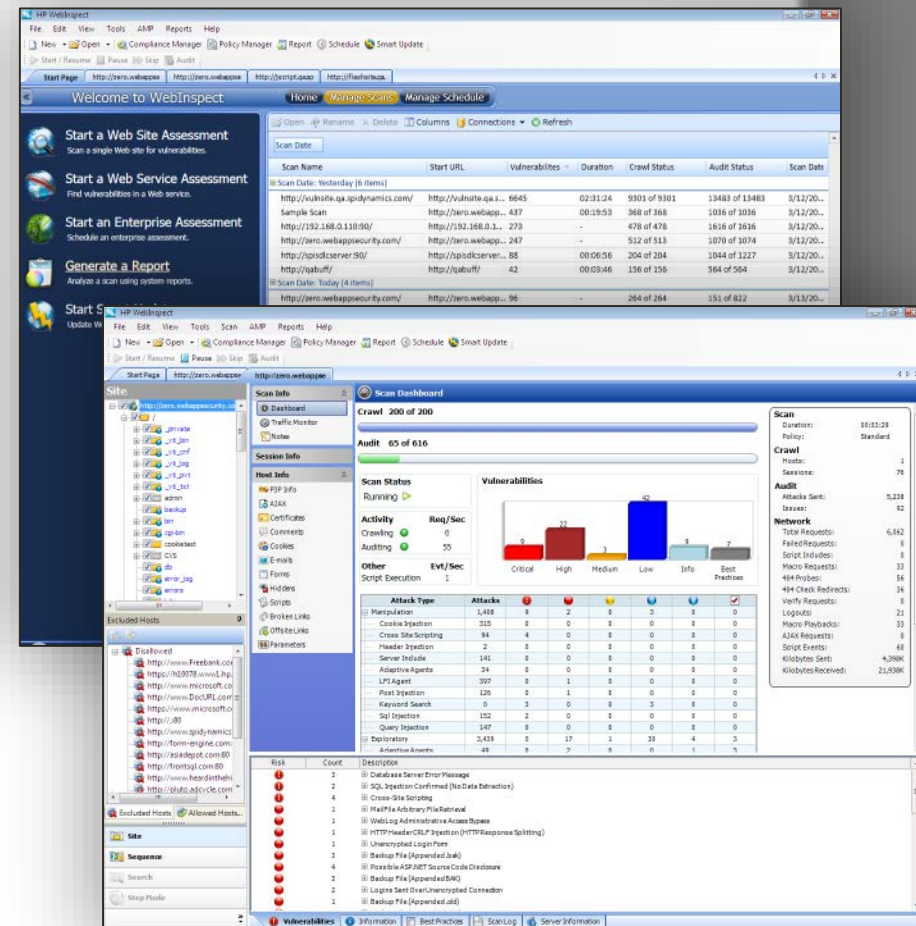
presented by



HP WebInspect

Accelerate security through more actionable information

- Accelerate vulnerability detection
 - Test more applications in less time
- Provide more actionable information
 - Focus on what really matters
- Increase technology coverage
 - Assurance in testing the latest technologies for the latest vulnerabilities
 - JavaScript, Ajax, Flash, Oracle ADF
 - Backed by HP Web Security Research Group
- Facilitate vulnerability remediation
 - Extensive remediation description, steps, code samples & role based content
- Improve security knowledge
 - Security expertise within the solution





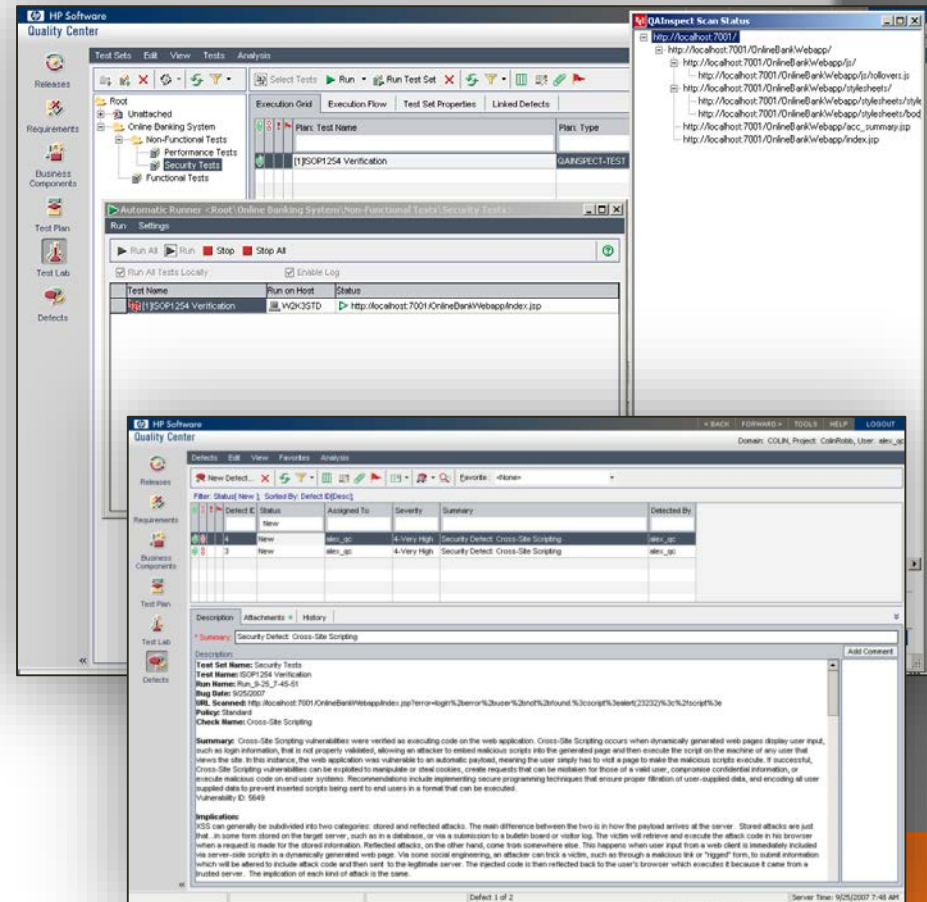
presented by



HP QAInspect

Empower QA teams with embedded security testing

- Bring security process into ALM
 - 'Build it in' rather than 'bolt in on'
- Lower cost of attaining security
 - Earlier vulnerability detection
- Lower application risk
 - Build secure code, find defects early
- Integrate dynamic security testing into test planning, QM environment
 - Familiar environment for QA professionals
- Increase QA team value
 - Security testing without being security experts





presented by

