IBM Software Group

Security and Compliance are necessary: High costs are optional

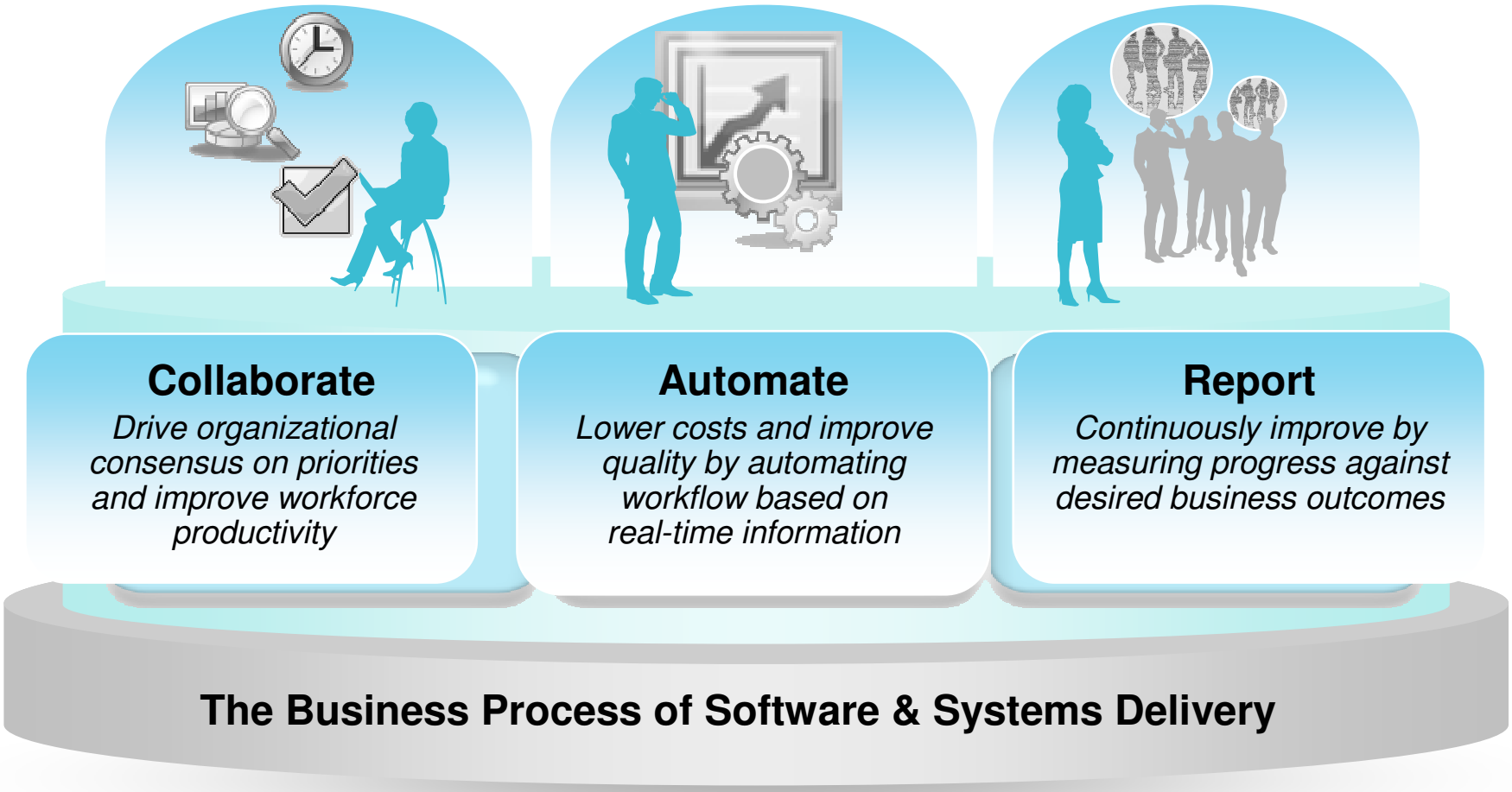
John Smith
Senior Security Architect

Go to IBM

Executive Summary

- Application security continues to be a top security threat
- Monetization of attacks, Regulatory Compliance (PCI), user demand (Web 2.0) and Enterprise Modernization (SOA) are driving awareness and action for security testing
- The cost and lack of coverage of reactive security is driving companies towards proactive measures – building security into the application development process
- Traditional approaches make it unlikely that development will support security testing due to schedule risks and potential project failure

Governing the process of software and systems delivery aligned with evolving business priorities

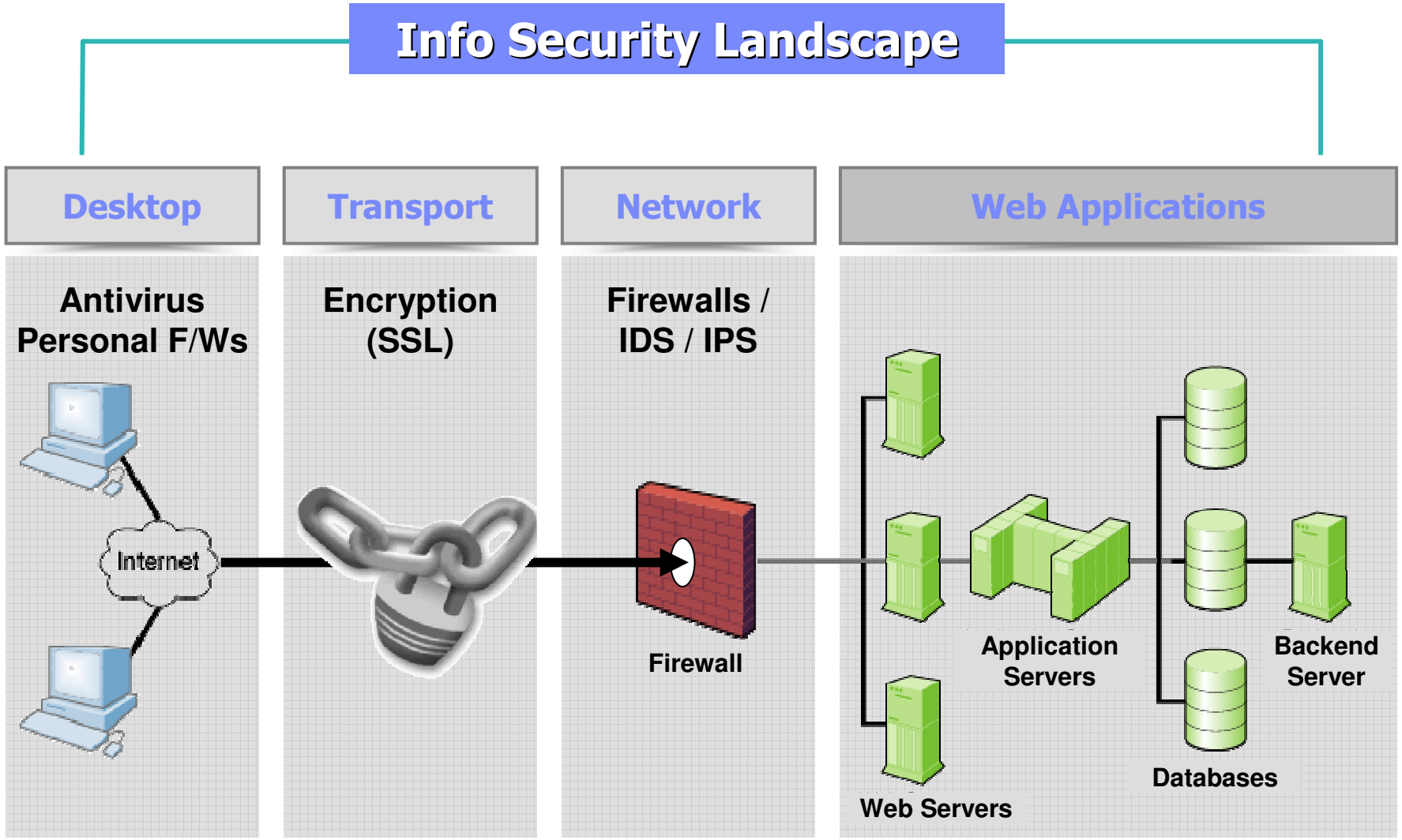


Agenda

- **Application Security Primer**
- Lowering the cost of compliance
- Case Studies

Go to IBM

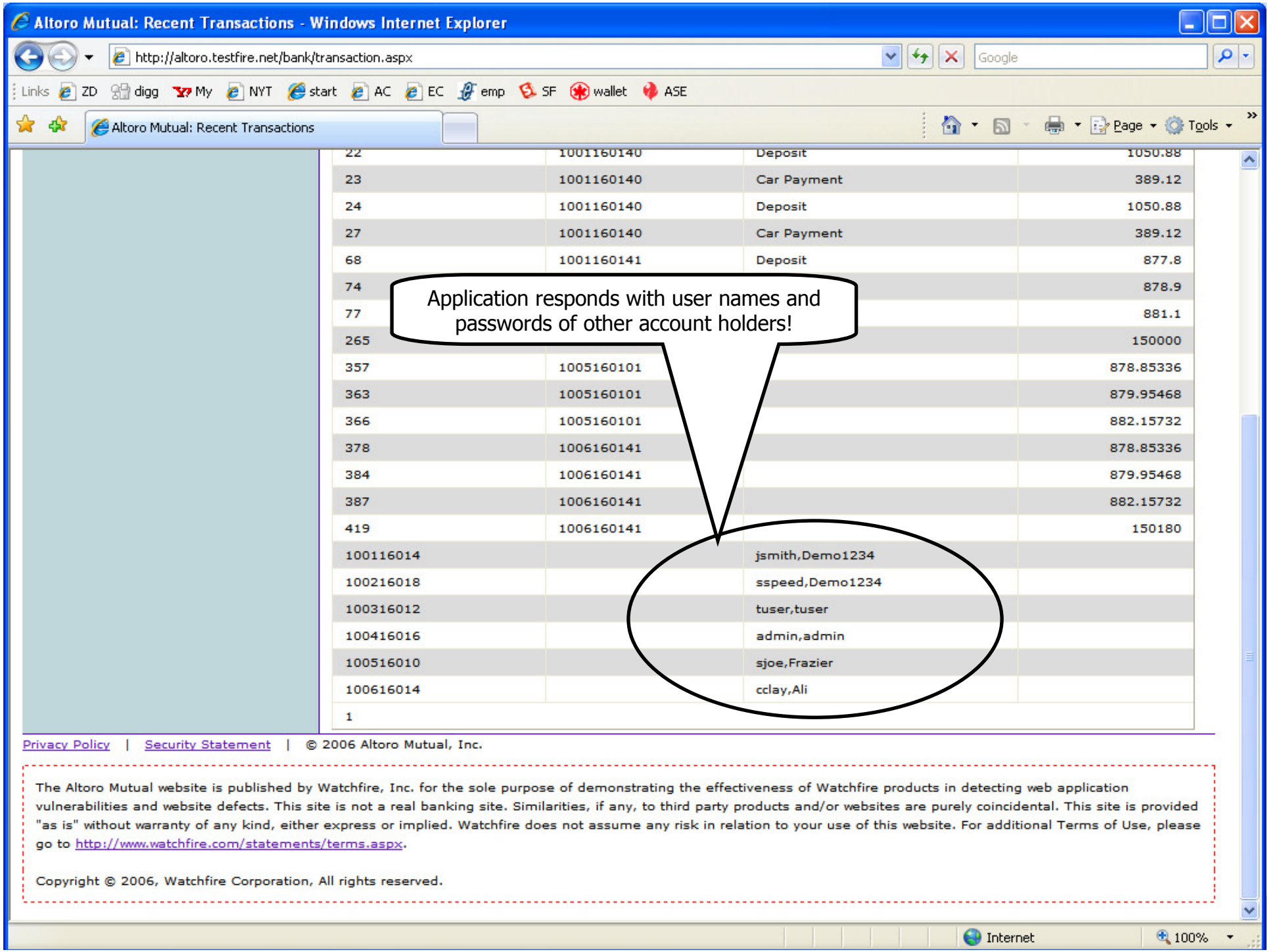
Application Security - Understanding the Problem



IBM Software Group

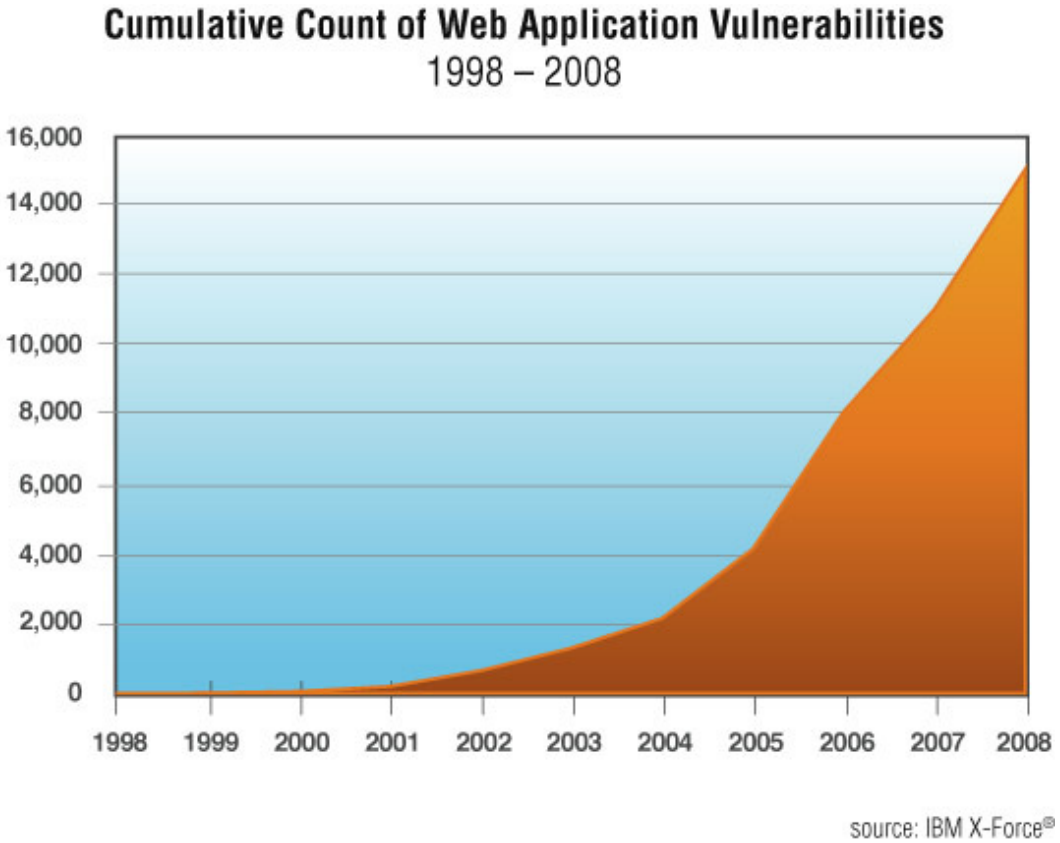
Application Security Hacking Example

Go to IBM

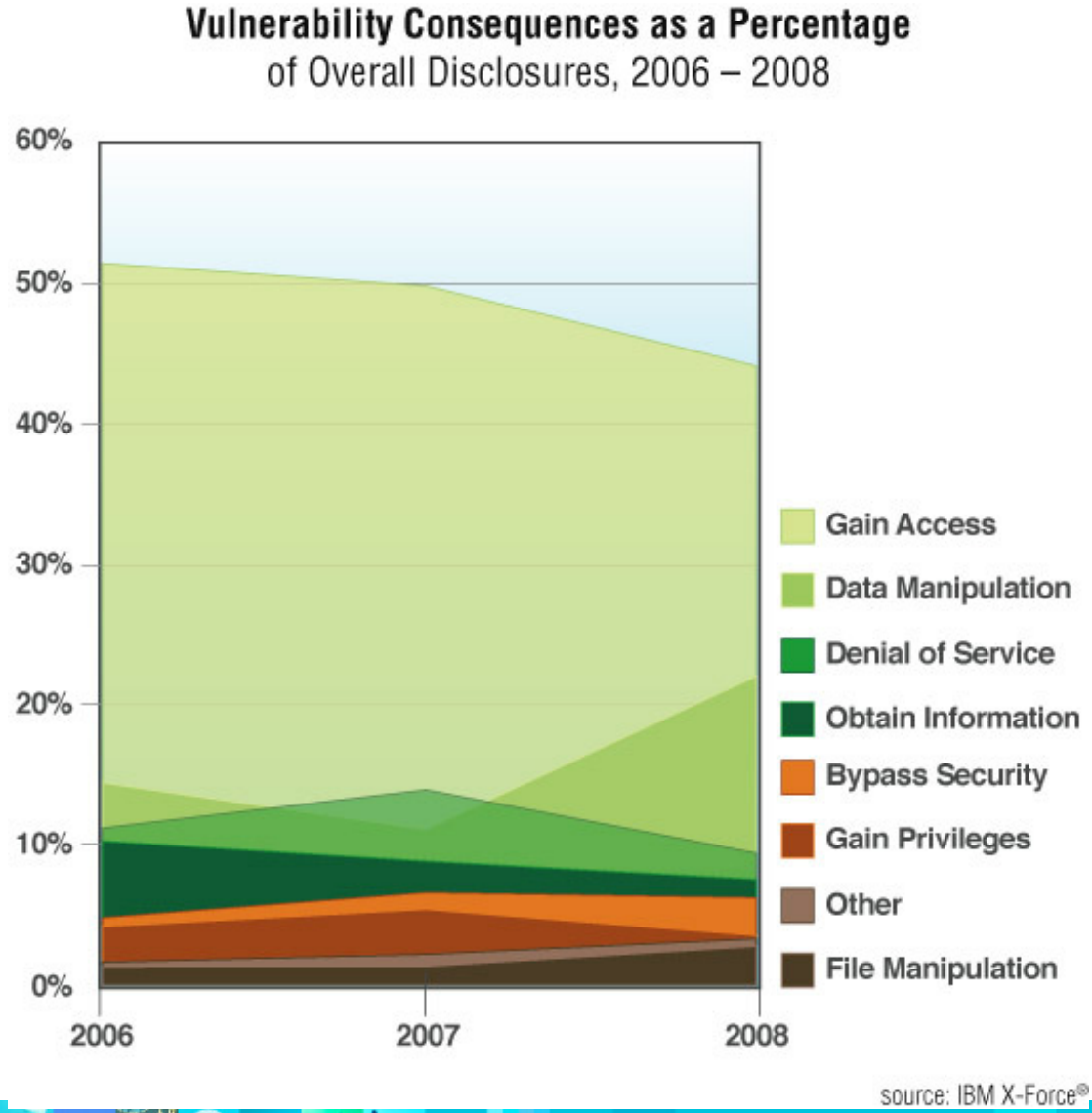

Altoro Mutual: Recent Transactions - Windows Internet Explorer
http://altoro.testfire.net/bank/transaction.aspx
Altoro Mutual: Recent Transactions
Application responds with user names and passwords of other account holders!
22 1001160140 Deposit 1050.88
23 1001160140 Car Payment 389.12
24 1001160140 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
Privacy Policy | Security Statement | © 2006 Altoro Mutual, Inc.
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.
Internet
100%

Growth In Web Application Vulnerabilities

- Most prevalent type of vulnerability affecting servers today is vulnerabilies related to Web applications
- 54% of new vulnerability disclosures were Web application vulnerabilities

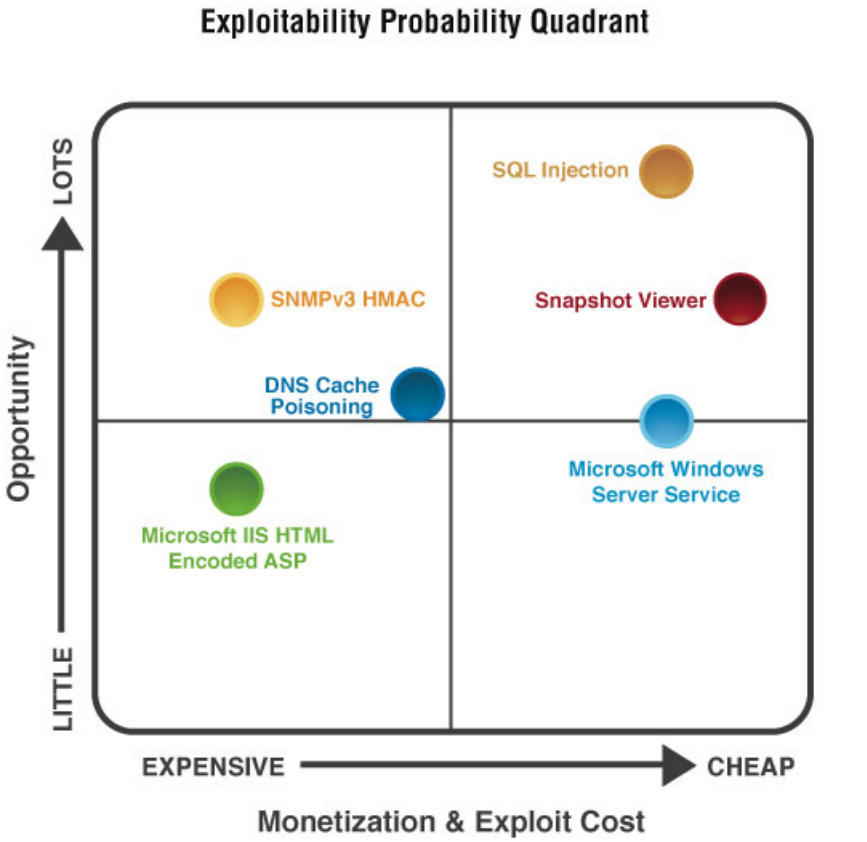


Motives Behind Application Hacking Incidents



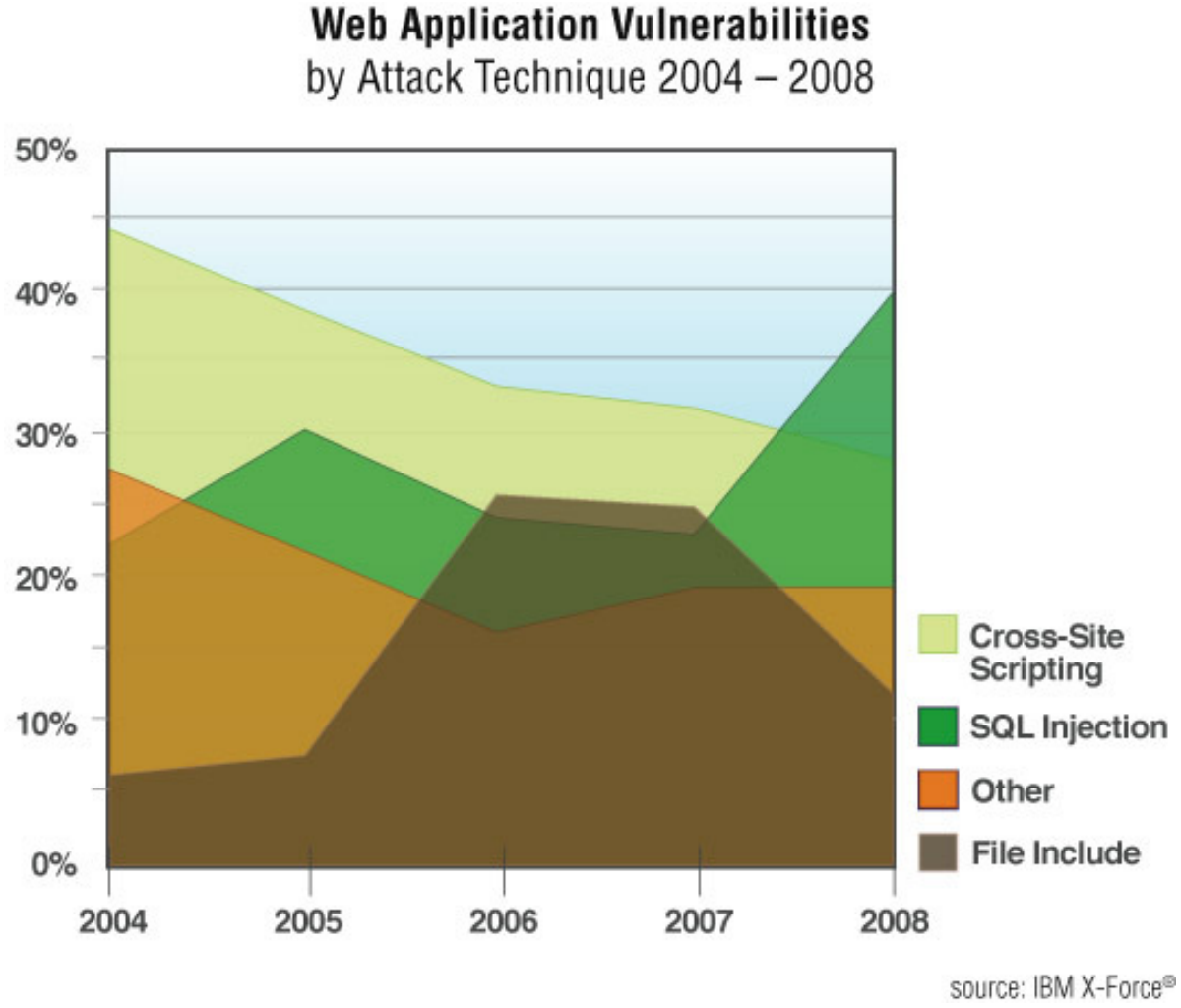
Monetization of Attacks

- No longer are amateur hackers taking joy-rides on corporate IS
- Today's hacker is sophisticated, likely part of organized crime, and is looking for financial reward for their efforts
- Vulnerability scoring systems fail to take into account economic opportunity when analyzing threats



source: IBM X-Force®

Mechanisms hackers use to attack Web applications



Where Do These Problems Exist?

Type:

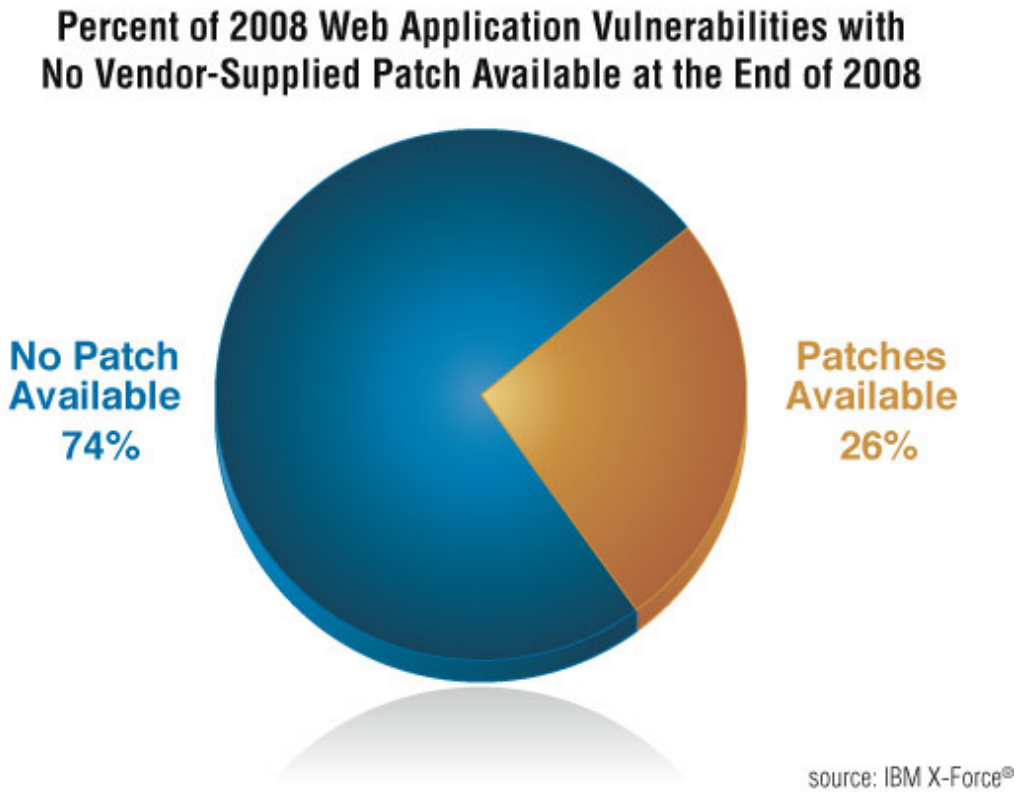
- Customer facing services
- Partner portals
- Employee intranets

Source:

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

No patch for you

- 74% of Web app vulnerabilities have no vendor-supplied patches
- This doesn't include custom developed applications which may never have had vulnerability testing performed against them



What is the Root Cause?

1. Developers not trained in security
   - Most computer science curricula have no security courses
   - Focus is on developing features
2. Under investment from security teams
   - Lack of tools, policies, process,
   - Lack of resources
3. Growth in complex, mission critical online applications
   - Online banking, commerce, Web 2.0, etc

Result: Application security incidents are on the rise

Axcess News
News for the X generation

USDA admits data breach, thousands of social security numbers revealed

THE WALL STREET JOURNAL.

BJ's Settles Case with FTC over Customer Data

Associated Press

Visa, Amex Cut Ties with CardSystems

IBM Internet Security Systems: X-Force® 2008 Mid-Year Trend Statistics, July 2008

Agenda

- Application Security Primer
- **Lowering the cost of compliance**
- Case Studies

Go to IBM

What is the cost of a fixing a vulnerability?

…same as the cost of a defect, with greater implications.

80% of development costs are spent **identifying and correcting defects**!

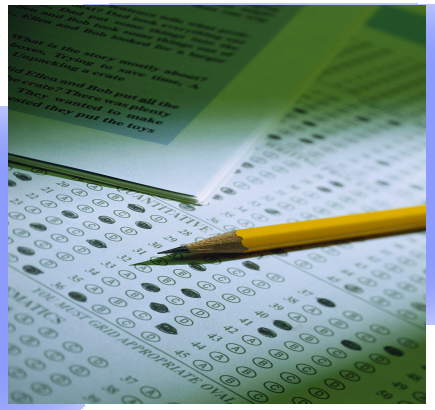
National Institute of Standards & Technology

During the coding phase

$25/defect

During the build phase

$100/defect



During the QA/Testing phase

$450/defect

Once released as a product

$16,000/defect

+

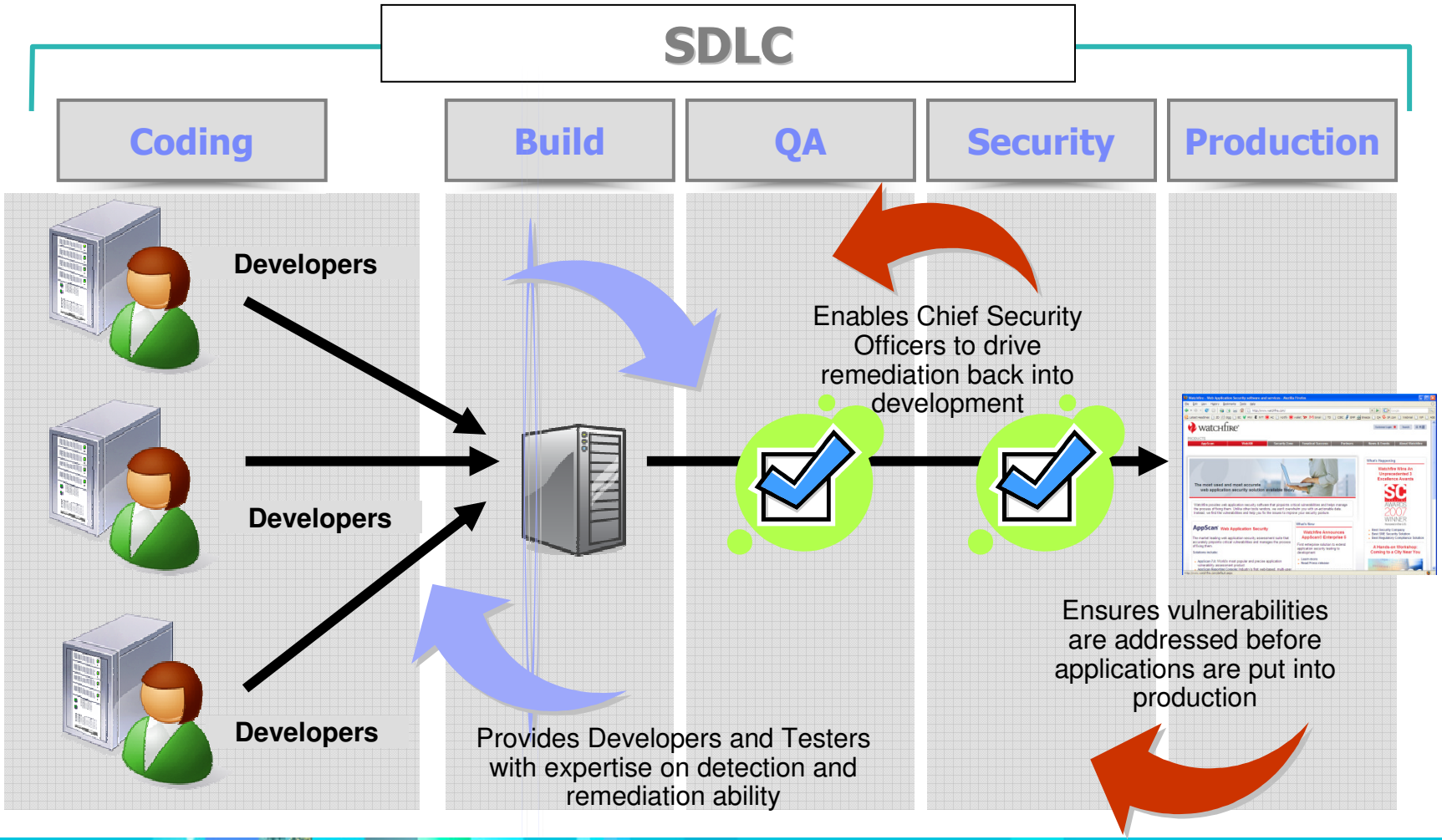
Law suits, loss of customer trust, damage to brand

The increasing costs of fixing a defect….

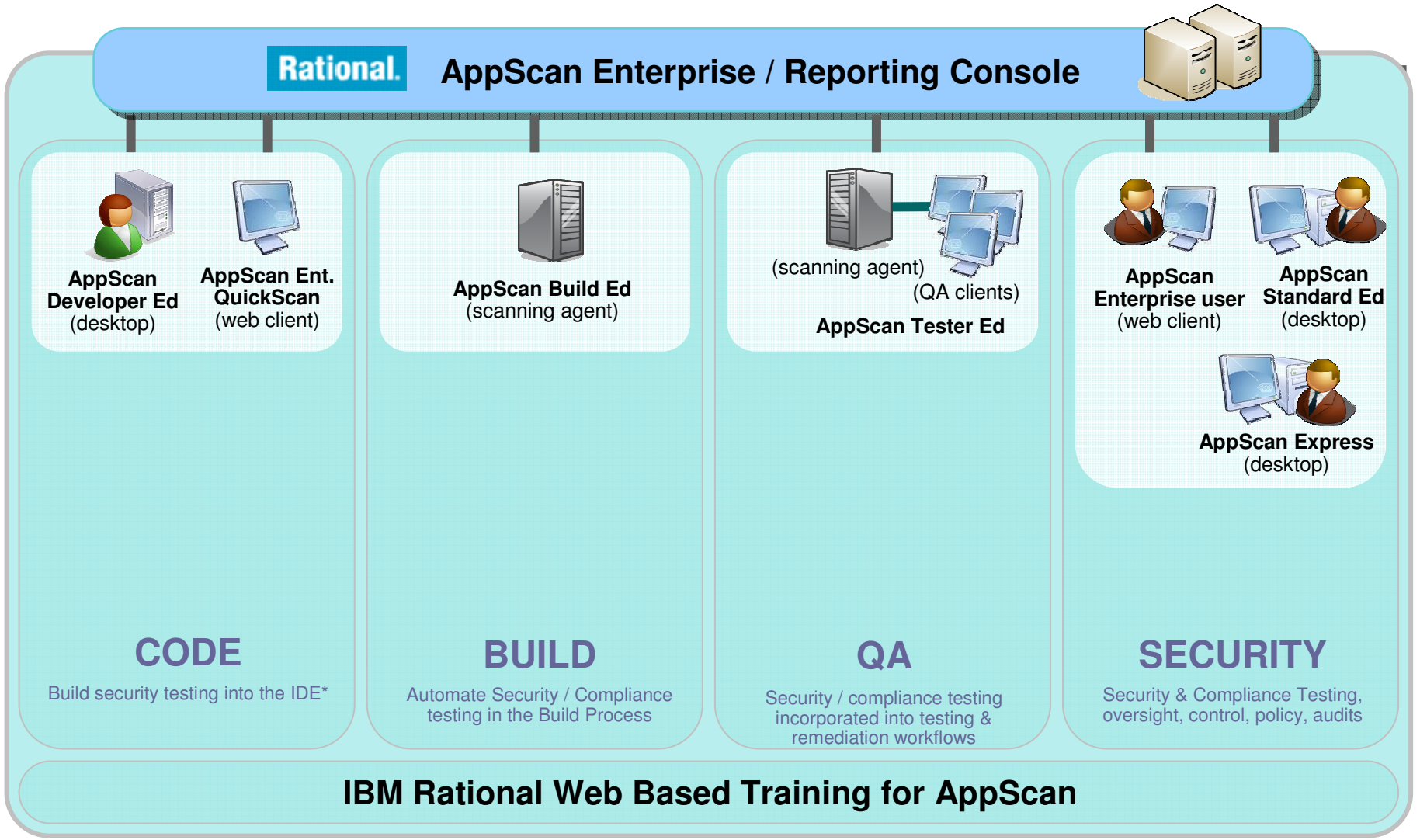
Caper Jones, Applied Software Measurement, 1996

Why Rational Security Analysis solution?

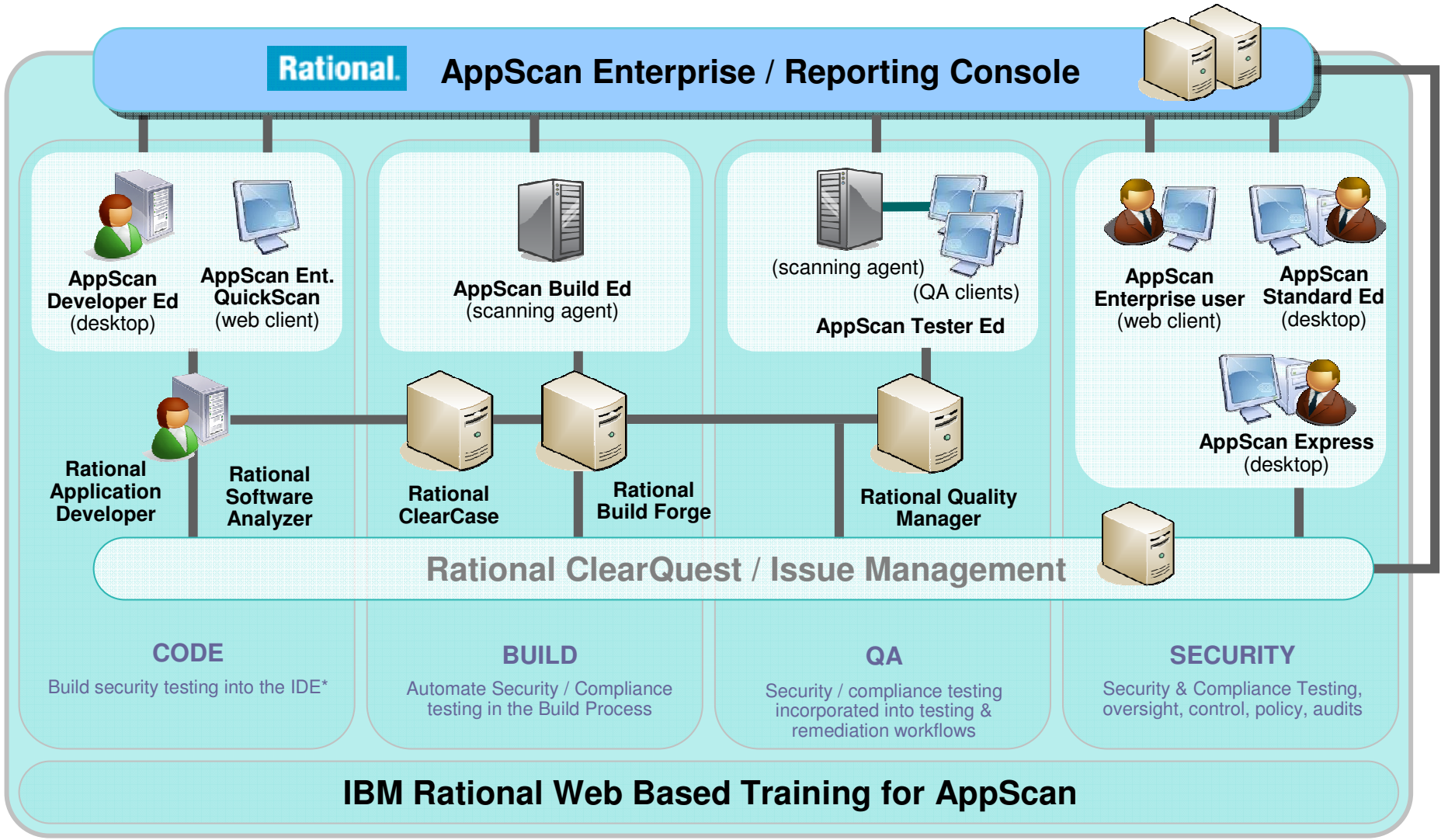
AppScan Enables the Detection & Remediation of Vulnerabilities across the entire SDLC.
Targetting code and build phases reduces cost of compliance



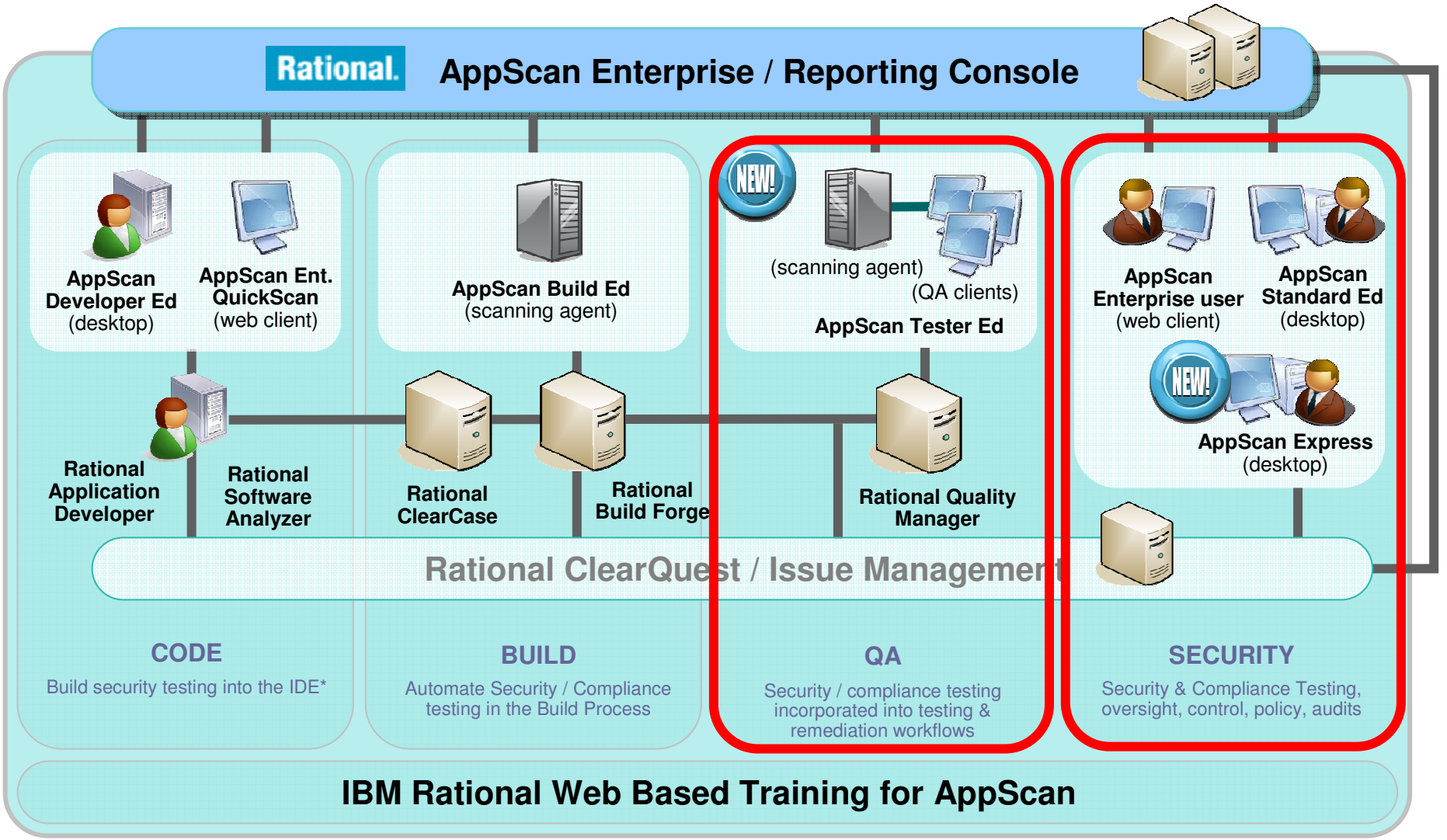
IBM Rational AppScan Offerings



IBM Rational AppScan Ecosystem

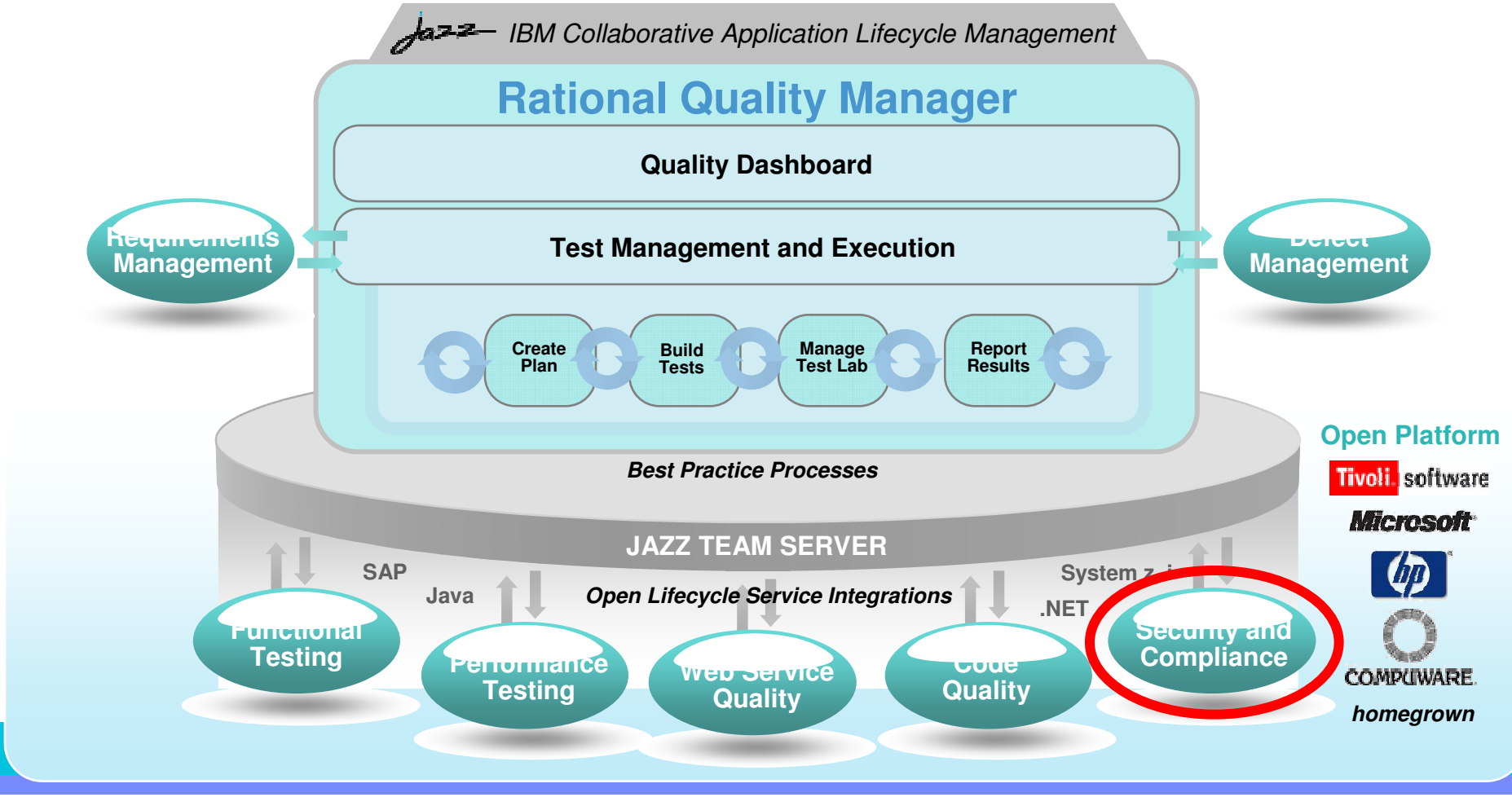


IBM Rational AppScan Ecosystem

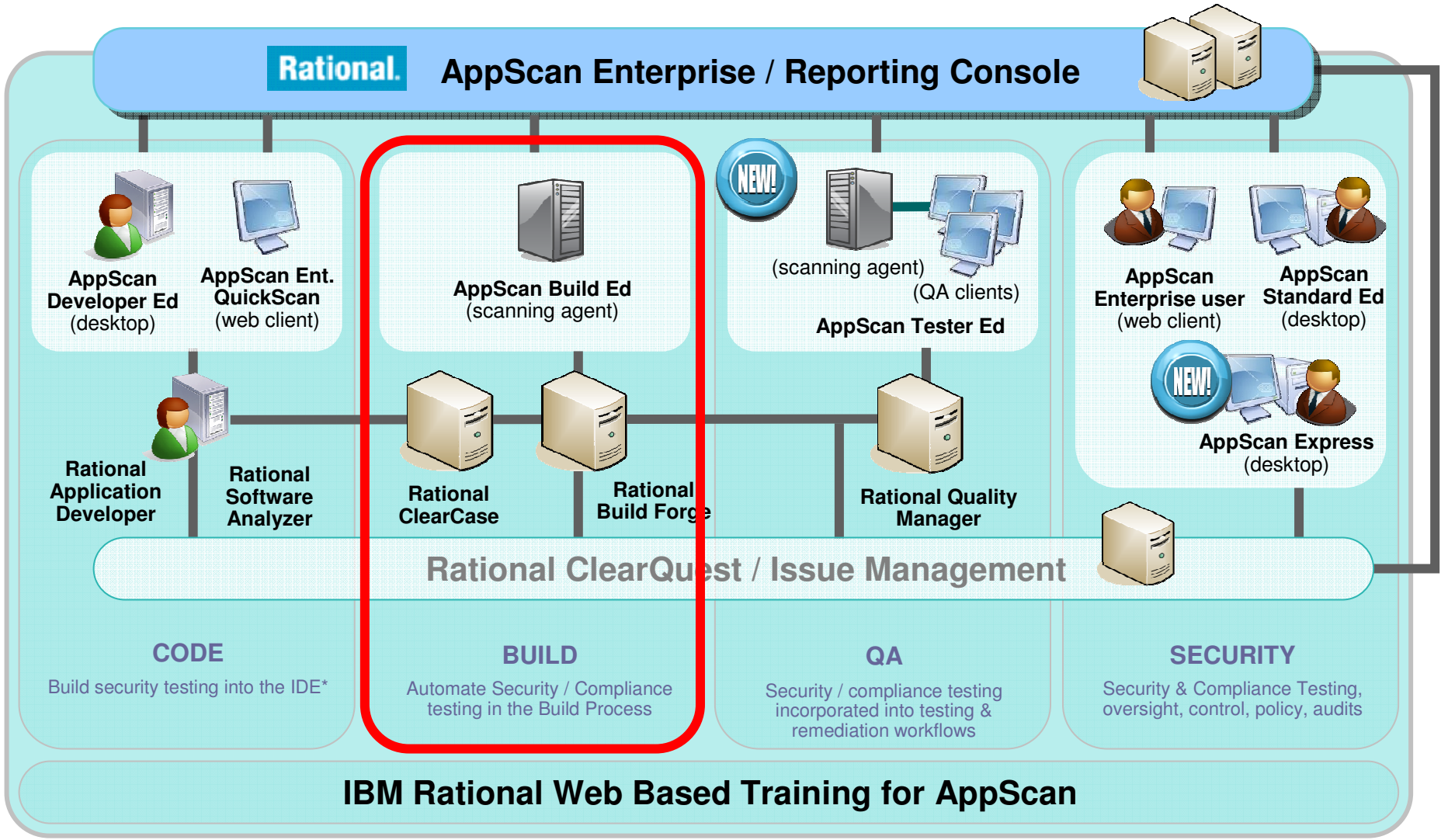


AppScan Tester Edition for RQM

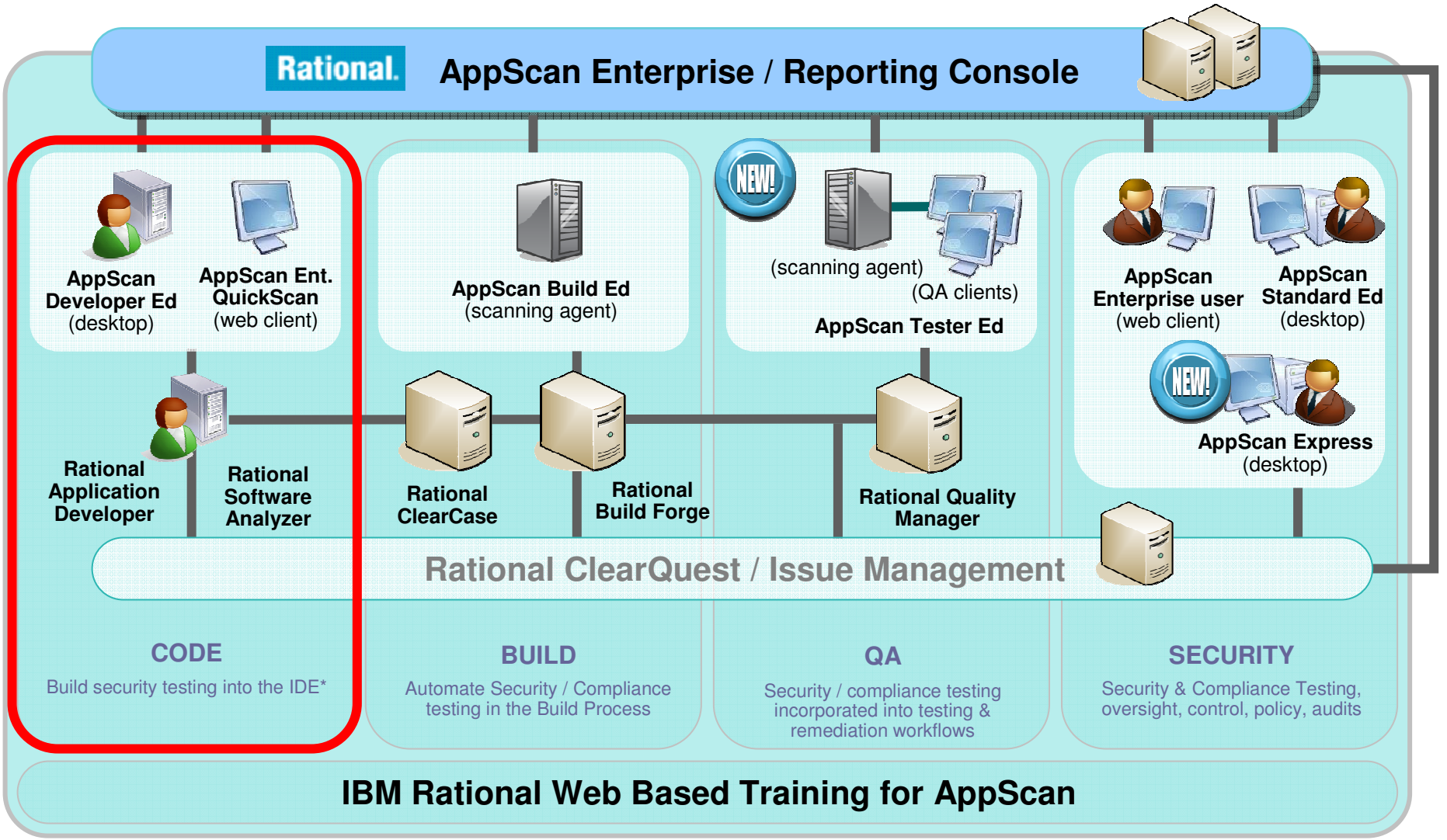
- Seamless integration of security testing into Rational Quality Manager (RQM)
- Embedded into the QA environment to allow full management of security testing in the same process flow as functional, performance and services testing



IBM Rational AppScan Ecosystem



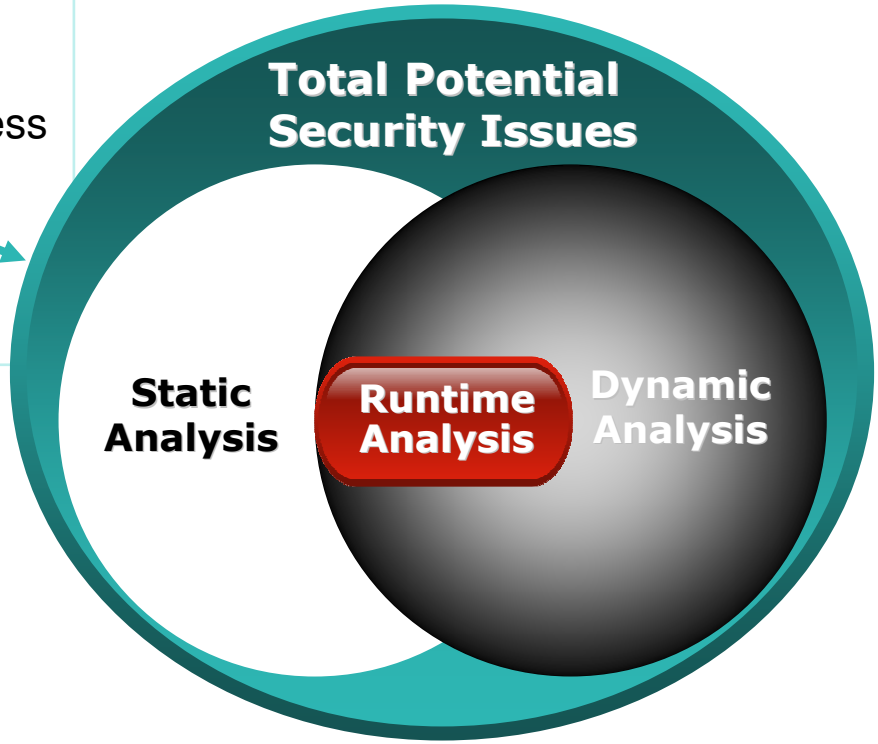
IBM Rational AppScan Ecosystem



Security In Development: **Code Offerings & Integration**

Rational AppScan Developer Edition Themes

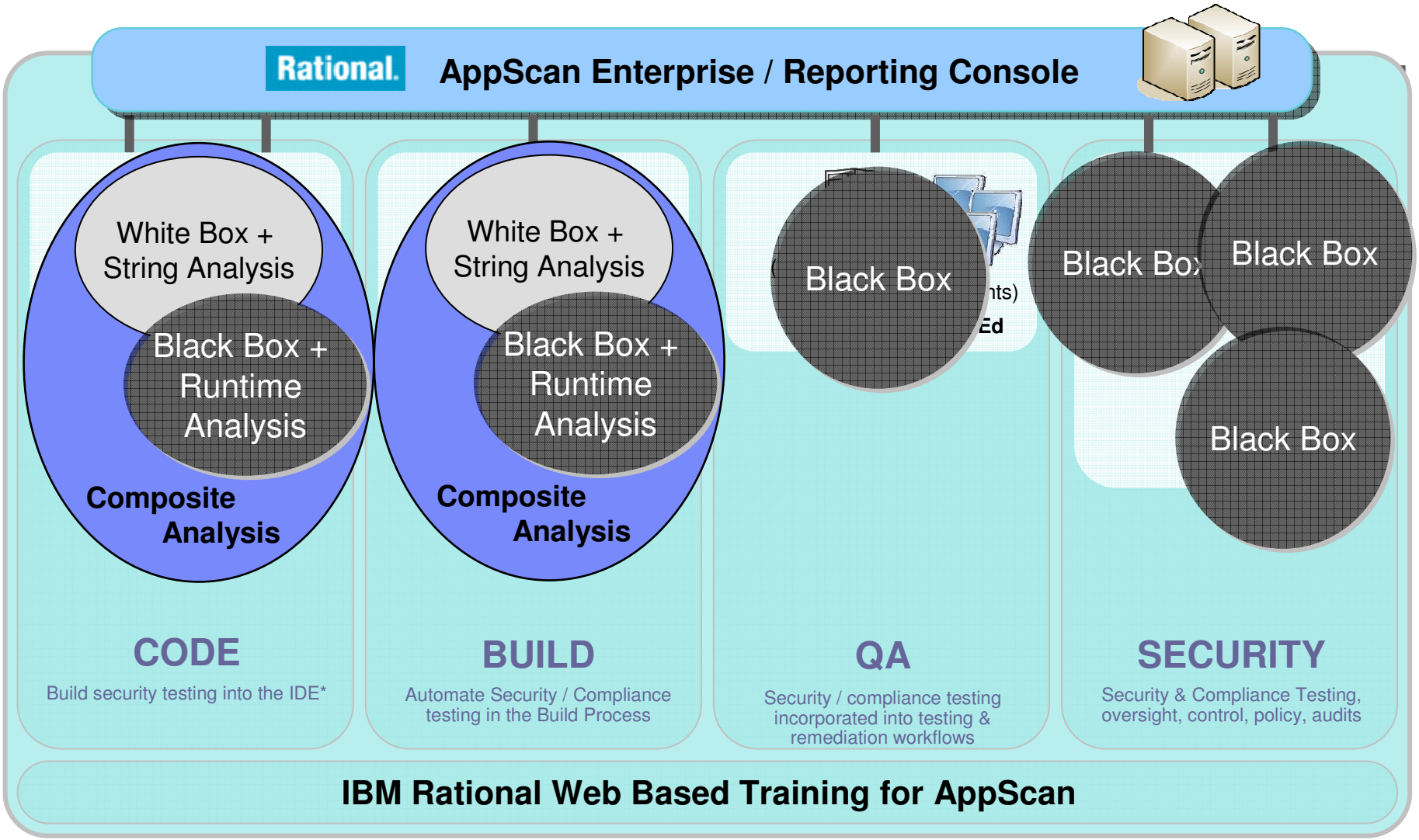
- Designed for Developers, not Security Auditors
- Self-Serve – No Security Expertise Required
- Natural fit into the Development Lifecycle Process & Tools
- The only holistic Security Solution in the marketplace



Business Outcome

- **Enable more people** to contribute to security testing coverage with solutions for specific use cases
- Use case offerings **facilitate the adoption of security with minimal disruption** to existing objectives

IBM Rational AppScan Ecosystem



IBM Software Group

AppScan OnDemand

Go to IBM

Rational SaaS – AppScan on Demand

- **Perfect for new Web Application Security & Compliance Initiatives**
  - Ideal for companies who don't write their own code, purchase packaged applications or outsource development

Proven Results

- Leverages industry-leading AppScan Suite of Tools
- Outsourced to highly experienced team of product experts who:
- Work cross-industry, share learnings
- Maximize product capabilities on the customers' behalf

Economic Benefits

- Low startup costs, no Capital Expenditure (subscription)
- Fast time-to-value
- Lower ongoing Total Cost of Ownership (TCO) vs. licensed solutions
- Increases efficiency of IT organizations

Ideal for Compliance

- **Simplifies and Centralizes compliance scanning**
- Auditable system of record
- Automates management and compliance of Web content

- **Execute with reduced business risk and cost**

Introducing expanded Rational AppScan OnDemand

- **Web application & service automated security testing**
  - **AppScan OnDemand:**
    - Comprehensive testing of pre-production applications
    - Periodic assessment of applications in QA or Security
    - Monthly scans
    - Flexible offerings based on organization (Small/Medium/Large)

  - **AppScan OnDemand Production Site Monitoring:**
    - Continuous scanning of production Web sites for vulnerabilities that may have been introduced after the app went live
    - Dynamic or interactive content and forms, online registrations
    - Weekly scans

The Result: Reduce online cost and risk without in-house resources with the fastest route to actionable information

Agenda

- Application Security Primer
- Lowering the cost of compliance
- **Case Studies**

Go to IBM

Case Study: A Federal Government Department

- Customer Pains
- **Serious breaches of key website including defacement**
- **No consistent approach to security testing**

- Outcome
  - Deployed Rational AppScan Enterprise in various ways:
    - Hosted and managed by sub-department
    - Hosted by sub-department, managed by IBM
    - Hosted and managed by IBM (SaaS model)
  - Creating Standard Operating Procedures to use product in consistent way across sub-departments
    - On-site training
    - Web-based training
    - Documented processes
    - Developers trained on secure code practices

- Phase 1: Scan all production applications
  - Deploy AppScan Enterprise to each sub-department
  - Configure to look for critical issues (SQL Injection, Cross-site scripting

- Phase 2: Testing in pre-production
  - Implemented a gating process
  - Zero high vulnerabilities in order to go live

- Phase 3: Deploy to QA
  - Enable QA team to implement security testing during development cycles

Case Study: A Federal Government Department

- Challenges
  - Myriad products already being used
  - Lack of Executive champions
  - Outsourced application development and hosting

- Competitive products
  - Demonstrate capabilities
  - Achieve early success to build credibility

- Executive Champions
  - Identify evangelists
  - Carry a big stick

- Outsourced Development
  - Security testing becomes part of User Acceptance testing
  - Include security specifications in contracts

Case Study: A Networking Company

- Customer Pains
- **Small, niche security team had become a bottleneck to the 2,000+ development organization**
- **Web applications portfolio estimated at 2,500 applications – about 425 applications changed yearly**
- **Had an experienced application team using AppScan, but needed a way to scale and involve many more testers in the process**

- Outcome
  - Deployed Rational AppScan Enterprise, providing access to **ALL** developers to test applications and address security issues before being pushed downstream
    - Essential to abstract security complexities and maintain efficient development timelines
    - Ensured security team could manage project, configure scans and control access to vulnerability data
  - Web-based training was a key component to project success
    - Developers trained on secure code practices
    - Custom training created to facilitate adoption

"We are completely dependent on development teams to deliver vulnerability-free code."
--Vice President, IT Security