IBM Software Group

The New Imperative: Automating Web Application Security

Rational. software

Go to IBM

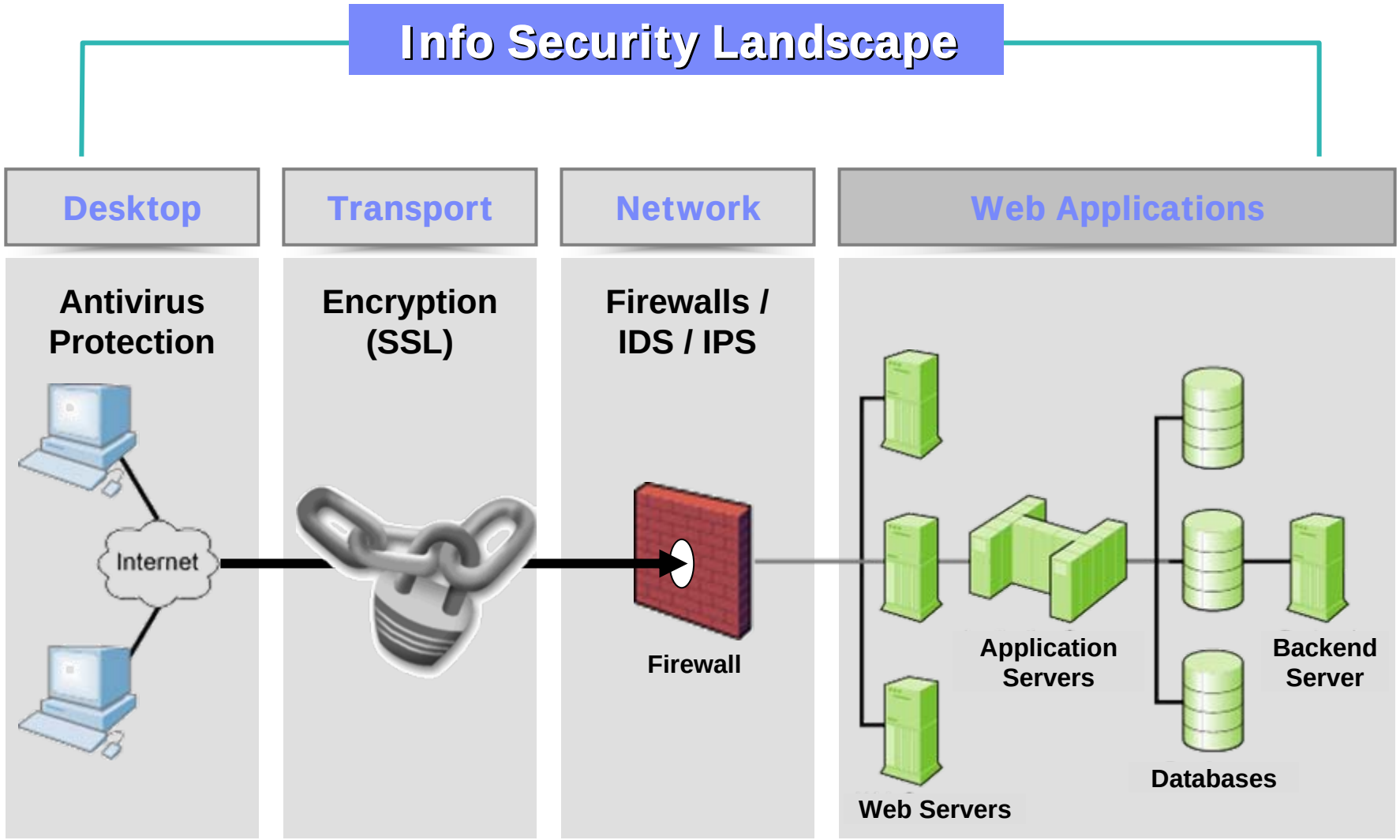
Agenda

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

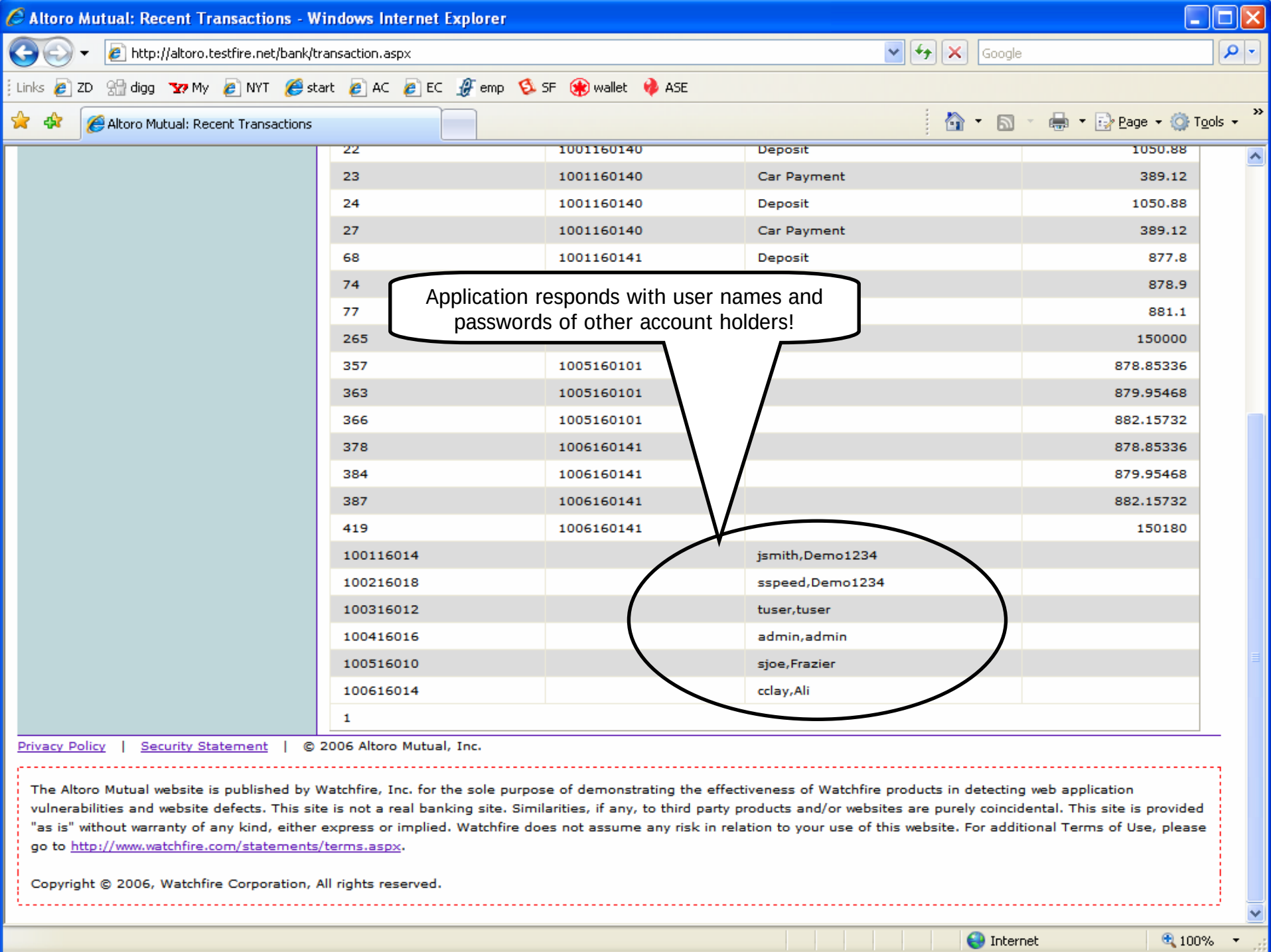
Agenda

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

Application Security - Understanding the Problem



Application Security Hacking Example



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

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

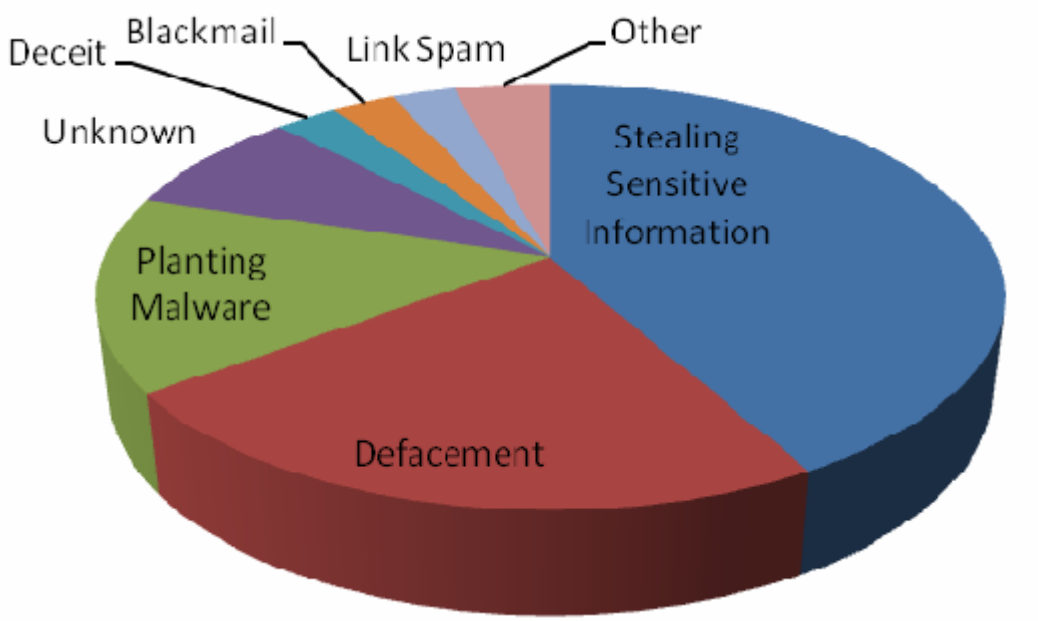
- **Security Breach**
  - Every lost record costs $138 to the organization who lost it
  - Media Attention > Brand Damage > Sharp Decline in Stock Prices

PCI Application Security Requirements

PCI Security Standards Council

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

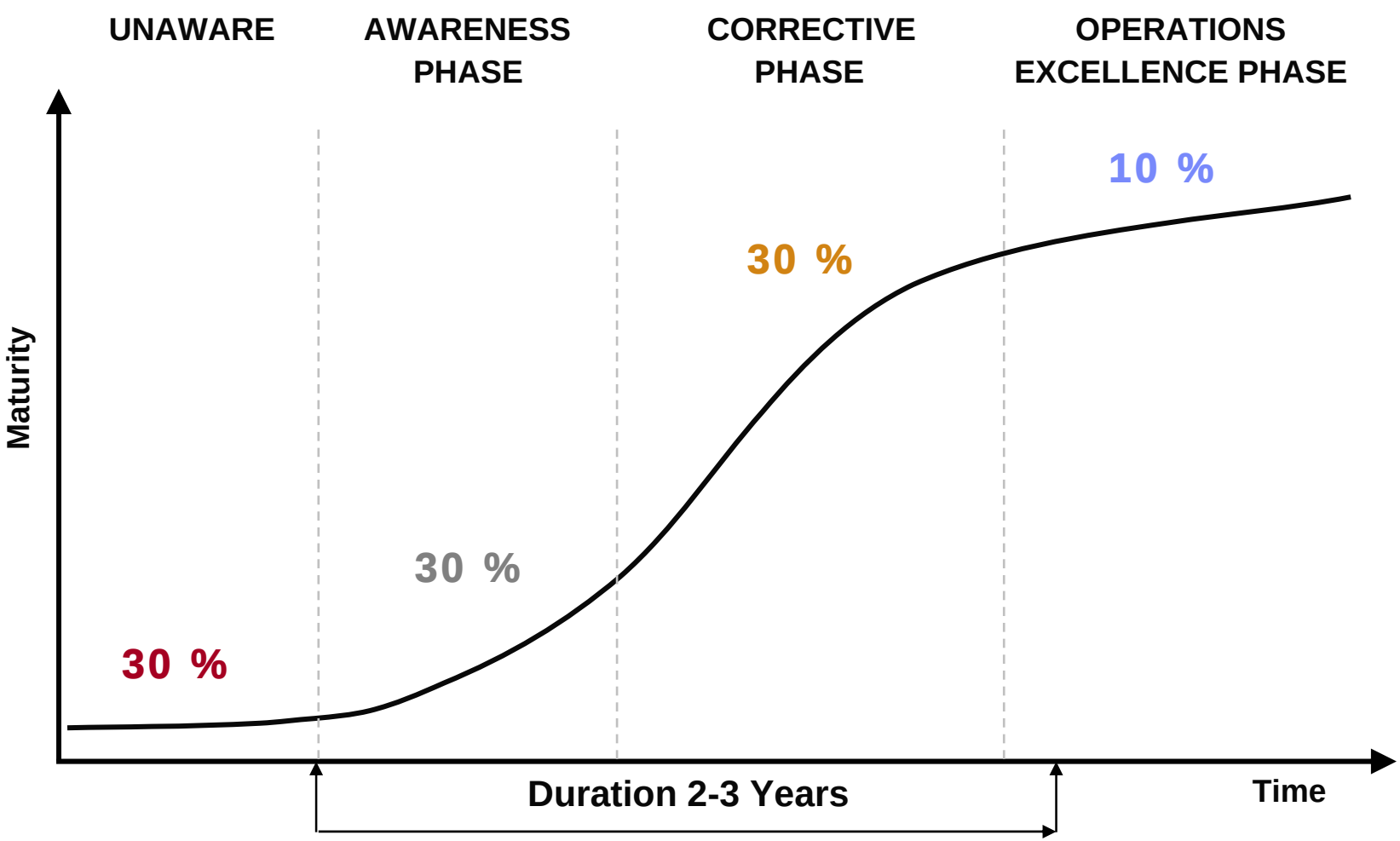
Source:

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

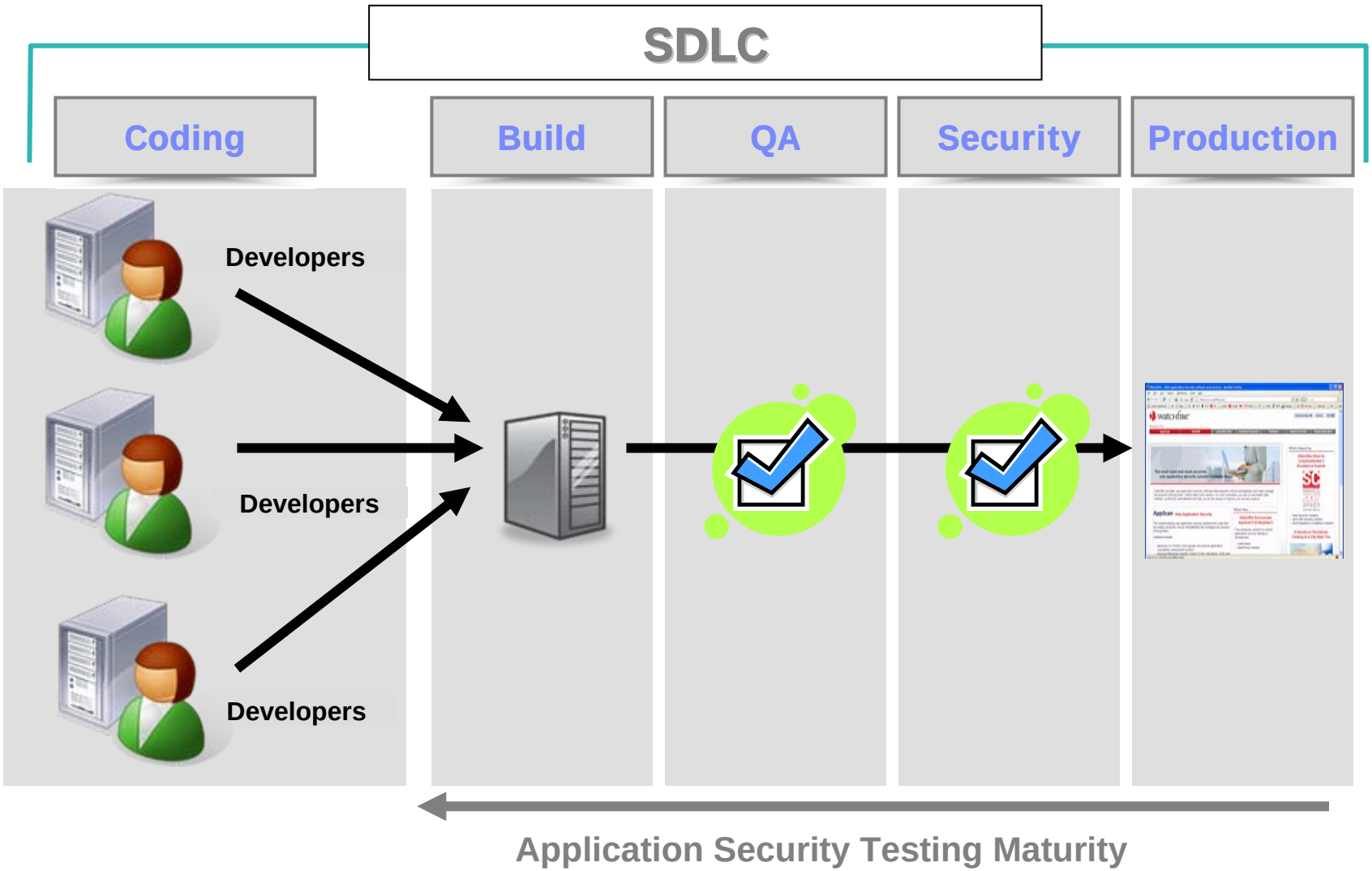
What's the Root Cause of this Problem?

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

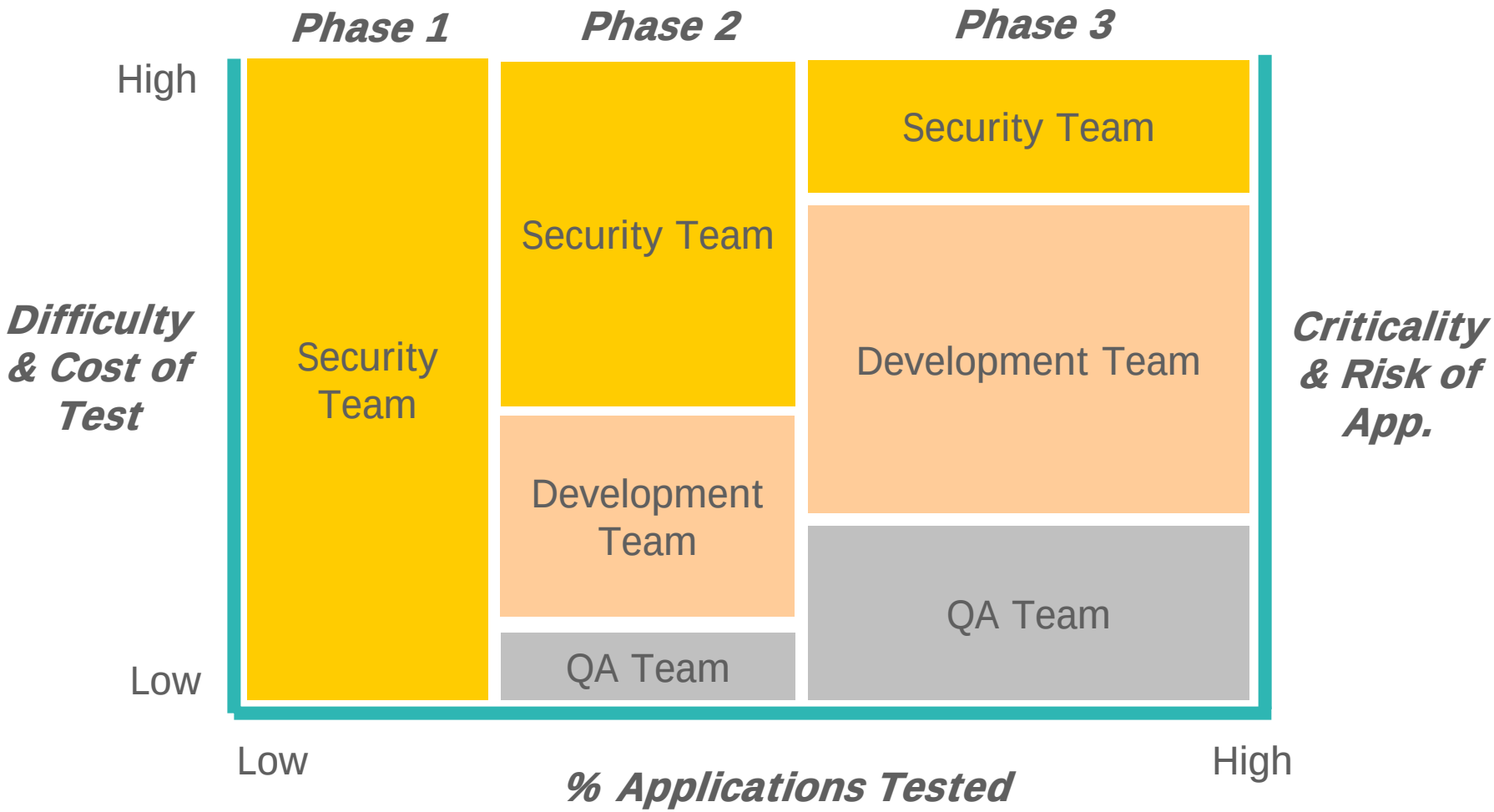
Application Security Maturity Model



Security Testing Within the Software Lifecycle



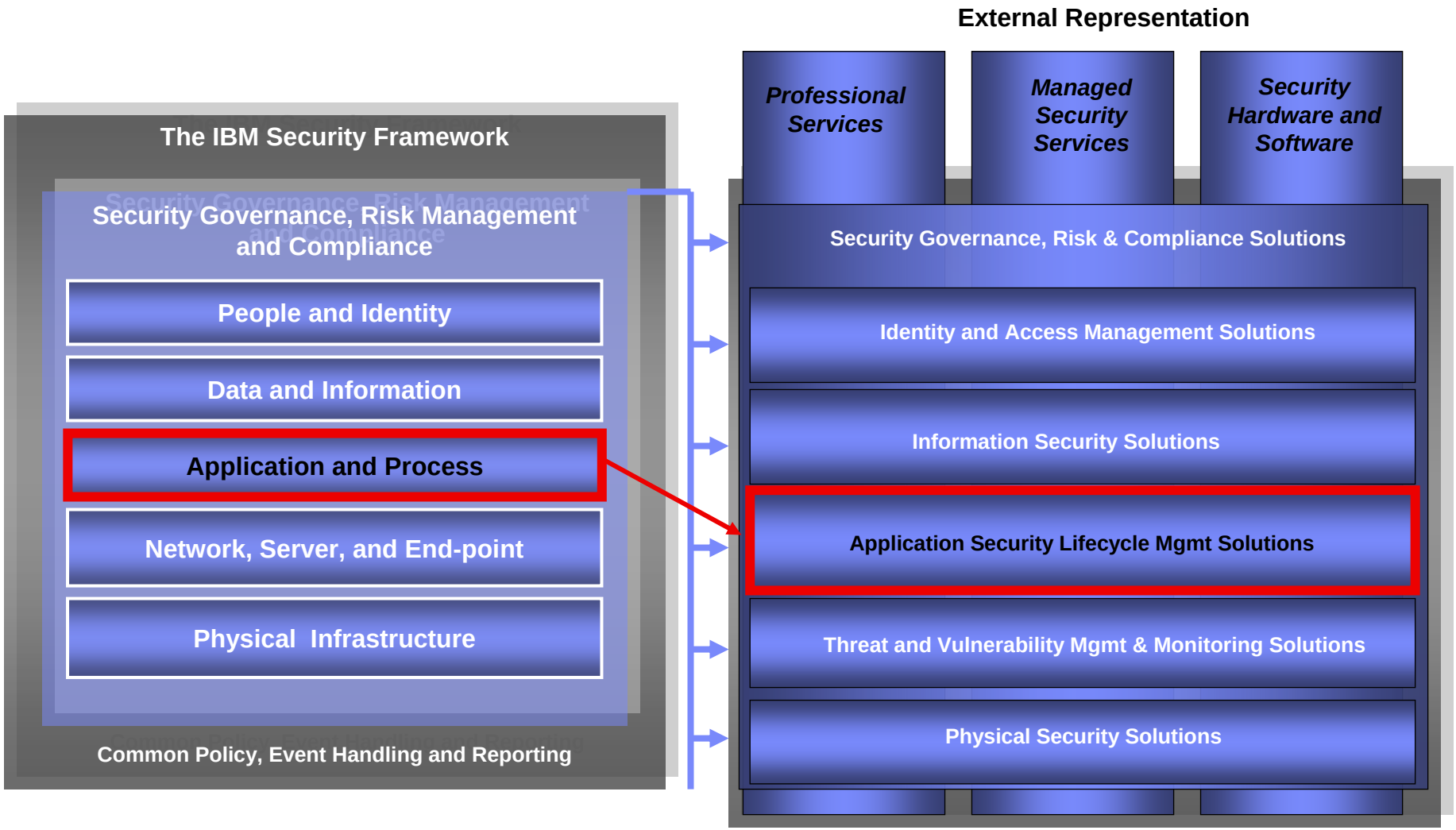
Application Security Adoption Within the SDLC



Agenda

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

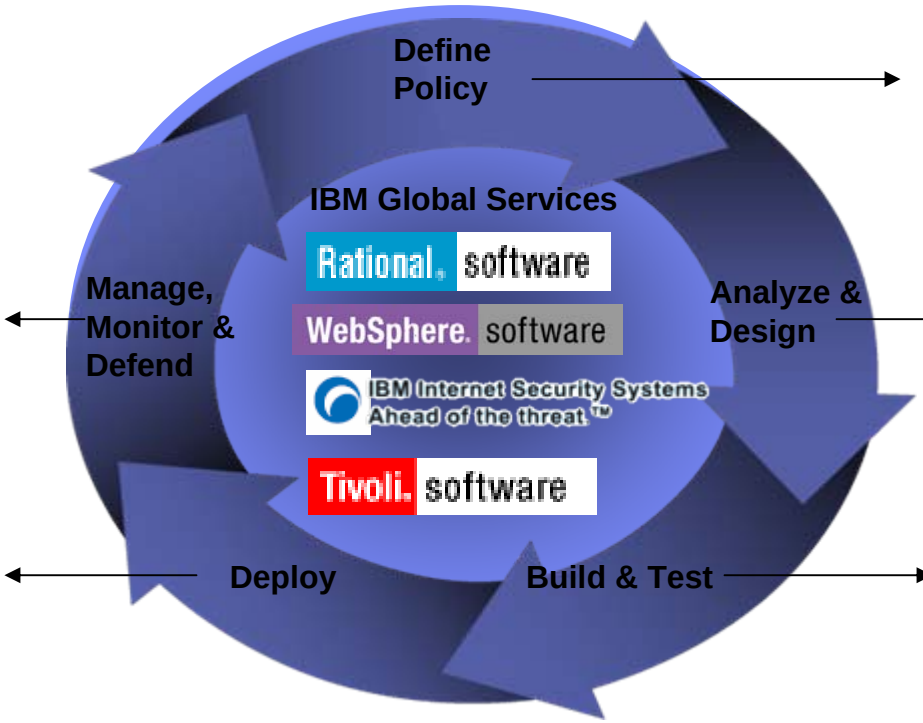
IBM Security Framework



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**

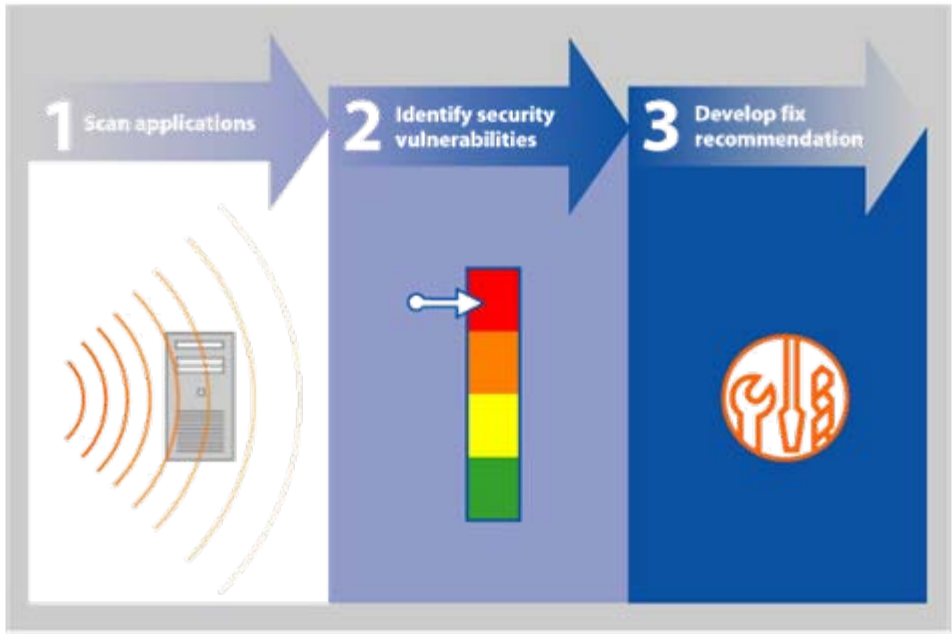
Application Security Management Lifecycle



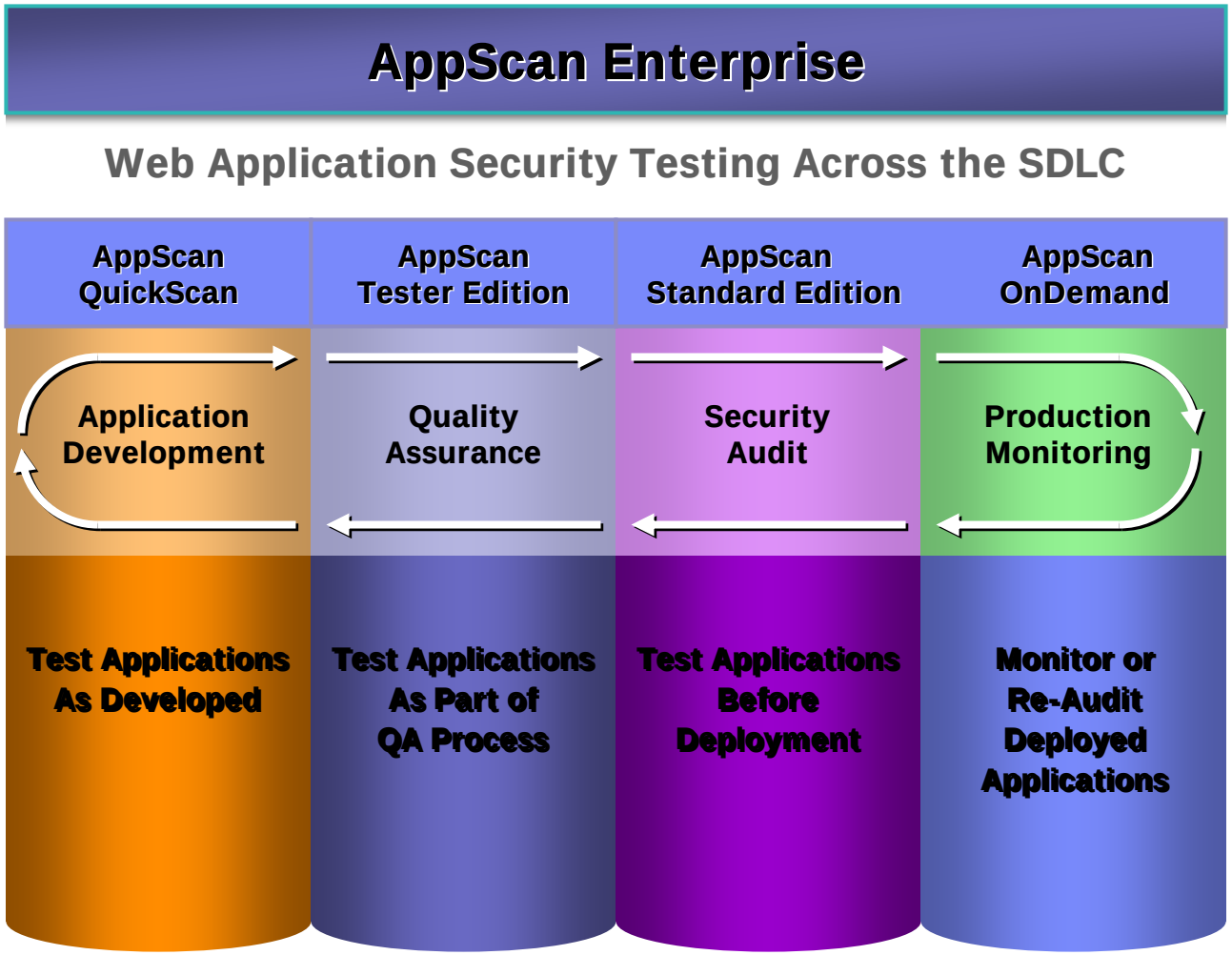
Rational AppScan: Find and fix web application security and compliance issues

Web application and web service security testing

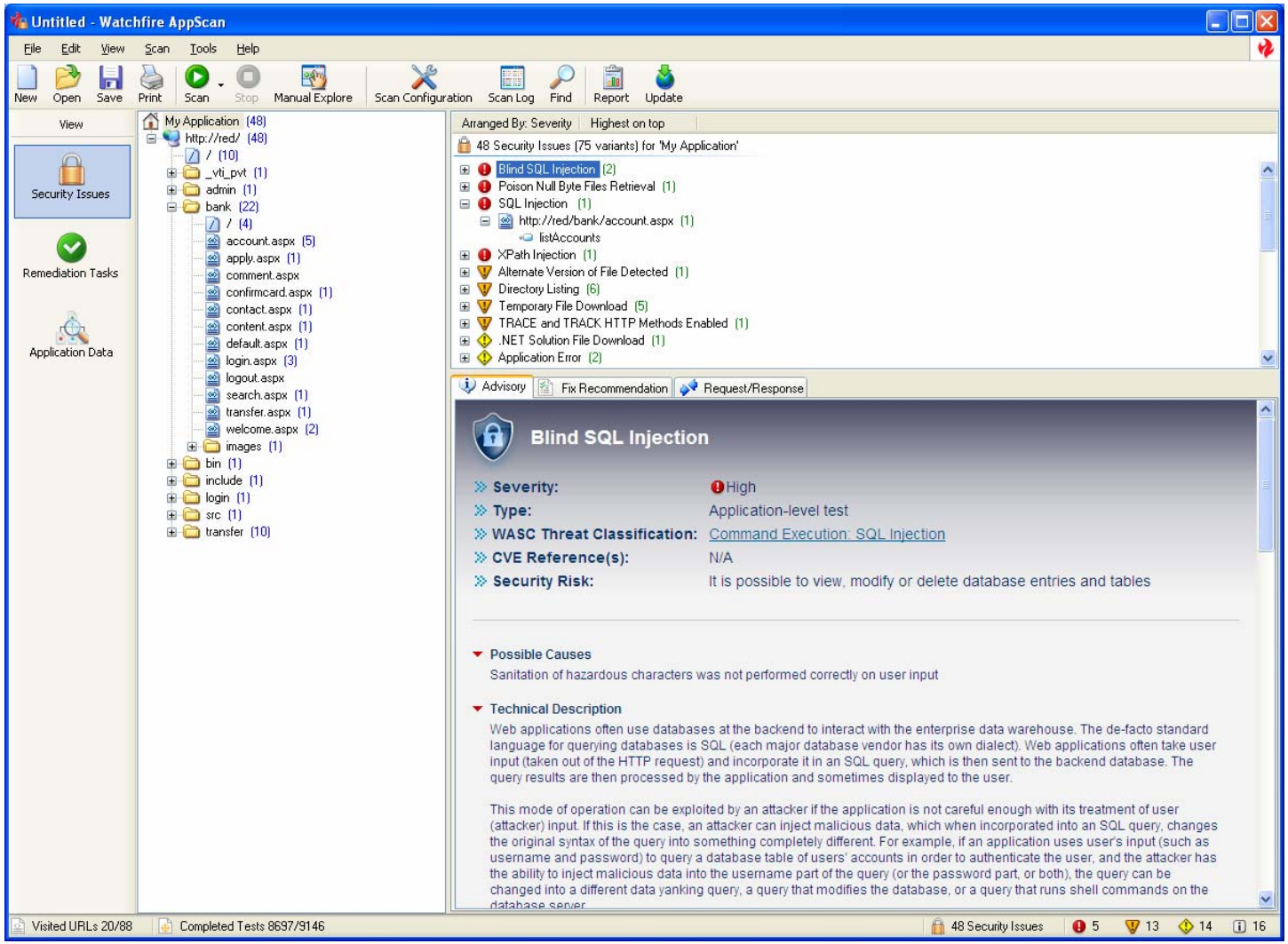
- ✓ **Individual and enterprise scalable solutions for assessing and remediating security vulnerabilities**
- ✓ **Different solutions for developers, testers, security professionals, and management**



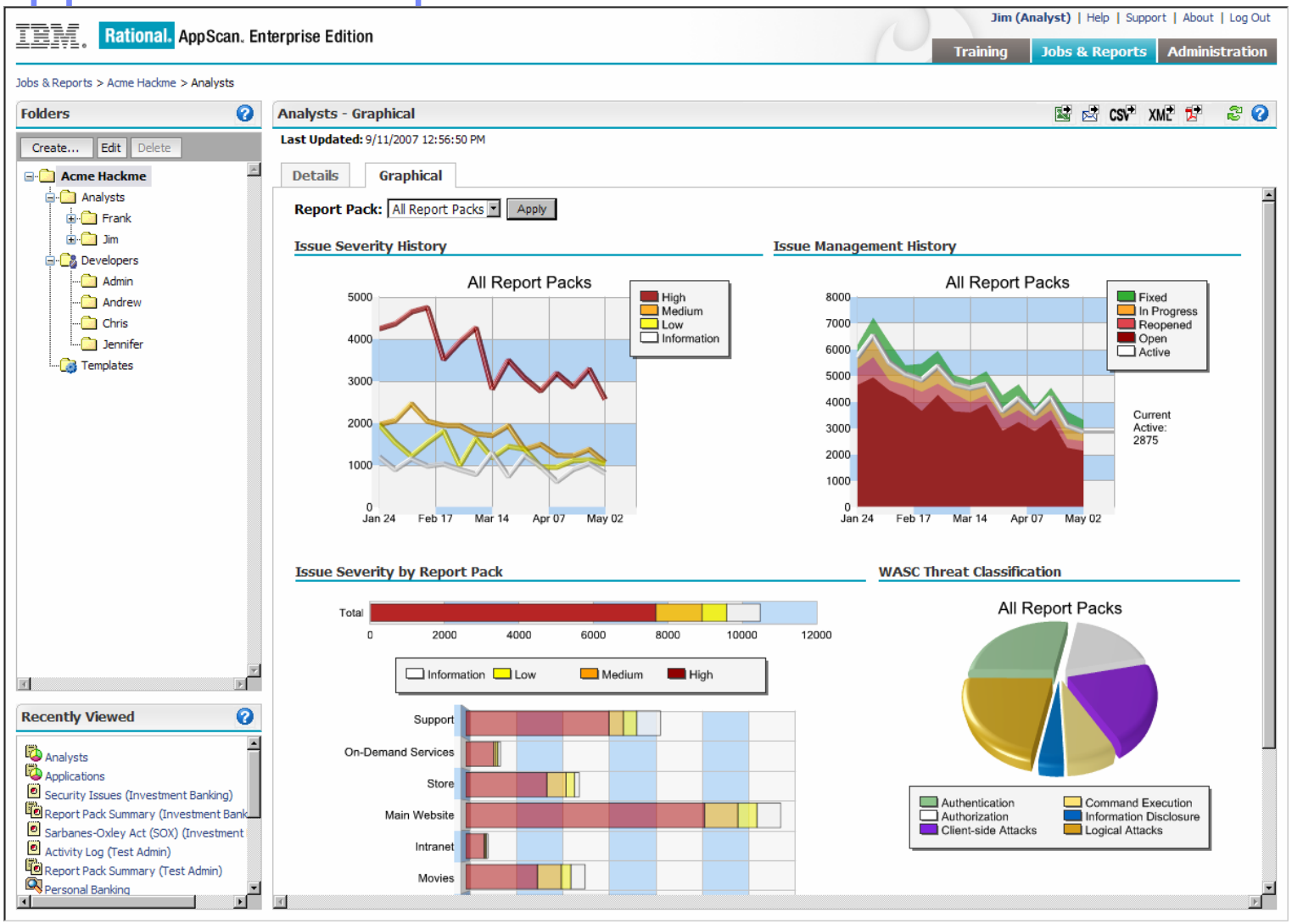
Watchfire Application Security Testing Products



AppScan - Automated Application Security Testing

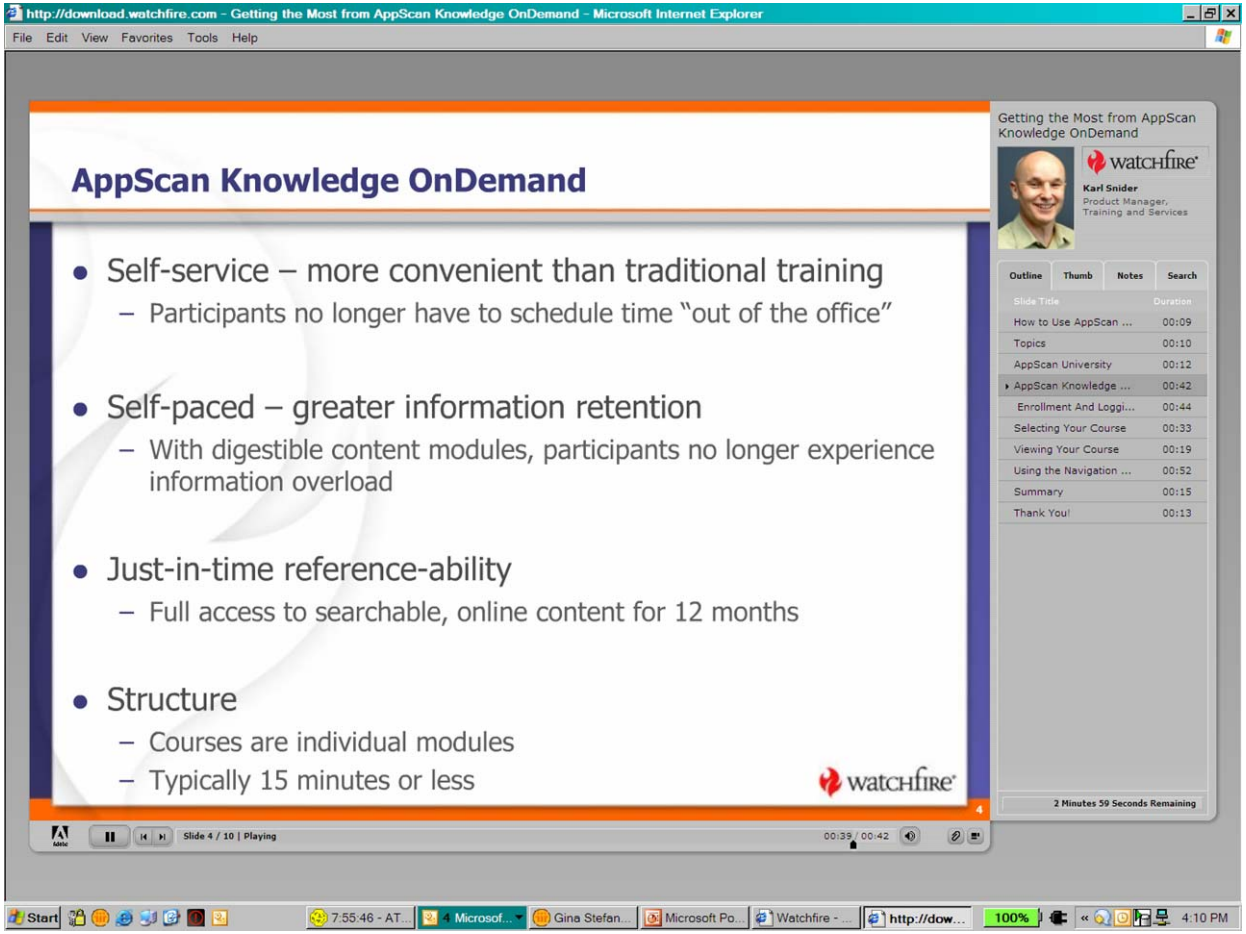


AppScan Enterprise – Dashboards and Metrics

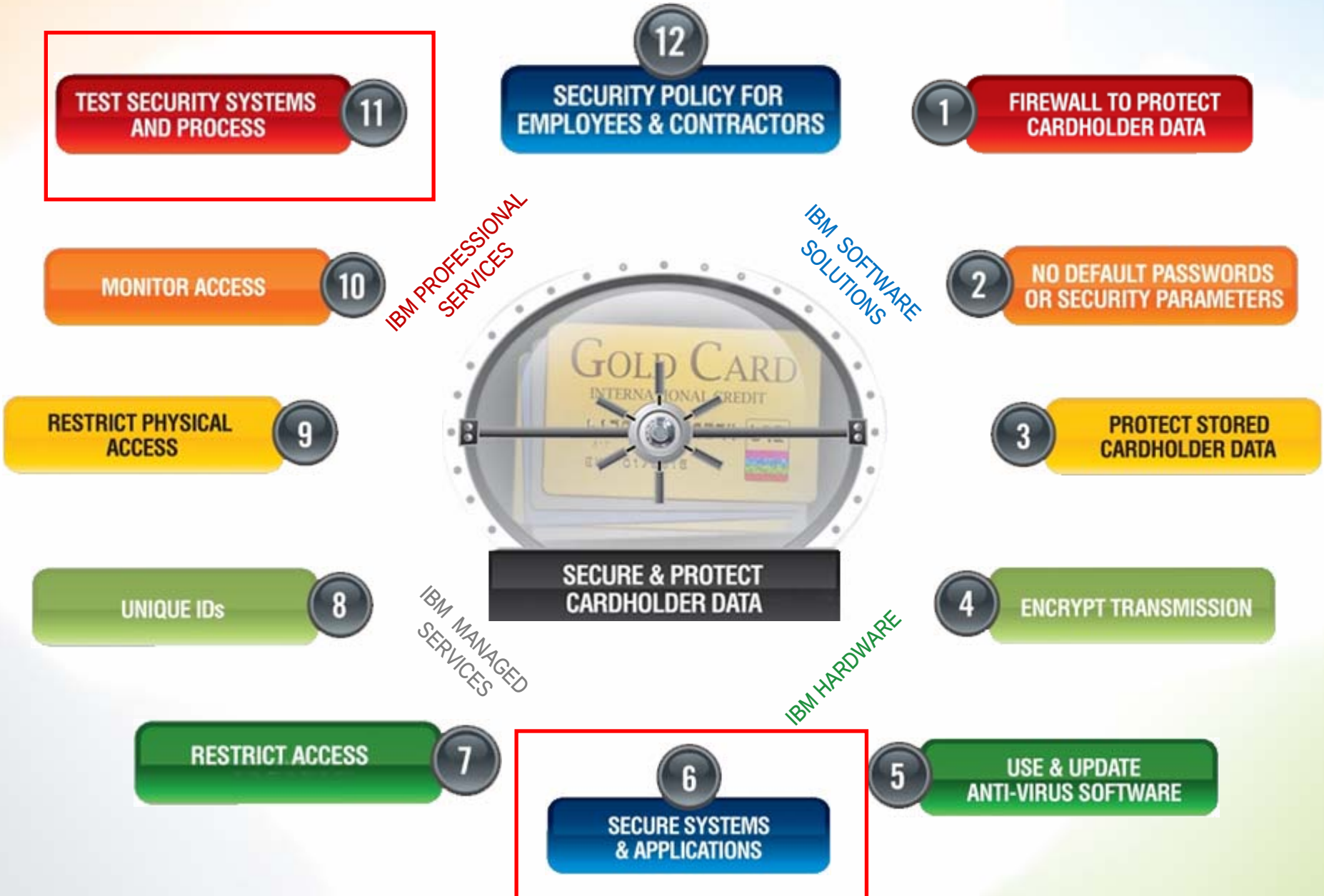


Integrated Computer Based Training

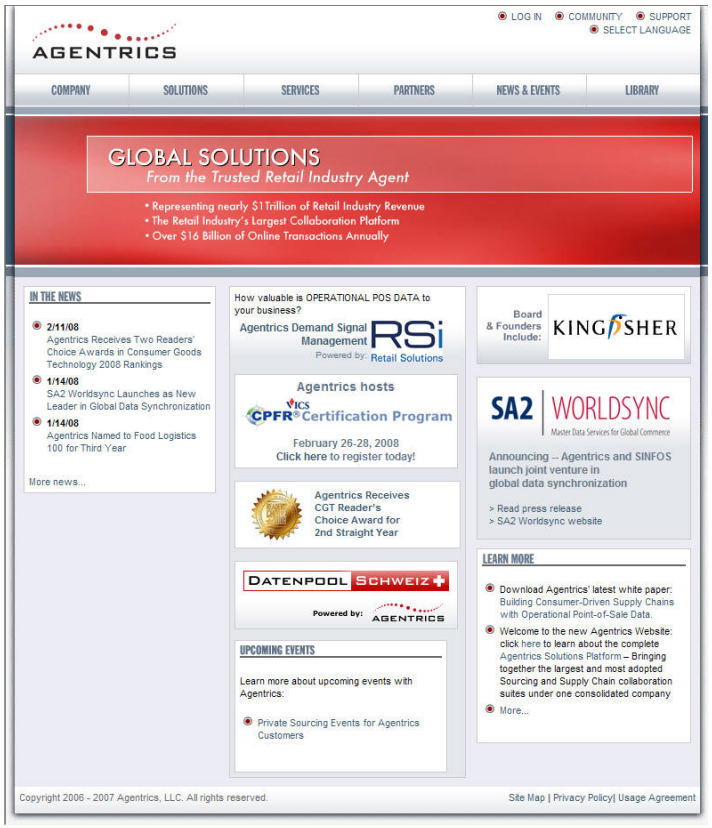
Key to adoption across the organization is education



IBM Services, Software and Hardware:
Only IBM has solutions to address all 12 PCI requirements

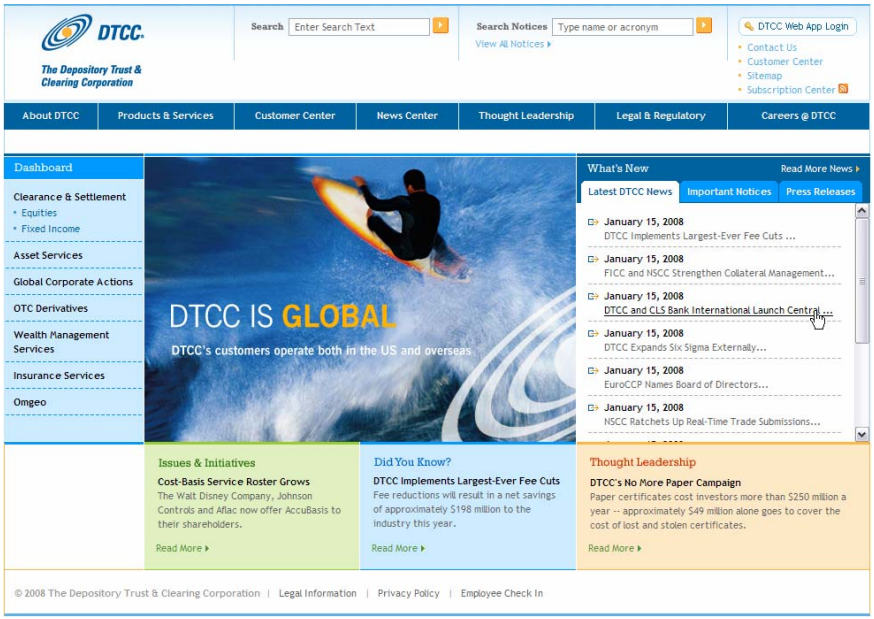


Agentrics
Application Security



- Challenge
  - Agrentrics, 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**
- **Selected as a "Top Pick" in the ITDefense Product Directory for 2007**

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