



IBM Software Group

The New Imperative: Automating Web Application Security

Rational. software

[Go to IBM](#)

Agenda

- Introduction to Application Security
- IBM Application Security Solutions
- Reference



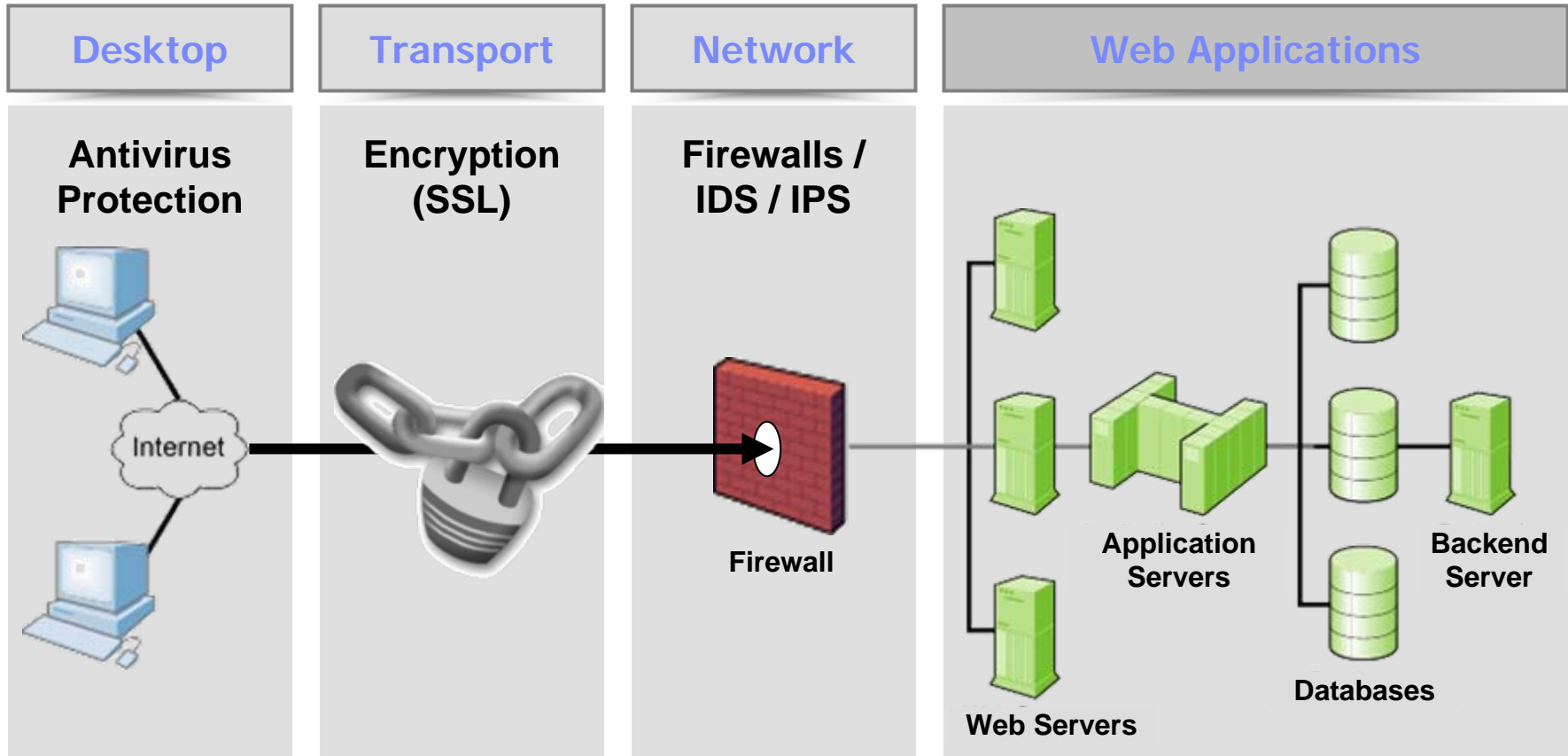
Agenda

- Introduction to Application Security
- IBM Application Security Solutions
- Reference



Application Security - Understanding the Problem

Info Security Landscape





IBM Software Group

Application Security Hacking Example

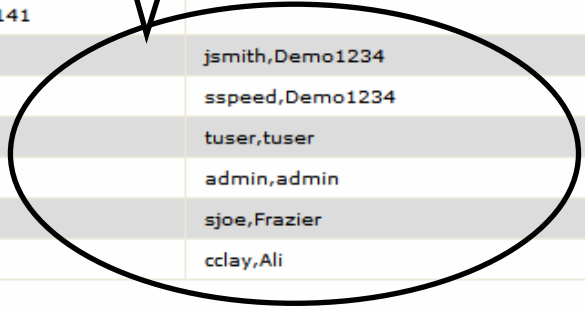
Rational. software

[→ Go to IBM](#)



22	1001160140	Deposit	1050.88
23	1001160140	Car Payment	389.12
24	1001160140	Deposit	1050.88
27	1001160140	Car Payment	389.12
68	1001160141	Deposit	877.8
74			878.9
77			881.1
265			150000
357	1005160101		878.85336
363	1005160101		879.95468
366	1005160101		882.15732
378	1006160141		878.85336
384	1006160141		879.95468
387	1006160141		882.15732
419	1006160141		150180
100116014		jsmith,Demo1234	
100216018		sspeed,Demo1234	
100316012		tuser,tuser	
100416016		admin,admin	
100516010		sjoe,Frazier	
100616014		cclay,Ali	
1			

Application responds with user names and passwords of other account holders!



The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. Watchfire does not assume any risk in relation to your use of this website. For additional Terms of Use, please go to <http://www.watchfire.com/statements/terms.aspx>.

Copyright © 2006, Watchfire Corporation, All rights reserved.

State of the Application Security Threat

Growing Threat

- Past customer spending focused on Network security – yet 75% of attacks come through web applications – market is now focusing on spending on web application security
- Mitre group indicates that application issues (XSS and SQL Injection) are the top 2 hacks
- Most websites are vulnerable (Watchfire/Gartner)

Analyst Views

“Gartner estimates that 90 percent of externally-accessible applications today are web-enabled, and that two-thirds of them have exploitable vulnerabilities.

“64% of developers are not confident in their ability to write secure applications”

Microsoft Developer Research

Cost of Application Security Breach

- **Security Breach**
 - Every lost record costs \$138 to the organization who lost it
 - Media Attention > Brand Damage > Sharp Decline in Stock Prices



PCI Application Security Requirements



Build and Maintain a Secure Network

- Requirement 1: Install and maintain a firewall configuration to protect cardholder data
- Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Requirement 3: Protect stored cardholder data
- Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

- Requirement 5: Use and regularly update anti-virus software
- Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Requirement 7: Restrict access to cardholder data by business need-to-know
- Requirement 8: Assign a unique ID to each person with computer access
- Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

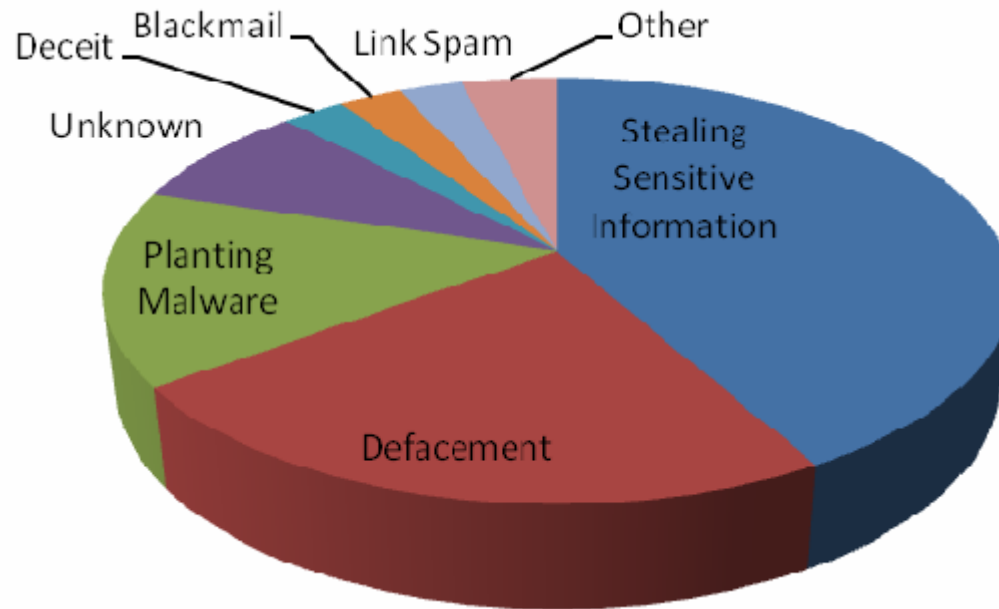
- Requirement 10: Track and monitor all access to network resources and cardholder data
- Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

- Requirement 12: Maintain a policy that addresses information security



Motives Behind Application Hacking Incidents



Source: WASC 2007 Web Hacking Incident Annual Report



Where Do These Problems Exist?

Type:

- Customer facing services
- Partner portals
- Employee intranets

Source:

1. Applications you buy – e.g. COTS
2. Applications you build internally
3. Applications you outsource

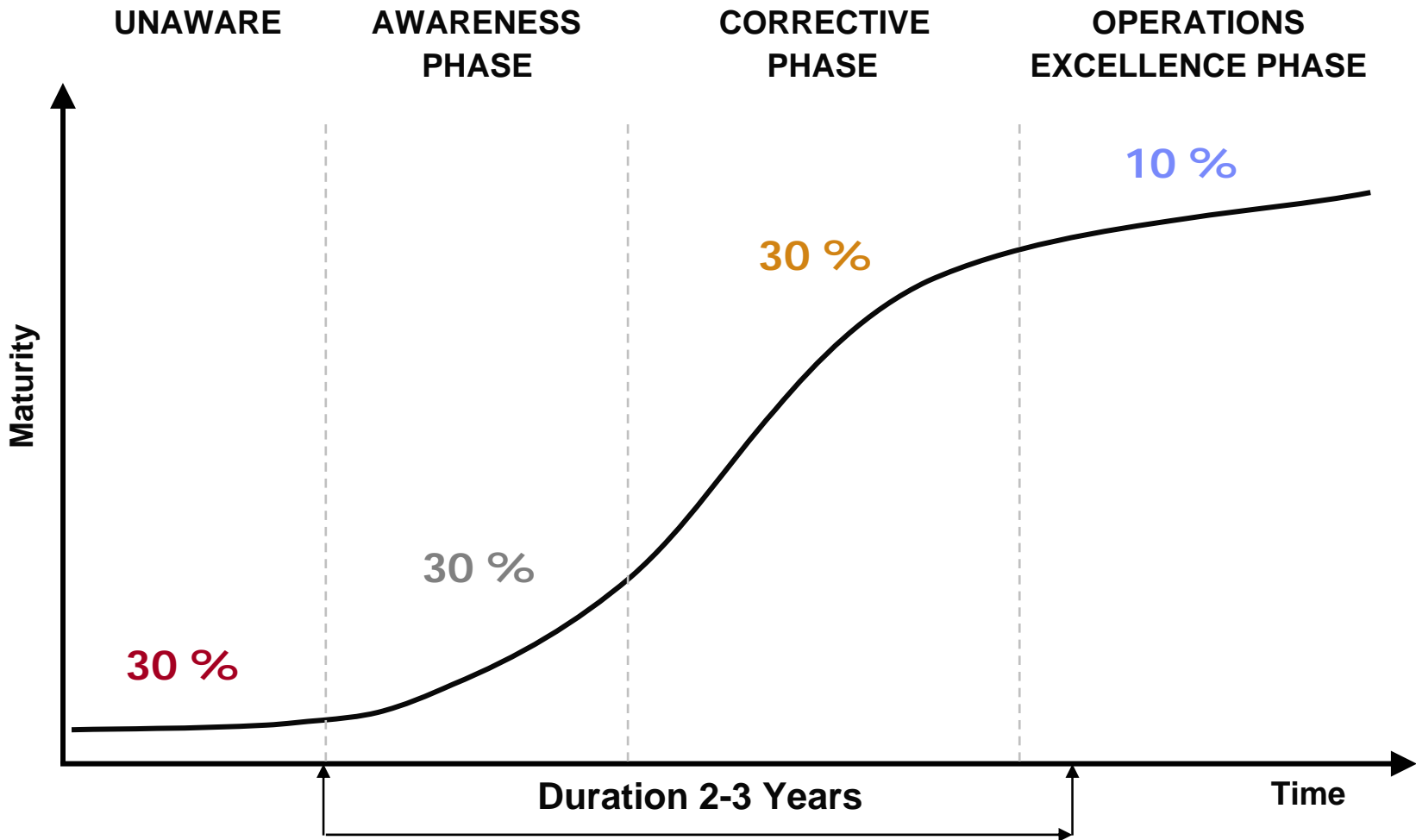


What's the Root Cause of this Problem?

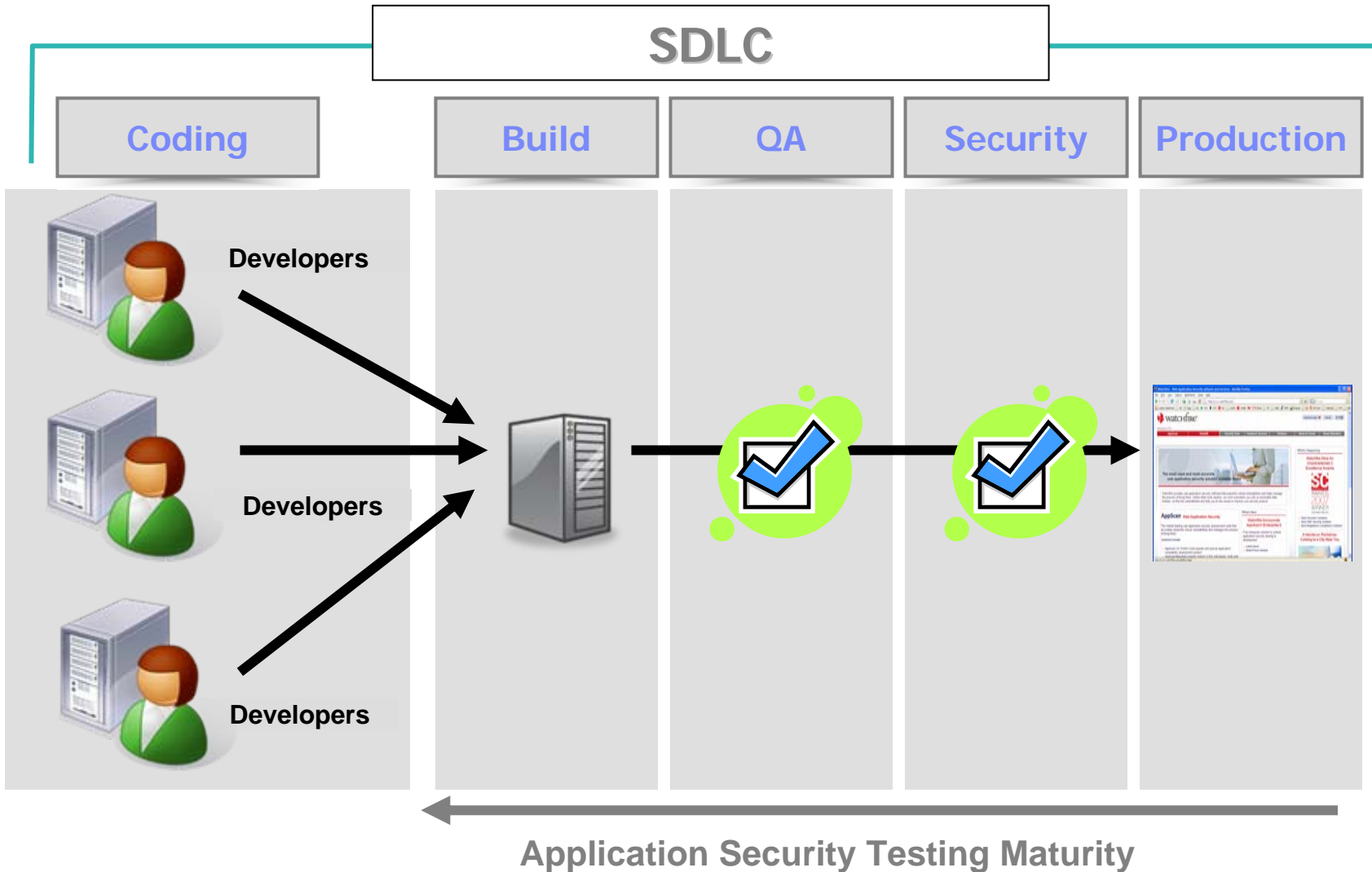
1. Software developers were never trained (or mandated) on security
2. Existing defenses do not address application level threats
3. Security teams are focused on other issues (network, desktops, etc) and overwhelmed
4. No defined policy, accountability or process to deal with this issue



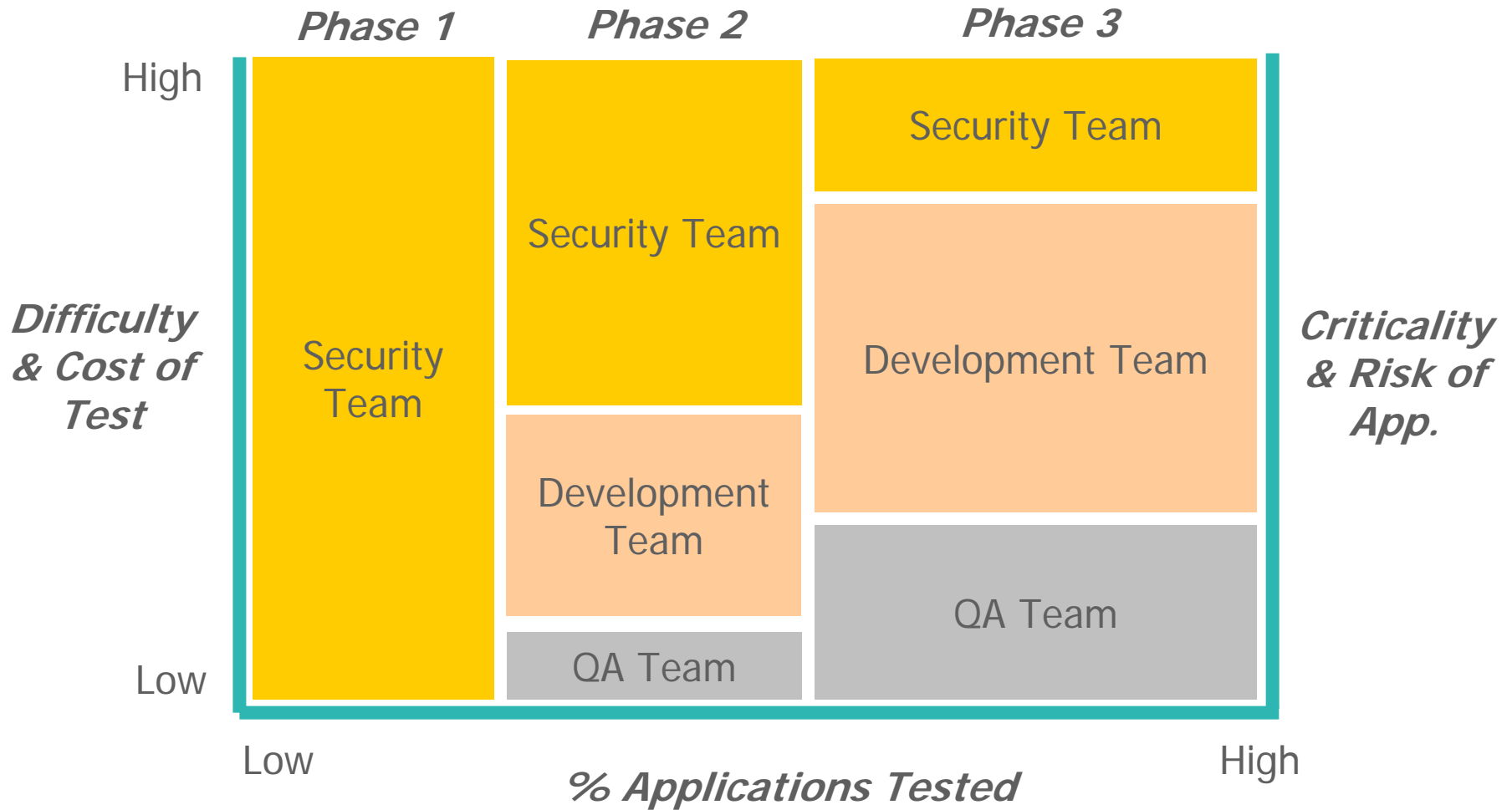
Application Security Maturity Model



Security Testing Within the Software Lifecycle



Application Security Adoption Within the SDLC

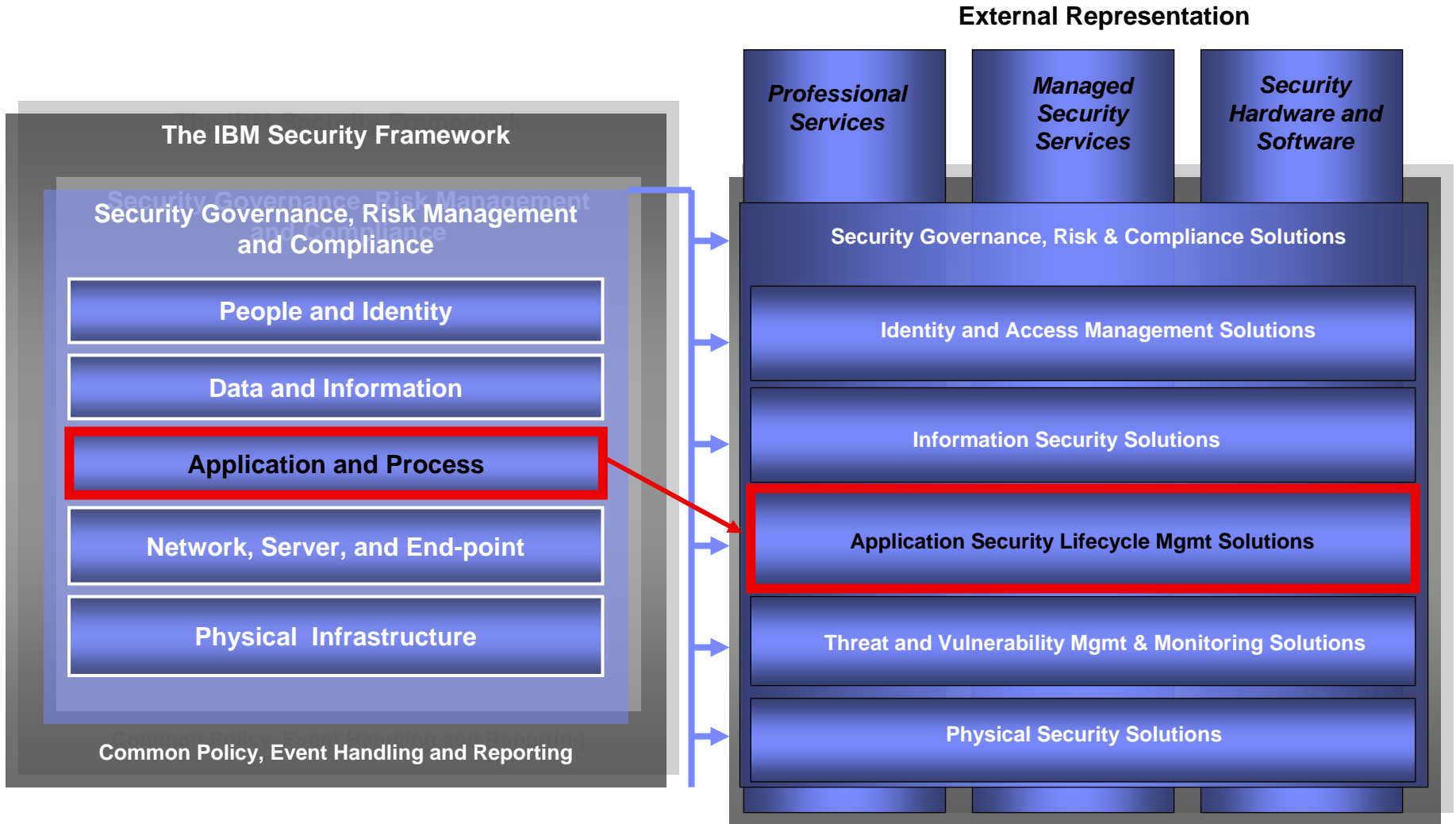


Agenda

- Introduction to Application Security
- **IBM Application Security Solutions**
- Reference



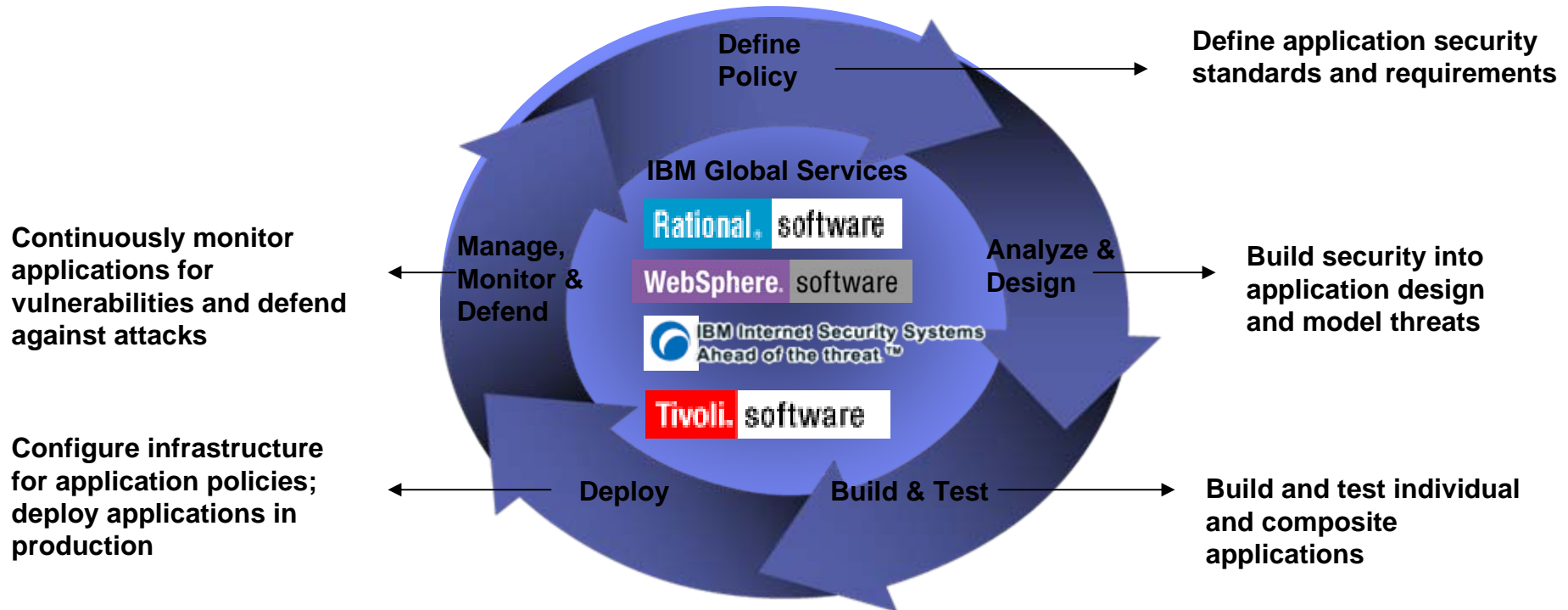
IBM Security Framework



IBM is laying the foundation for end-to-end application security

- IBM Global Services – **security risk assessments** helping define policies and processes
- Rational – **automated vulnerability testing** for web applications/web services across the development cycle
- IBM Technology Services/ISS – **managed services** for network and application vulnerability assessment
- Tivoli – **access control and security information** and event management to web applications/web services
- DataPower – **provides SOA security solutions**

Application Security Management Lifecycle



Rational AppScan: Find and fix web application security and compliance issues

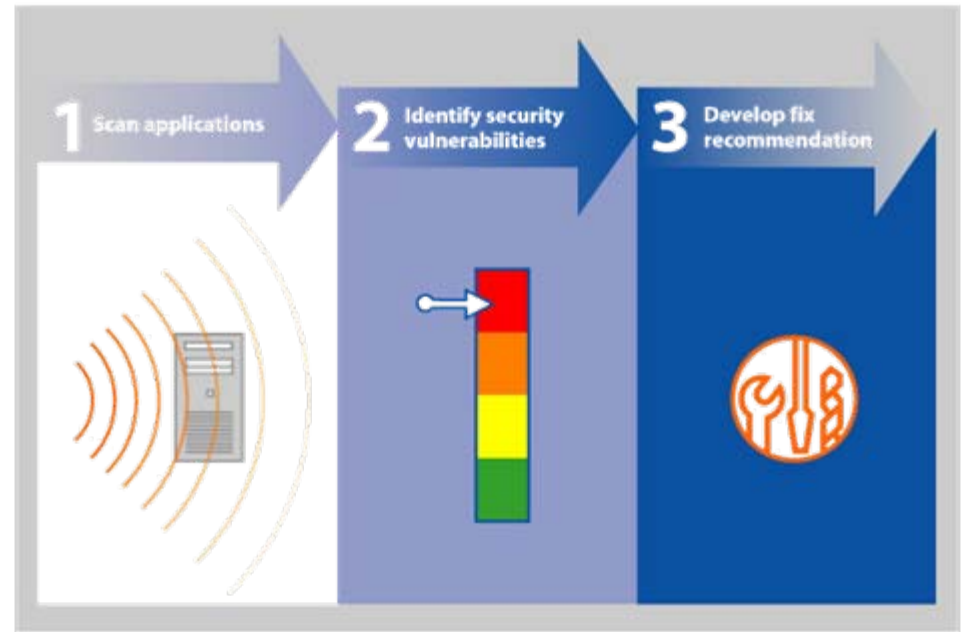
AppScan[®]

WEB APPLICATION SECURITY

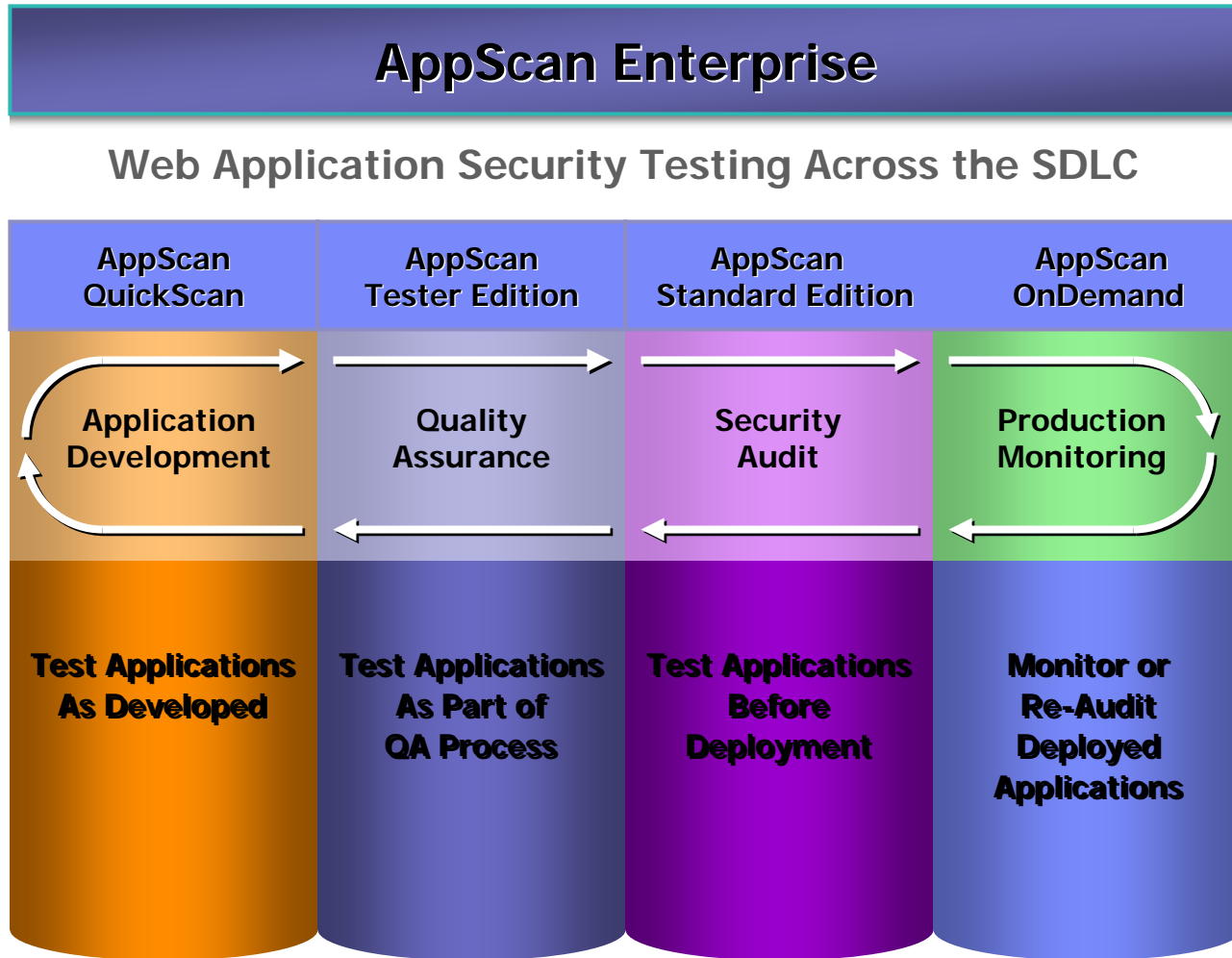


Web application and web service security testing

- ✓ Individual and enterprise scalable solutions for assessing and remediating security vulnerabilities
- ✓ Different solutions for developers, testers, security professionals, and management



Watchfire Application Security Testing Products



AppScan - Automated Application Security Testing

The screenshot displays the Watchfire AppScan interface. The main window is titled "Untitled - Watchfire AppScan" and features a menu bar (File, Edit, View, Scan, Tools, Help) and a toolbar with icons for New, Open, Save, Print, Scan, Stop, Manual Explore, Scan Configuration, Scan Log, Find, Report, and Update.

The interface is divided into several sections:

- Left Panel:** Contains navigation options: "Security Issues" (with a lock icon), "Remediation Tasks" (with a checkmark icon), and "Application Data" (with a magnifying glass icon).
- Tree View:** Shows the scanned application structure:
 - My Application (48)
 - http://red/ (48)
 - / (10)
 - _vti_pvt (1)
 - admin (1)
 - bank (22)
 - / (4)
 - account.aspx (5)
 - apply.aspx (1)
 - comment.aspx
 - confirmcard.aspx (1)
 - contact.aspx (1)
 - content.aspx (1)
 - default.aspx (1)
 - login.aspx (3)
 - logout.aspx
 - search.aspx (1)
 - transfer.aspx (1)
 - welcome.aspx (2)
 - images (1)
 - bin (1)
 - include (1)
 - login (1)
 - src (1)
 - transfer (10)

- Right Panel:**
- Arranged By: Severity | Highest on top
- 48 Security Issues (75 variants) for 'My Application'
- Summary of issues:
 - Blind SQL Injection (2)
 - Poison Null Byte Files Retrieval (1)
 - SQL Injection (1)
 - XPath Injection (1)
 - Alternate Version of File Detected (1)
 - Directory Listing (6)
 - Temporary File Download (5)
 - TRACE and TRACK HTTP Methods Enabled (1)
 - .NET Solution File Download (1)
 - Application Error (2)
- Selected Issue: **Blind SQL Injection**
 - Severity: High
 - Type: Application-level test
 - WASC Threat Classification: [Command Execution: SQL Injection](#)
 - CVE Reference(s): N/A
 - Security Risk: It is possible to view, modify or delete database entries and tables
 - Possible Causes: Sanitation of hazardous characters was not performed correctly on user input
 - Technical Description: Web applications often use databases at the backend to interact with the enterprise data warehouse. The de-facto standard language for querying databases is SQL (each major database vendor has its own dialect). Web applications often take user input (taken out of the HTTP request) and incorporate it in an SQL query, which is then sent to the backend database. The query results are then processed by the application and sometimes displayed to the user. This mode of operation can be exploited by an attacker if the application is not careful enough with its treatment of user (attacker) input. If this is the case, an attacker can inject malicious data, which when incorporated into an SQL query, changes the original syntax of the query into something completely different. For example, if an application uses user's input (such as username and password) to query a database table of users' accounts in order to authenticate the user, and the attacker has the ability to inject malicious data into the username part of the query (or the password part, or both), the query can be changed into a different data yanking query, a query that modifies the database, or a query that runs shell commands on the database server.
- Bottom Panel:**
- Visited URLs: 20/88
- Completed Tests: 8697/9146
- Summary: 48 Security Issues, 5 High, 13 Medium, 14 Low, 16 Info

AppScan Enterprise – Dashboards and Metrics

IBM Rational AppScan Enterprise Edition

Jim (Analyst) | Help | Support | About | Log Out

Training | Jobs & Reports | Administration

Jobs & Reports > Acme Hackme > Analysts

Folders

Create... Edit Delete

- Acme Hackme
 - Analysts
 - Frank
 - Jim
 - Developers
 - Admin
 - Andrew
 - Chris
 - Jennifer
 - Templates

Analysts - Graphical

Last Updated: 9/11/2007 12:56:50 PM

Details | Graphical

Report Pack: All Report Packs [Apply]

Issue Severity History

All Report Packs

Issue Management History

All Report Packs

Issue Severity by Report Pack

WASC Threat Classification

All Report Packs

Recently Viewed

- Analysts
- Applications
- Security Issues (Investment Banking)
- Report Pack Summary (Investment Bank)
- Sarbanes-Oxley Act (SOX) (Investment)
- Activity Log (Test Admin)
- Report Pack Summary (Test Admin)
- Personal Banking

Support

On-Demand Services

Store

Main Website

Intranet

Movies

Integrated Computer Based Training

Key to adoption across the organization is education

The screenshot shows a Microsoft Internet Explorer browser window displaying a training slide titled "AppScan Knowledge OnDemand". The slide content includes a bulleted list of features and a sidebar with a table of contents.

AppScan Knowledge OnDemand

- Self-service – more convenient than traditional training
 - Participants no longer have to schedule time "out of the office"
- Self-paced – greater information retention
 - With digestible content modules, participants no longer experience information overload
- Just-in-time reference-ability
 - Full access to searchable, online content for 12 months
- Structure
 - Courses are individual modules
 - Typically 15 minutes or less

watchfire®

Outline	Thumb	Notes	Search
Slide Title			Duration
How to Use AppScan ...			00:09
Topics			00:10
AppScan University			00:12
AppScan Knowledge ...			00:42
Enrollment And Loggi...			00:44
Selecting Your Course			00:33
Viewing Your Course			00:19
Using the Navigation ...			00:52
Summary			00:15
Thank You!			00:13

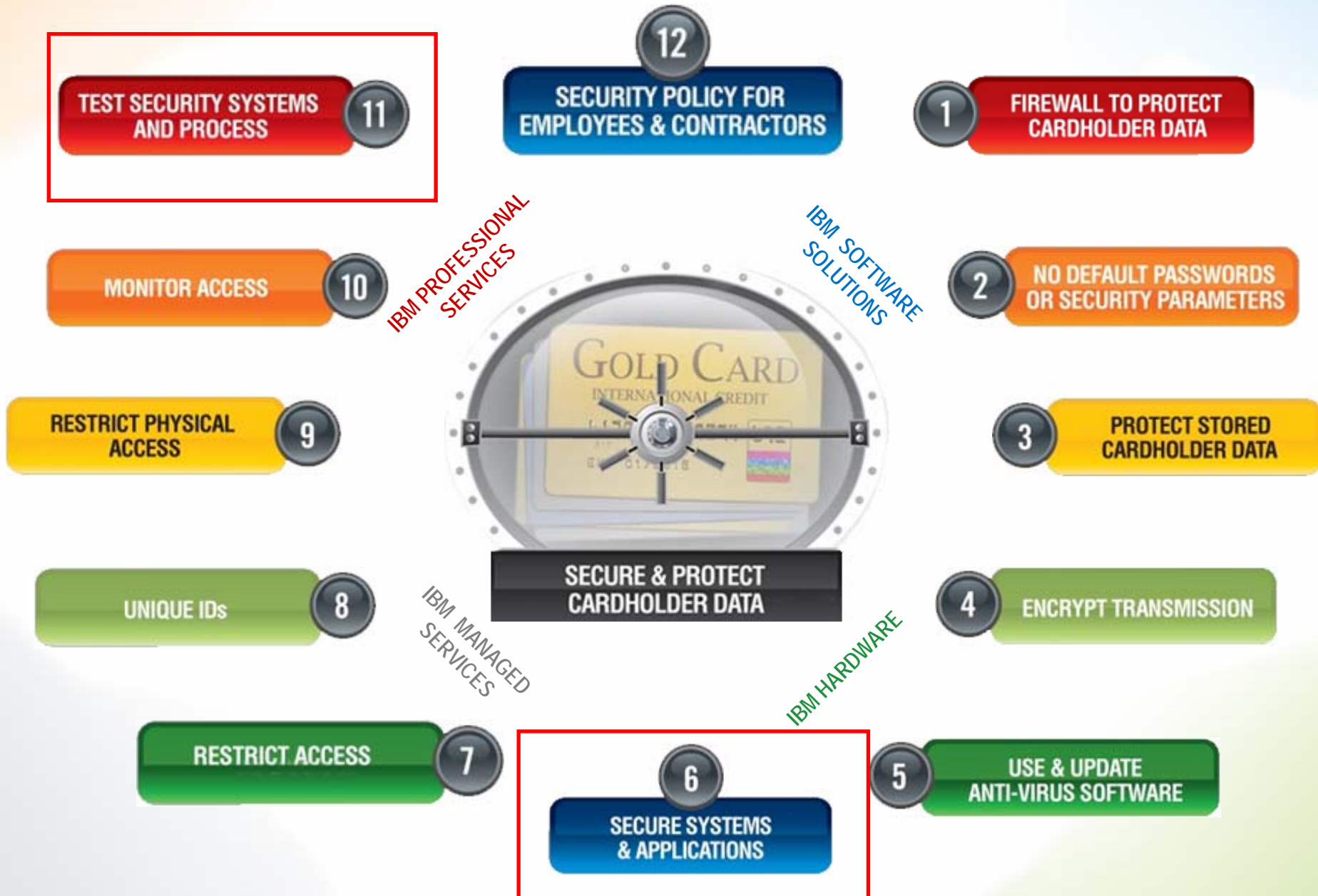
2 Minutes 59 Seconds Remaining

Slide 4 / 10 | Playing 00:39 / 00:42

Start | 7:55:46 - AT... | Microsoft... | Gina Stefan | Microsoft Po... | Watchfire - | http://dow... | 100% | 4:10 PM

IBM Services, Software and Hardware:

Only IBM has solutions to address all 12 PCI requirements



Agentrics Application Security

The screenshot shows the Agentrics website interface. At the top, there is a navigation menu with links for COMPANY, SOLUTIONS, SERVICES, PARTNERS, NEWS & EVENTS, and LIBRARY. A red banner highlights 'GLOBAL SOLUTIONS' with the tagline 'From the Trusted Retail Industry Agent'. Below the banner, there are several news and event sections. The 'IN THE NEWS' section lists articles from 2/11/08 and 1/14/08. The 'UPCOMING EVENTS' section mentions a registration event for February 26-28, 2008. Various partner logos and awards are also displayed on the page.

- Challenge
 - ▶ Agentrics, a leading solution provider to the world's largest retailers and their suppliers, leverages the latest web-based technology and services for its clients

- Solution
 - ▶ In a competitive evaluation, AppScan was better at finding vulnerabilities than any other solution

- Result
 - ▶ increased confidence and safer applications for their high-profile retail clients



Depository Trust and Clearance Corporation (DTCC)

Application Security

- Challenge:
 - ▶ applications handle clearance and settlement of more than \$1 quadrillion in securities transactions per year – security is imperative
 - ▶ need to implement security as part of the application development process

- Solution:
 - ▶ educated 450 developers on testing security across the SDLC
 - ▶ acquired AppScan for vulnerability scanning

- Result:
 - ▶ Security is designed and built into more than 225 new applications per year
 - ▶ Stabilized processes and practices leverage AppScan for industrial-strength vulnerability assessment and remediation for high risk and complex applications



Agenda

- Introduction to Application Security
- IBM Application Security Solutions
- **Reference**



IBM Rational AppScan - a Recognized Leader

- **#1 World-wide market share revenue position (2006) according to Gartner**

Source: Gartner Dataquest, "Market Share: Application Development and Project and Portfolio Management Software, Worldwide, 2006," Laurie F. Wurster, Asheesh Raina, Fabrizio Biscotti, 22 May, 2007.

- **# 1 World-wide market share revenue position according to IDC**

Source: Worldwide Security and Vulnerability Management Software 2006-2010 Forecast and Analysis: Managing Security Knowledge and Control, IDC #204693, December 2006

- **Winner of SC Magazine's top Security Company 2007**
- **Winner SD Times 100 security category**
- **Winner of Dr. Dobb's Journal 17th annual Jolt Award for security**
- **Watchfire named one of the top 25 innovations by Financial IT Security Magazine in its 2007 "Future Now" list**

For additional information

- **IBM Security Defense**

<http://www-306.ibm.com/software/tivoli/governance/security/defend.html>

- **IBM Rational AppScan**

<http://www-306.ibm.com/software/rational/offerings/testing/webapplicationsecurity/>

- **IBM Tivoli Access Manager for e-business**

<http://www-306.ibm.com/software/tivoli/products/access-mgr-e-bus/>

- **IBM Internet Security Solutions**

<http://www-935.ibm.com/services/us/index.wss/offerfamily/igs/a1025846>





Learn more at:

- [IBM Rational software](#)
- [IBM Rational Software Delivery Platform](#)
- [Process and portfolio management](#)
- [Change and release management](#)
- [Quality management](#)
- [Architecture management](#)
- [Rational trial downloads](#)
- [developerWorks Rational](#)
- [IBM Rational TV](#)
- [IBM Rational Business Partners](#)

© Copyright IBM Corporation 2007. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, the on-demand business logo, Rational, the Rational logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

