IBM Software Partner Academy Program

Telefonkonferenz am 24.07.09

„Sicherheit von Webanwendungen mit Rational AppScan“

Thomas Neudert (*Product Sales Specialist – Rational)*

Rückblick in das Jahr 1989: „Yankee Doodle“

Computervirus: Mit der Bezeichnung „Yankee Doodle“ wurde ein Computervirus benannt, das im September 1989 erstmals isoliert wurde. Es handelt sich um ein speicherresidentes MS-DOS-Virus, das täglich um 17 Uhr den Refrain des Yankee-Doodle-Liedes über den Systemlautsprecher abspielt.[1]

Der Mythos “Wir sind sicher”

Wir haben Firewalls

Wir lassen jedes Jahr ein Audit durchführen

Wir haben SSL Verschlüsselung

Wir haben Netzwerk-Scanner

Die Realität sieht ander aus, politischer und wirtschaftlicher Schaden:

Website von Bundesinnenminister Schäuble gehackt
Die offizielle Internet-Präsenz von Bundesinnenminister Wolfgang Schäuble ist am heutigen Samstag gehackt worden.

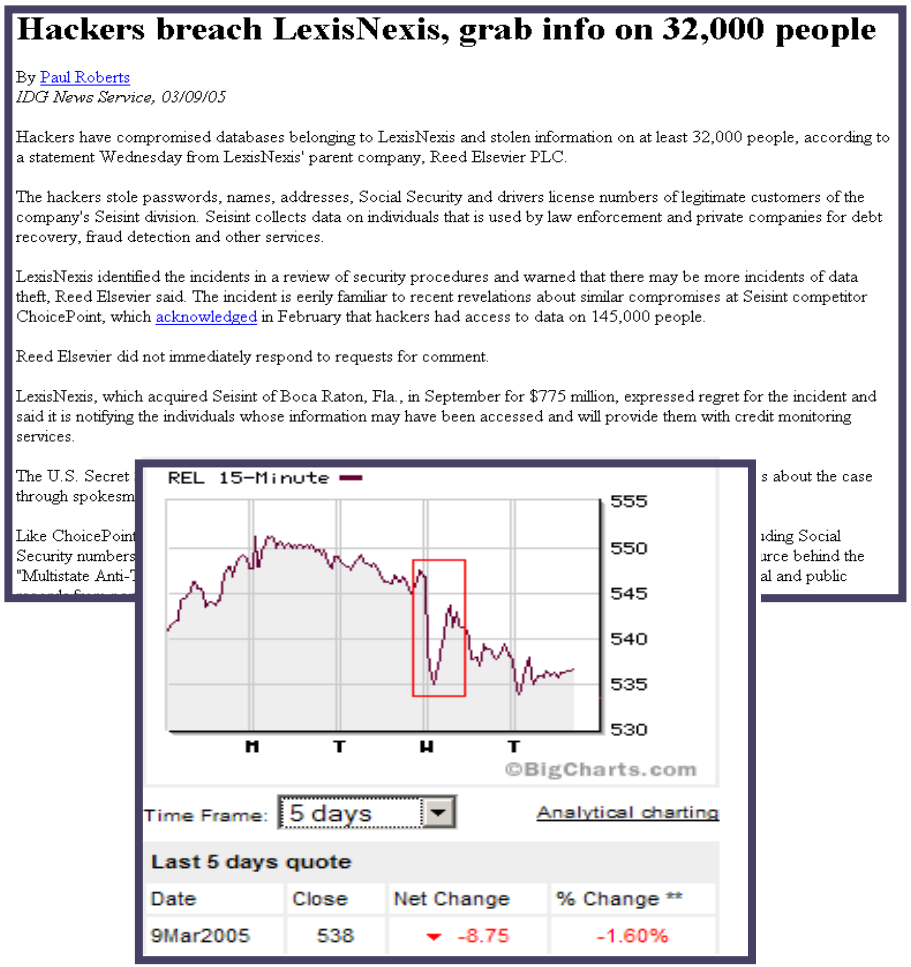
Daten von tausenden Studenten der Uni Magdeburg im Netz
Daten von rund 44.000 Studenten der Universität waren im Netz frei zugänglich. Inzwischen seien sie wieder entfernt worden, meldete jetzt die Universität.

Schleswig-Holstein: Betriebe von Computerkriminalität betroffen
… 39 Prozent der befragten Betriebe gaben an, innerhalb der vergangenen sechs Monate einmal oder mehrfach angegriffen worden zu sein …

Bank haftet für Schäden durch Phishing-Attacke
… haftet eine Bank für die einem Kunden durch einem Phishing-Angriff entstehenden Schäden …

Lücke in Überwachungssoftware für industrielle Anlagen
Möglicherweise kann ein Angreifer dadurch auch in ein verwundbares System eindringen.

Die Kosten fehlender Sicherheitslösungen



Hackers breach LexisNexis, grab info on 32,000 people

By Paul Roberts
IDG News Service, 03/09/05

Hackers have compromised databases belonging to LexisNexis and stolen information on at least 32,000 people, according to a statement Wednesday from LexisNexis' parent company, Reed Elsevier PLC.

The hackers stole passwords, names, addresses, Social Security and drivers license numbers of legitimate customers of the company's Seisint division. Seisint collects data on individuals that is used by law enforcement and private companies for debt recovery, fraud detection and other services.

LexisNexis identified the incidents in a review of security procedures and warned that there may be more incidents of data theft, Reed Elsevier said. The incident is eerily familiar to recent revelations about similar compromises at Seisint competitor ChoicePoint, which acknowledged in February that hackers had access to data on 145,000 people.

Reed Elsevier did not immediately respond to requests for comment.

LexisNexis, which acquired Seisint of Boca Raton, Fla., in September for $775 million, expressed regret for the incident and said it is notifying the individuals whose information may have been accessed and will provide them with credit monitoring services.

The U.S. Secret ... s about the case through spokesm...

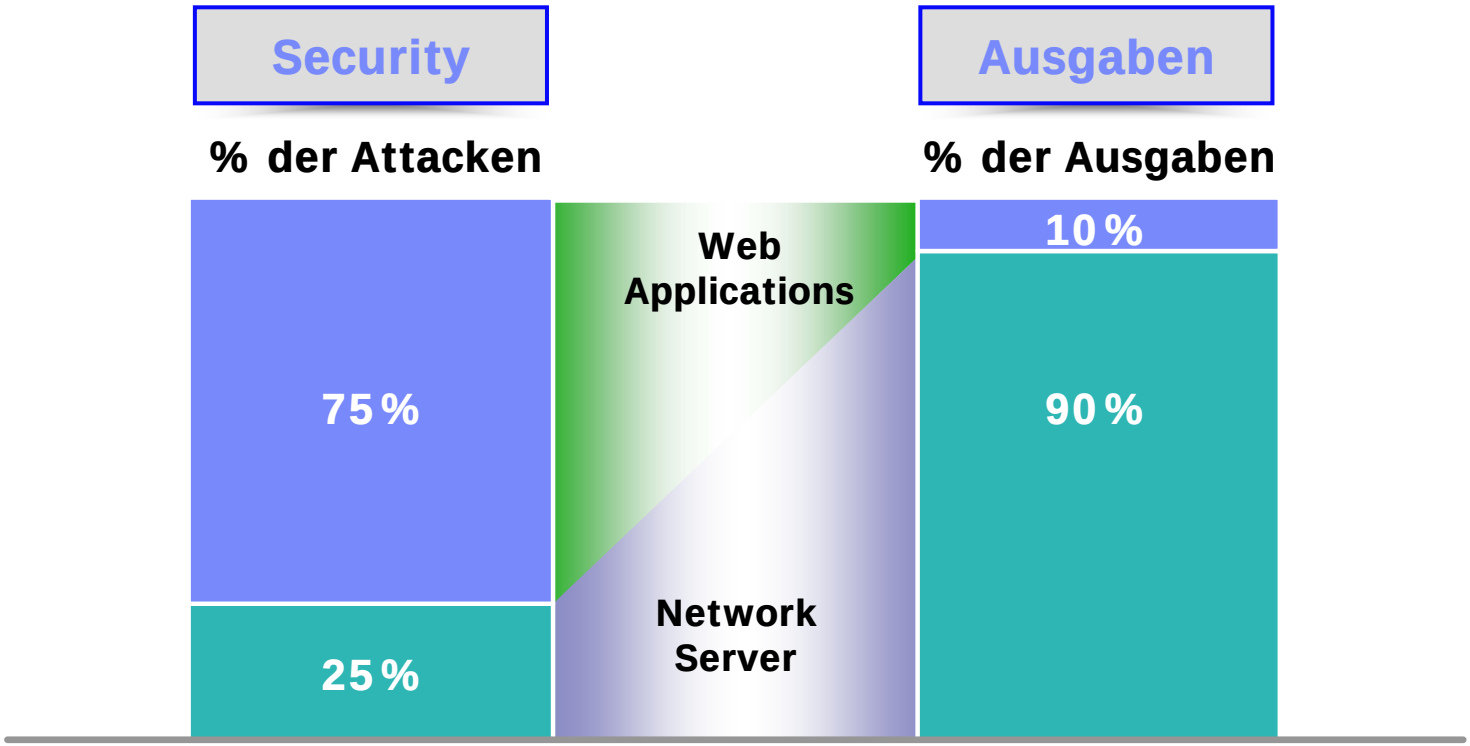
Like ChoicePoint ... uding Social Security numbers ... urce behind the "Multistate Anti-T... al and public ...

- **Mediale Aufmerksamkeit**
- Beschädigung der Marke
- Stark sinkende Aktienkurse
- **Hohe Kommunikationskosten**
- Gesetzliche Strafen
- **Verstärkte Audits**
- Klagewelle von Kunden
- **Verlust von Kunden**.

Warum ist “Application Security” so wichtig?

- **Web Applikationen stehen an erster Stelle der Hacker Attacken**
  - 75% aller Attacken betreffen die Applikationsschicht (Gartner)
  - “XSS” und “SQL Injection” stehen an erster und zweiter Stelle der Attacken
- **Die meisten Webseiten sind angreifbar**
  - 90% aller Webseiten sind angreifbar durch Applikations-Attacken (Watchfire)
  - 78% der einfach anwendbaren Attacken betreffen Web Applikationen (Symantec)
  - 80% aller Unternehmen werden bis 2010 mit Sicherheitsvorfällen konfrontiert werden (Gartner)
- **Web Applikationen sind für Hacker höchst interessant**
  - Zugriff auf persönliche Daten, Kundendaten, Unternehmensdaten, Kreditkarten usw.
- **Compliance Anforderungen werden verletzt**
  - Basel II, Datenschutzgesetze, SOX, Payment Card Industry (PCI) Standards, GLBA, HIPPA, FISMA.

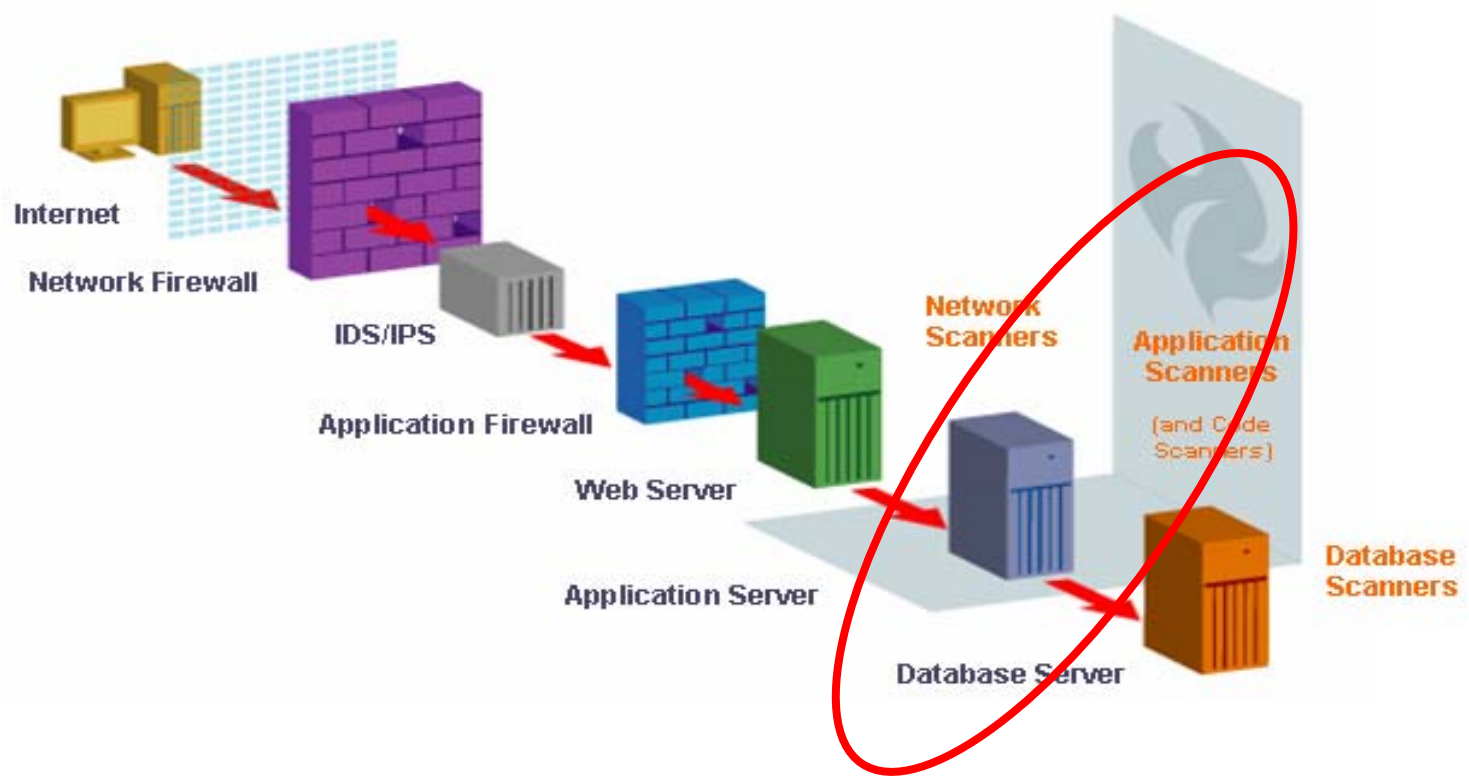
Ausgabenverteilung für Security



75% aller Attacken auf Informationssicherheit finden im Web Application Layer statt

2/3 aller Web Applicationen sind gefährdet. Gartner

Einordnung der „Web Application Security“



Web Application Security – Lösungsansätze

Sicherheit

z.B. AppScan Enterprise Ed

- Vollständige SDLC Intergration durch Einbindung der Entwicklunsabteilung.

Strategisch

Sichtbarkeit

z. B. Reporting Console

- Konsolidierung der internen Audits und Verteilung der Berichte zur Entwicklungs-abteilung und der Geschäftsführung

Operative Einbindung

Interne Audits

z.B. AppScan Standard Ed

- Aufbau interner Sicherheits- und Audit Teams welche selbständig mithilfe einer Scan SW Application Scans durchführt

Reaktion auf Schwachstellen

ausgelagerte Audits

Web App Penetration Tests

- Applikatinen werden erstmalig auf Schwachstellen analysiert
- Penetration-Testing durch Extern.

Keine / zu wenig Beachtung

Höhe der Fehlerkosten

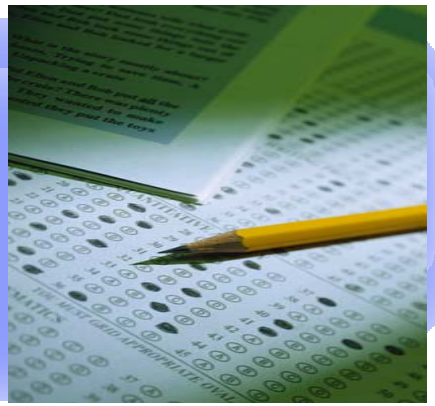
80% der Entwicklungskosten werden für das identifizieren und beseitigen von Schwachstellen ausgegeben!

während der Entwicklung

EUR 25 pro Fehler

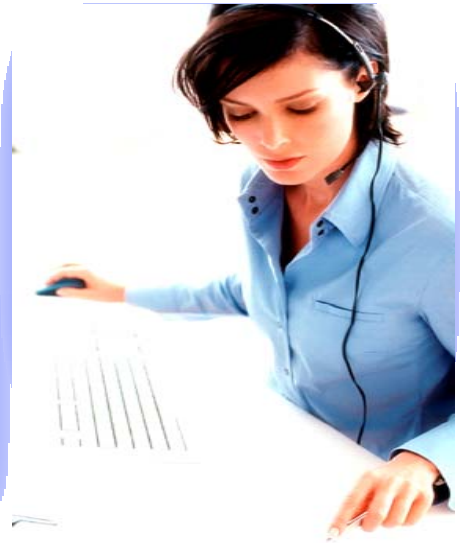
beim Zusammenbau

EUR 100 pro Fehler



während der Testphase

EUR 500 pro Fehler



nach Veröffentlichung

EUR 15,000 pro Fehler

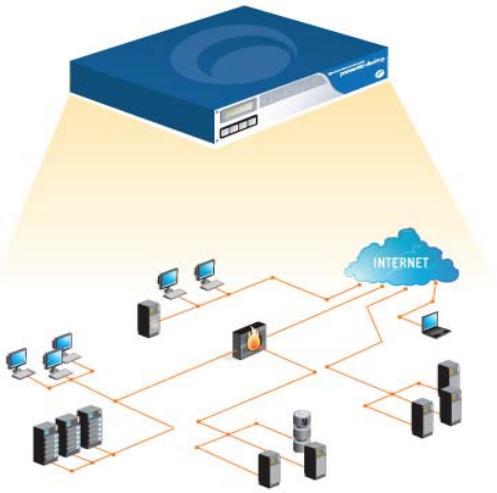
je später ein Fehler beseitigt wird, umso teurer wird es

Was macht ein Webapplication Scanner?

Automatisiertes Testen von Web Applikationen auf Sicherheitsschwachstellen

1

Analyse der Struktur und Komplexität der Web Site / Applikation



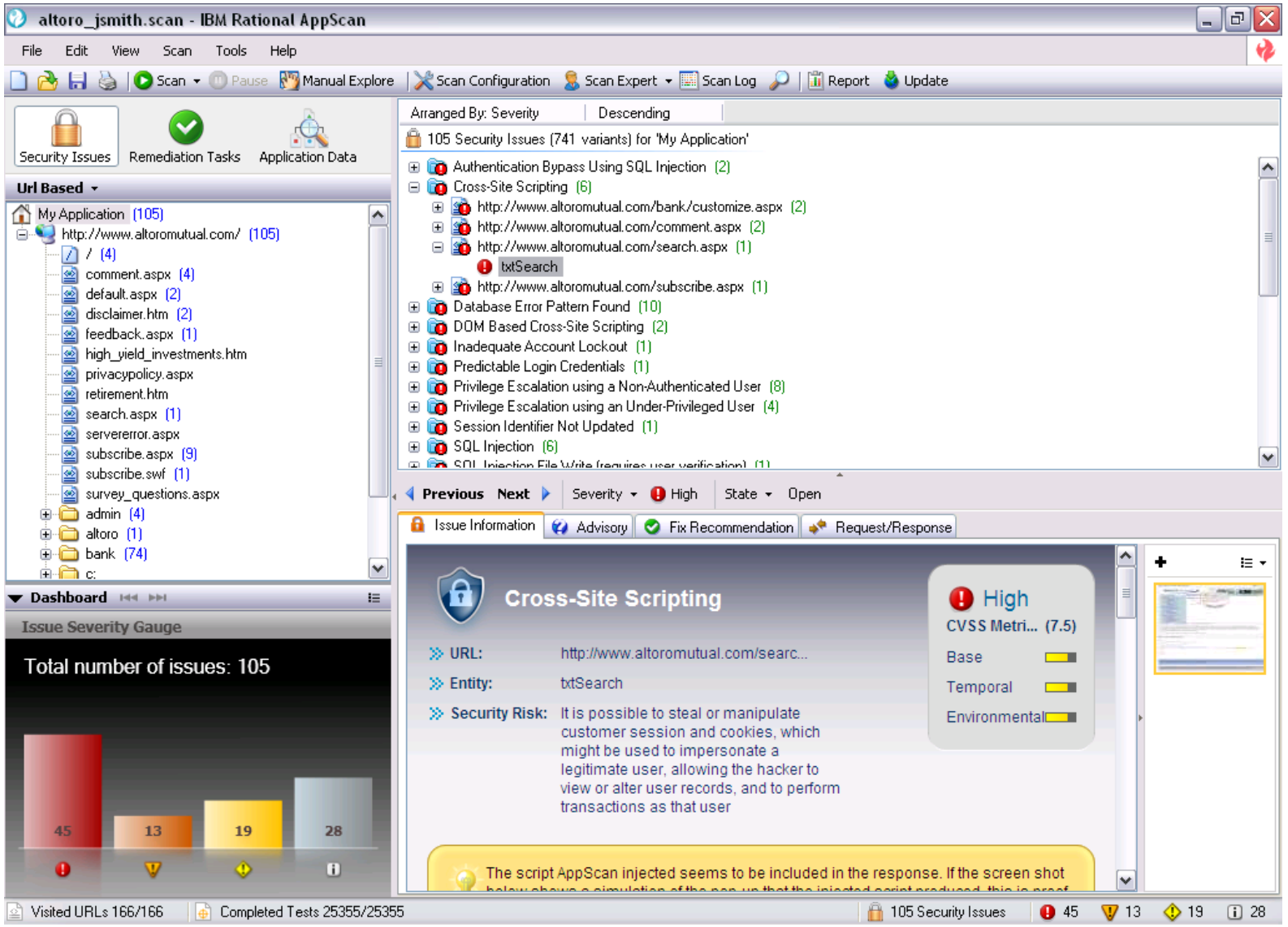
2

Identifizierung der Sicherheits-Schwachstellen, Berichtserstellung priorisiert nach Relevanz.

3

Konkrete Lösungsvorschläge und weiterführende Unterstüzung. Nachverfolgung und Compliance Unterstüzung

Beispiel eines Scans



Security / Herausforderungen

- Starker Ausbau der Webangebote und -services
- Einbindung neuer webbasierter Workflows
- Schnellere Anpassungszyklen der Applikationen
- Sichere Interne sowie Externe Webentwicklung
- Interne Kommunikationsaufwände
  Bereichsübergreifende Prozesse von Entwicklung und Sicherheit
- Nachverfolgung von Fehlerbehebungen
- Qualitätssicherung der Applikationsentwicklung (extern Güteprüfung)

KOSTEN & RESOURCEN

Woher kommt AppScan? Was ist Watchfire?

watchfire®
an IBM company

#1 in Market Share for Application Security
– Gartner & IDC

- 1996: Watchfire Gründung in Boston
- Entwicklung der Applikation Security Lösung (**AppScan + Web XM**)
- 2006: Gartner Marktführer in “Application Security 2006”
- 2007: SC Magazine Award als “Best Security Company”
- Mehr als 800 Referenzen
- 2007: Akquisition durch IBM
- IBM Rational AppScan + Rational Policy Tester

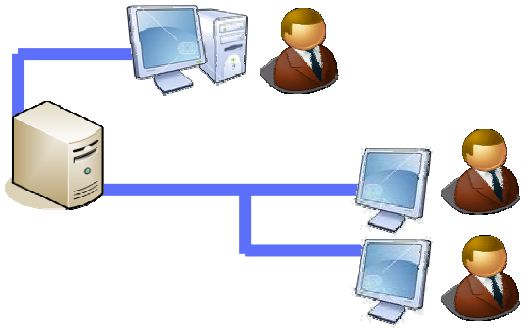
SC MAGAZINE AWARDS 2007 WINNER

AppScan Versionen (Black Box)

Appscan Standard Edition (Desktop)

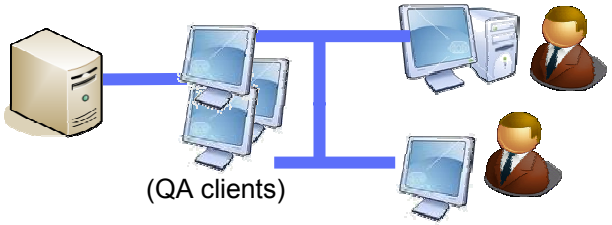
- Desktop basiertes Scanning
→ **Einstiegslösung**

+



Appscan Reporting Console (Server/Client)

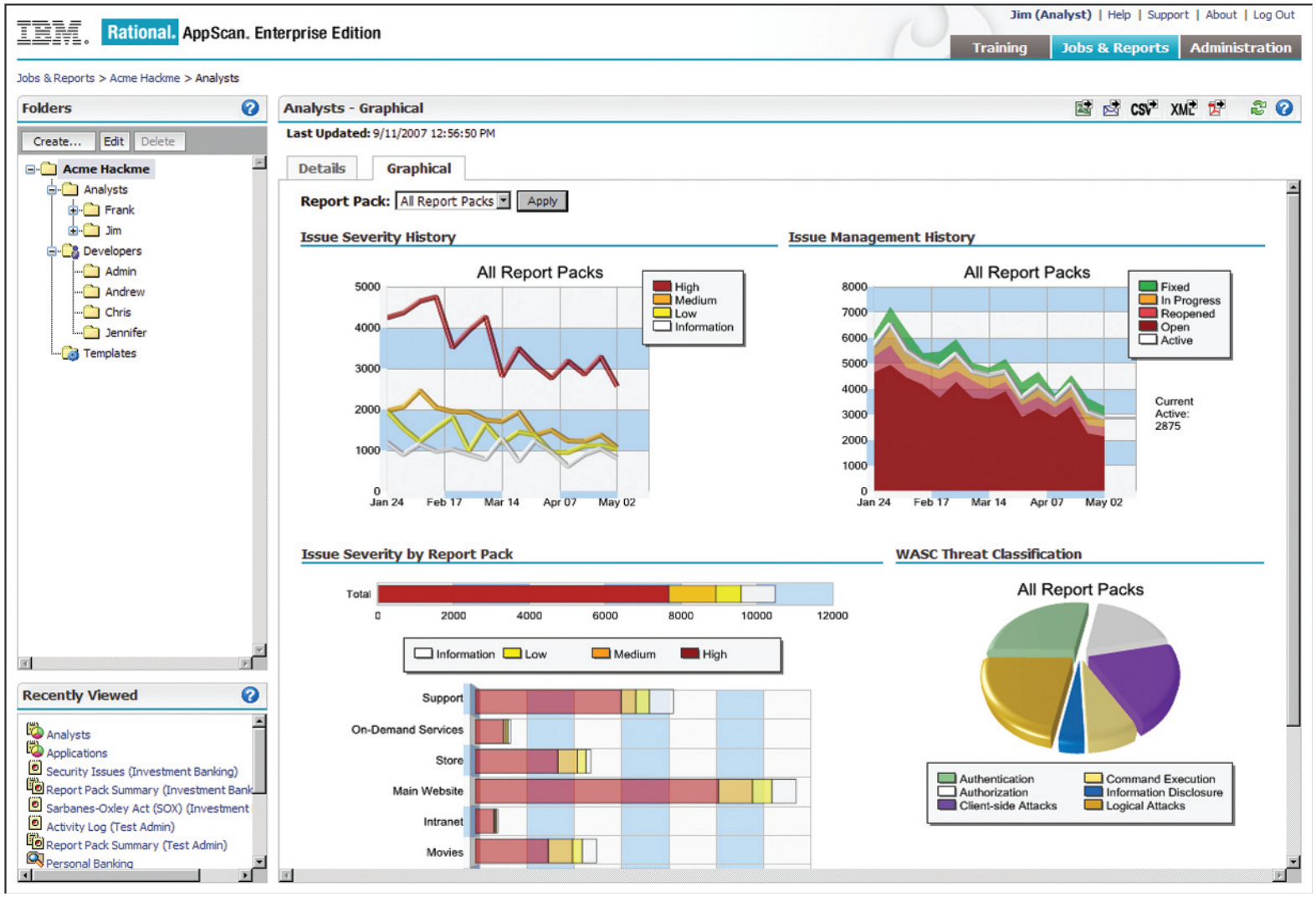
- Server & Rollen basierender SICHERER Austausch der Reports und Analyseergebnisse



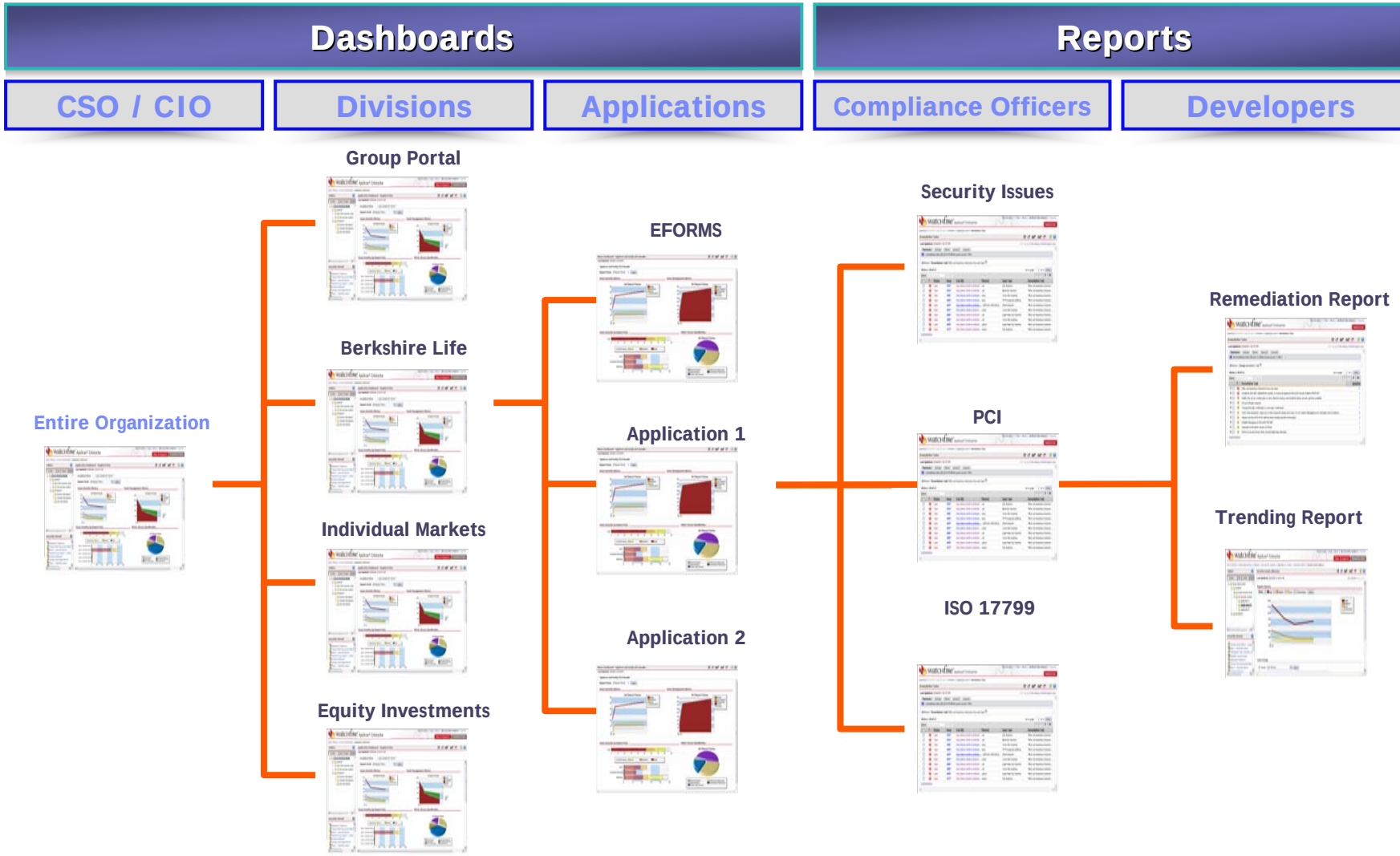
Appscan Enterprise Version (Server/Client)

- Server basiertes Scanning im gesamten SDLC / zentrale Steuerung, Workflow, Web-based

Beispiel Management Dashboards



Sichtbarkeit im gesamten Unternehmen



AppScan Einstiegslösung - Listpreise

AppScan Standard Edition		AppScan Express Edition	
Floating User 		**Authorized User** 	
User Licence	31.394	User Licence	17.387
Renewal	6.279	Renewal	3.477
oder			
„**Consulting Licence**“	27.627	entspricht Rabattstufe D	
Renewal	5.525	der Standard Edition	

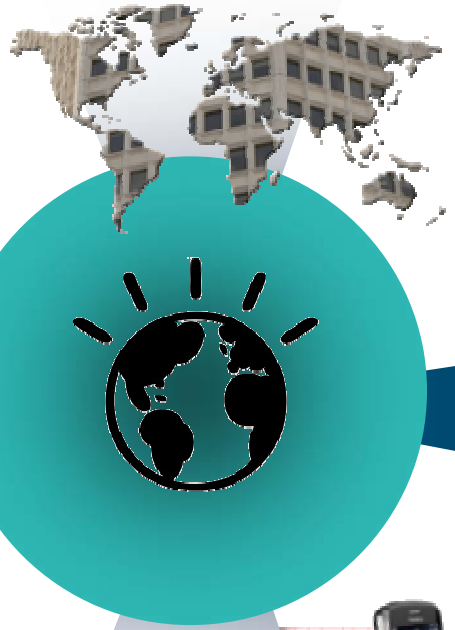
Was heißt „Ganzheitliche Sicherheit“ ?

- Markt und Trends
- Risiko kennen und managen
- Komplexität beherrschen
- Praktische Erfahrungen

Entdecke die Welt neuer Möglickeiten

Globalisierung schafft Zugang zu weltweiten Ressourcen

Milliarden mobile Geräte bekommen Zugang zum World Wide Web



Zugang zu Informationen ohne zeitliche Verzögerung

Neue Formen der Zusammenarbeit

Neue Möglichkeiten

Neue Komplexität

Neue Risiken

Gesamtheitliche Bewertung von Risiken

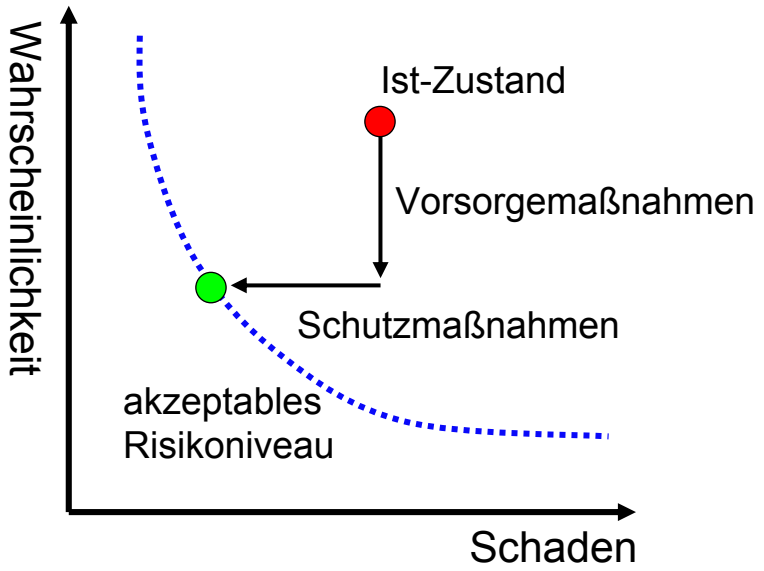
Interne Verfahren	Systeme	Menschen		Externe Ereignisse	
		Mitarbeiter	Externe	Direktes Umfeld	Katastrophen
▪ Falsche Strategie ▪ Fehlende Zielausrichtung ▪ Unklare Verantwortlichkeiten ▪ Schlechte Prozessdefinition und -umsetzung ▪ Mangelnde Anpassungsfähigkeit an neue Anforderungen	▪ Hardwaredefekte ▪ Softwarefehler ▪ Schlechte Administration ▪ Mangelhafte Benutzerfreundlichkeit ▪ Anfälligkeit gegen Würmer und Viren ▪ Inadäquate Architekturen ▪ Stromausfall	▪ Missbrauch ▪ Diebstahl ▪ Unachtsamkeit, Unwissenheit ▪ Menschliches Versagen ▪ Bestechung ▪ Fluktuation	▪ Computerviren und Würmer ▪ Hacking ▪ Einbruch ▪ Betrug ▪ Vandalismus ▪ Raub, Diebstahl ▪ Sabotage ▪ Spionage ▪ Terrorismus	▪ Ausfall der Kommunikationsverbindungen (Telefon, Mail, Web) ▪ Änderung der regulatorischen Anforderungen ▪ Verlust der Verkehrsverbindungen ▪ Extreme Nachfrageschwankungen	▪ Erdbeben ▪ Hochwasser ▪ Sturm ▪ Frost ▪ Feuer ▪ Explosion ▪ Chemieunfälle ▪ Flugzeugabsturz, Verkehrsunfälle ▪ Krieg

Externe Risikoquellen

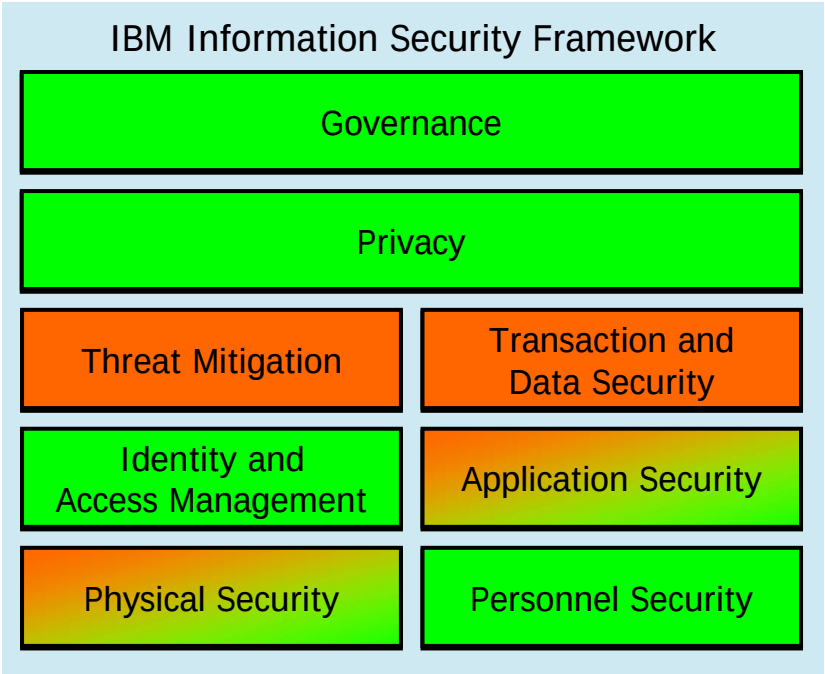
Interne Risikoquellen

Ganzheitliches Vorgehen

- Der aktuelle Risikozustand muss ermittelt werden und bekannt sein.
  - Das akzeptable Risikoniveau ist individuell für jedes Unternehmen abhängig von den geschäftlichen Aktivitäten und Werten.
  - Durch Planung der richtigen Maßnahmen soll das aktuelle Risiko verringert werden.
- **Vorsorgemaßnahmen** verringern die Wahrscheinlichkeit, dass Risiken eintreten
- **Schutzmaßnahmen** verringern den möglichen Schaden.
- Aufgrund der Dynamik von Gefährdungslage und Unternehmenswerten wird das Risiko kontinuierlich in einem **Regelkreis** gesteuert.
- Hundertprozentige Sicherheit kann nicht erreicht werden, ein Restrisiko muss akzeptiert werden.



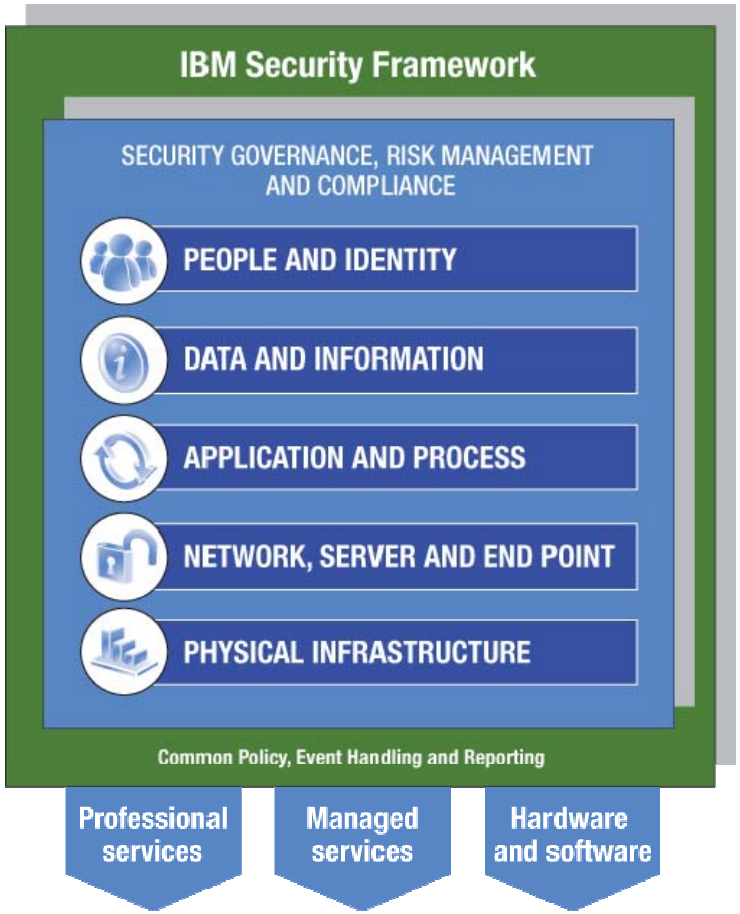
Rahmenwerk der Sicherheit



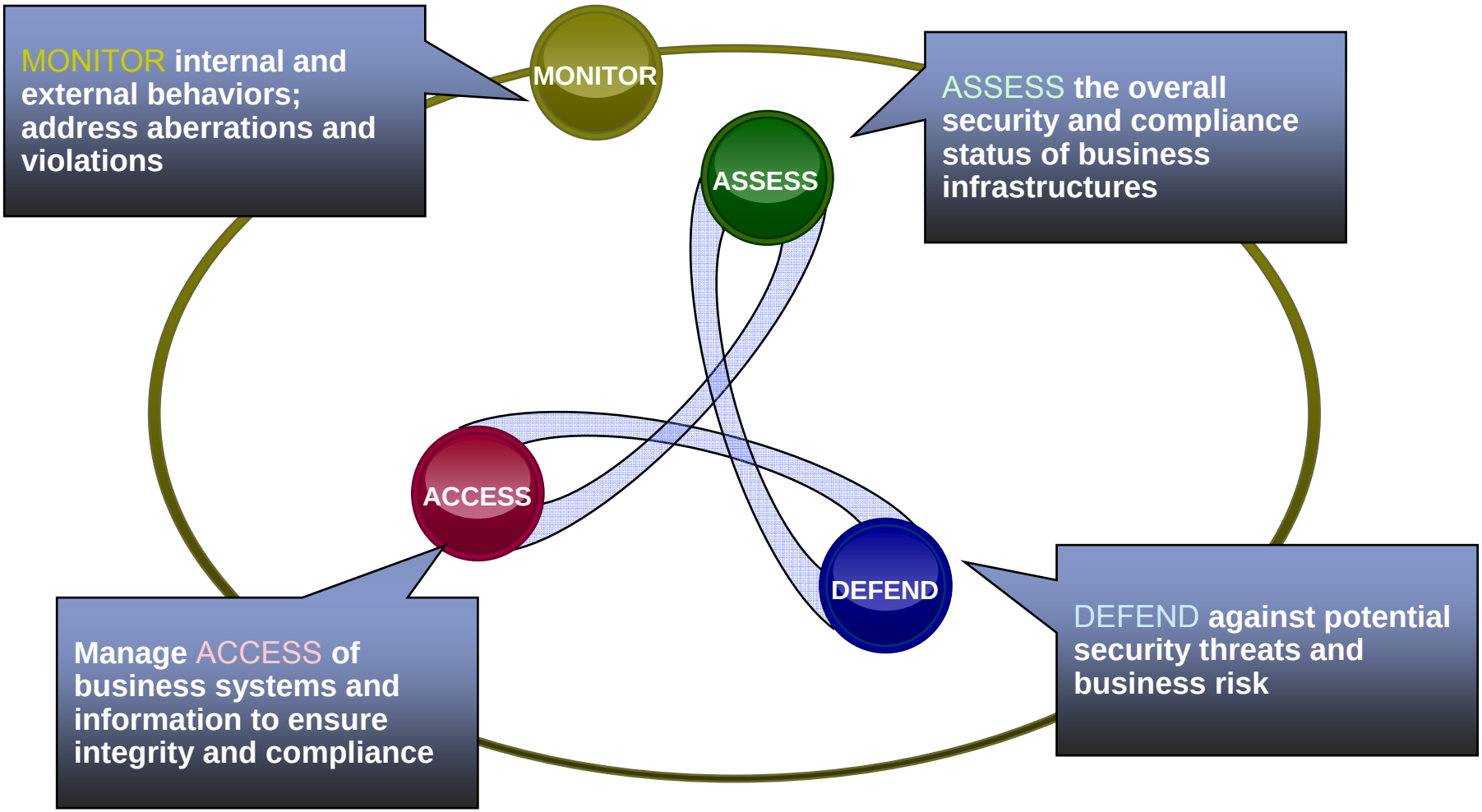
- Überblick über die gesamte Breite von Sicherheitsthemen
- Definition des notwendigen Sicherheitsniveaus
- Identifizierung von Geschäftsrisiken
- Ermittlung des Reifegrads der etablierten Sicherheitsmechanismen und Prozesse im Marktvergleich
- Maßnahmendefinition auf Basis von Best Practices
- Bereitstellungen von Lösungen auf Basis erprobter Referenzachitekturen

IBM: *Comprehensive* Security Risk & Compliance Management

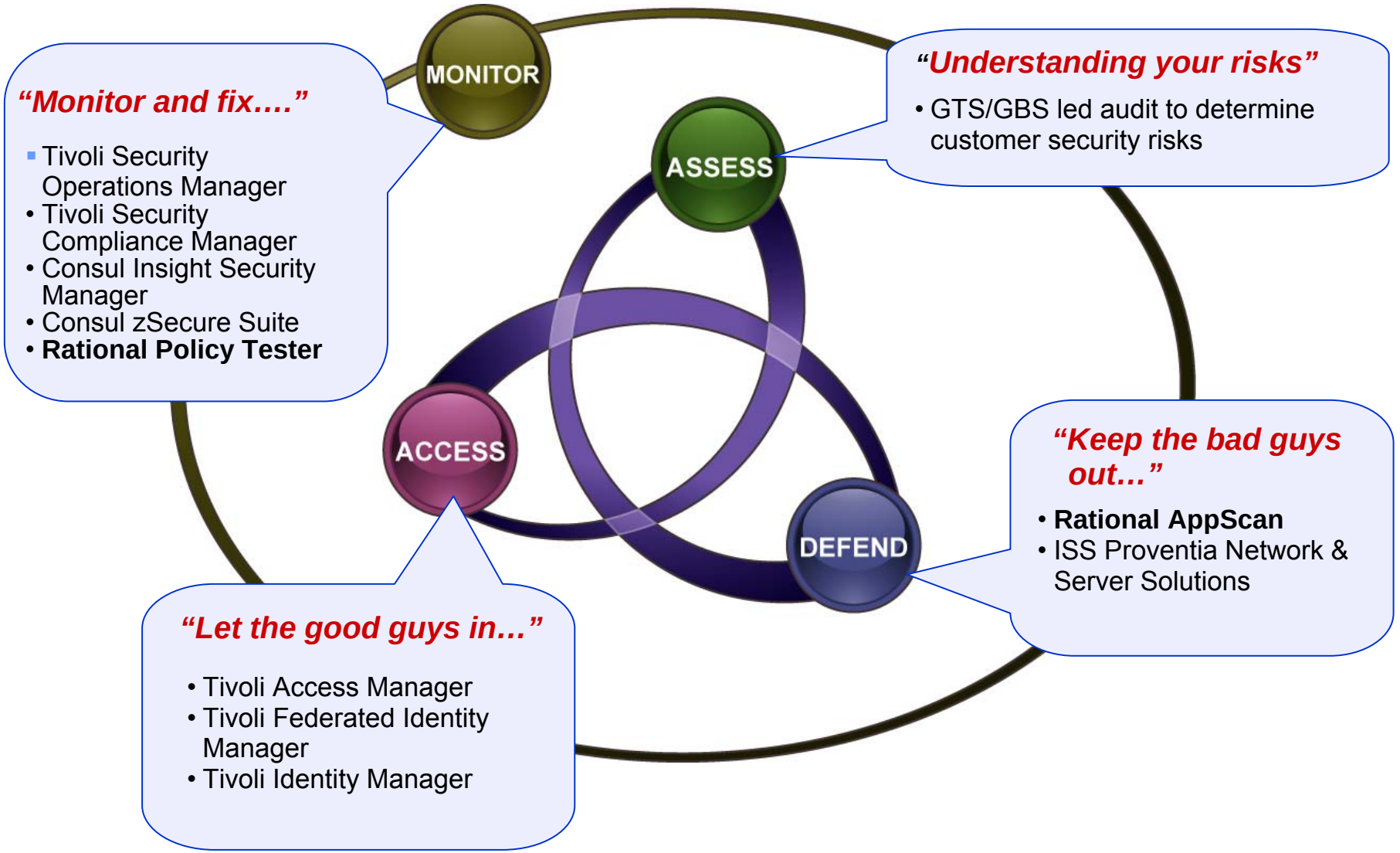
- The *only security vendor* in the market with *end-to-end coverage of the security foundation*
- 15,000 researchers, developers and SMEs on security initiatives
- 3,000+ security & risk management patents
- 200+ security customer references and 50+ published case studies
- 40+ years of proven success securing the zSeries environment
- Already managing more than 2.5B security events per day for clients
- $1.5 Billion security spend in 2008



IBM's Security Management Vision and Strategy



Solutions within IBM Security Portfolio



fix security defects *at the source*

Rational Solutions for Application Security and Compliance can:

- pinpoint vulnerabilities in web applications
- provide guidance for fixing security defects
- help ensure compliance with over 40 regulatory requirements

to reduce the risk of a security breach and improve compliance posture

Quality Management

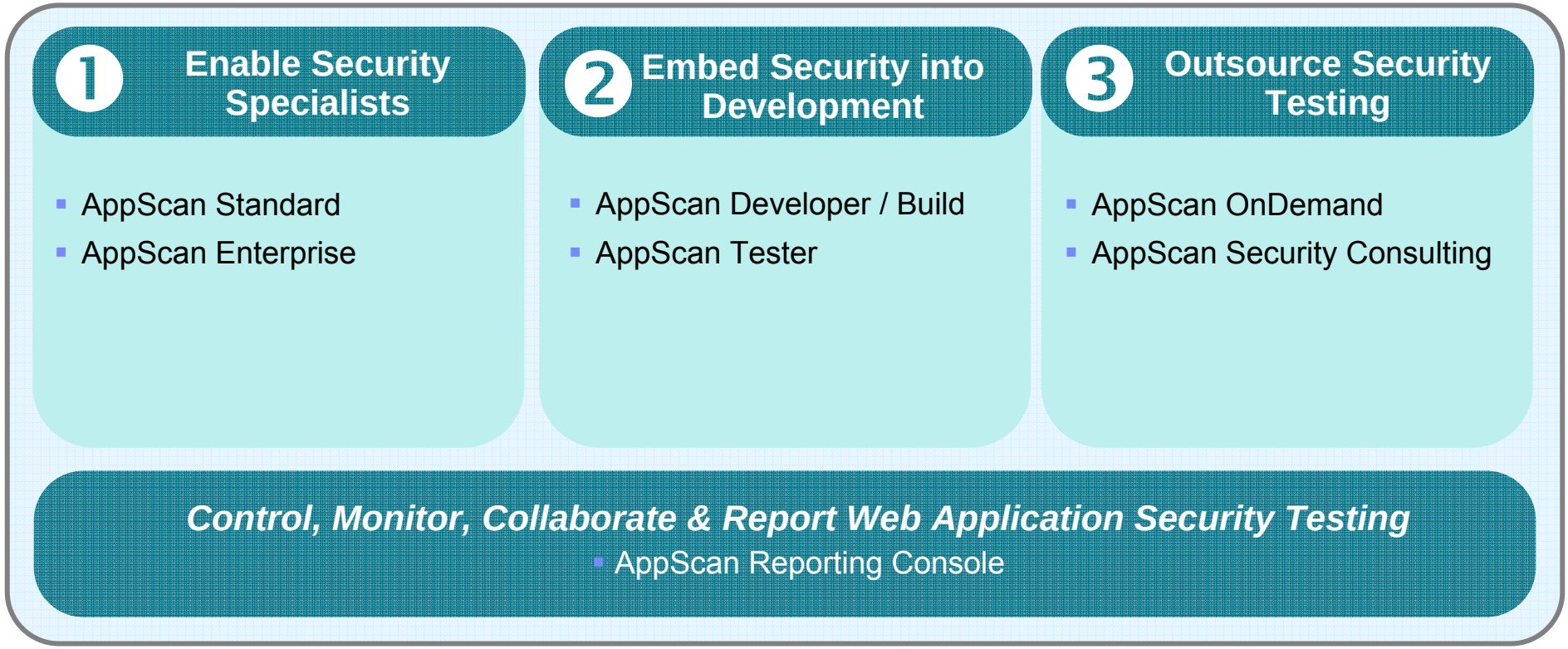
. Rational AppScan
. Rational Policy Tester
. Rational SaaS Offerings
. Computer-Based Training Courses

AppScan vs. Policy Tester

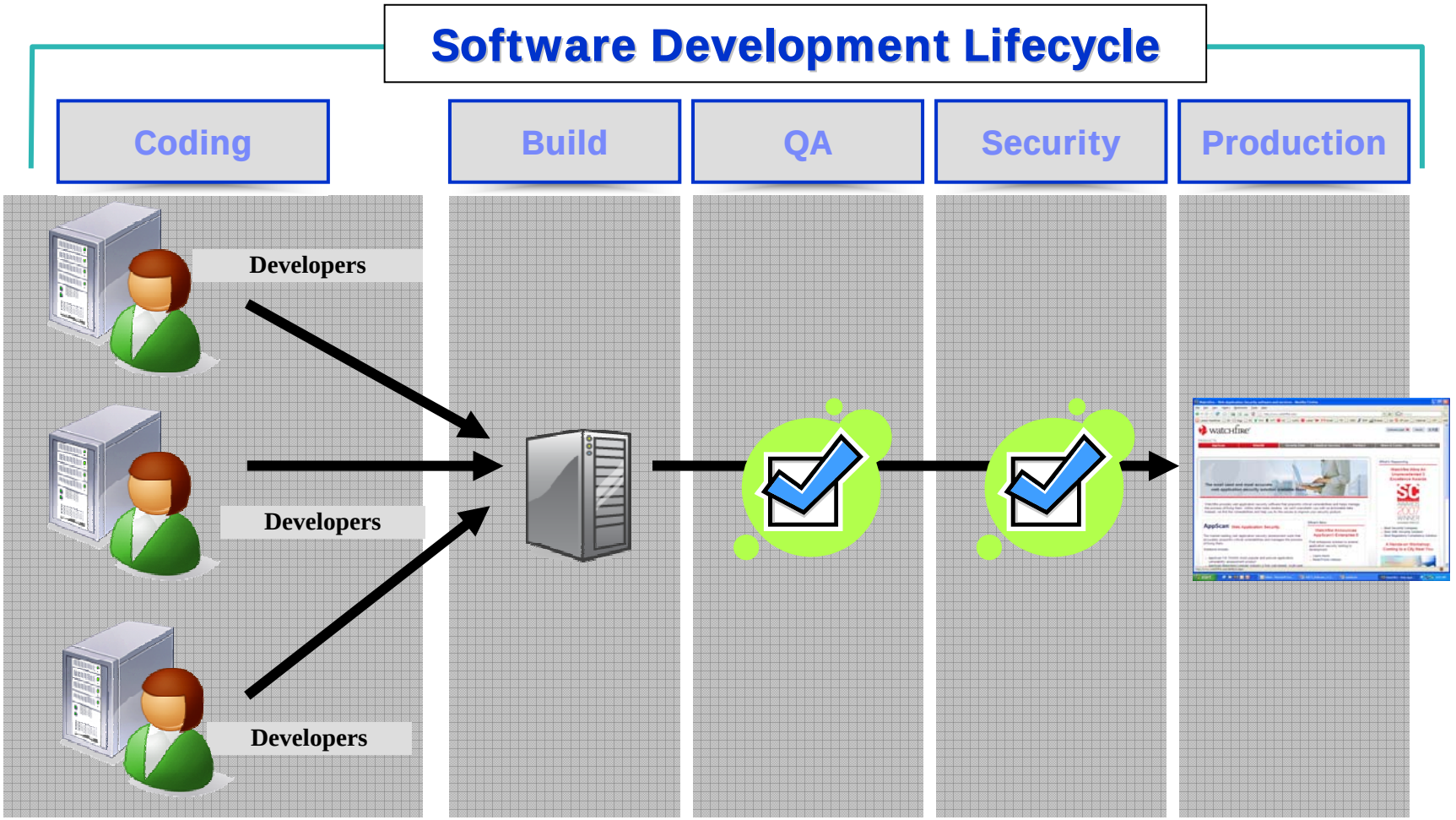
IBM Rational AppScan	IBM Rational Policy Tester
Web application and web service automated **Security** testing	Web Quality & Compliance testing platform to monitor and manage website quality, privacy and compliance
✓ Desktop and enterprise scalable solutions for assessing and remediating security vulnerabilities	✓ Web **Quality** testing to ensure website functionality and a positive user experience
✓ Built for developers, testers, security professionals, and executives	✓ Web **Privacy** testing to meet regulatory compliance such as HIPPA, COPPA, & Safe Harbor
✓ Enterprise-wide reporting and tracking	✓ Web **Accessibility** testing to ensure websites are available to those with disabilities and to meet compliance with Section 508 of the Rehabilitation Act

Operationalization of Security Testing

Customers are addressing Web Application Security in three ways:



Security Testing Within the Software Lifecycle



Security Testing Within the Software Lifecycle

Software Development Lifecycle

Production

Customer Step #1

- Test existing deployed apps in
- Eliminate security exposure in live applications

Application Security Testing Maturity

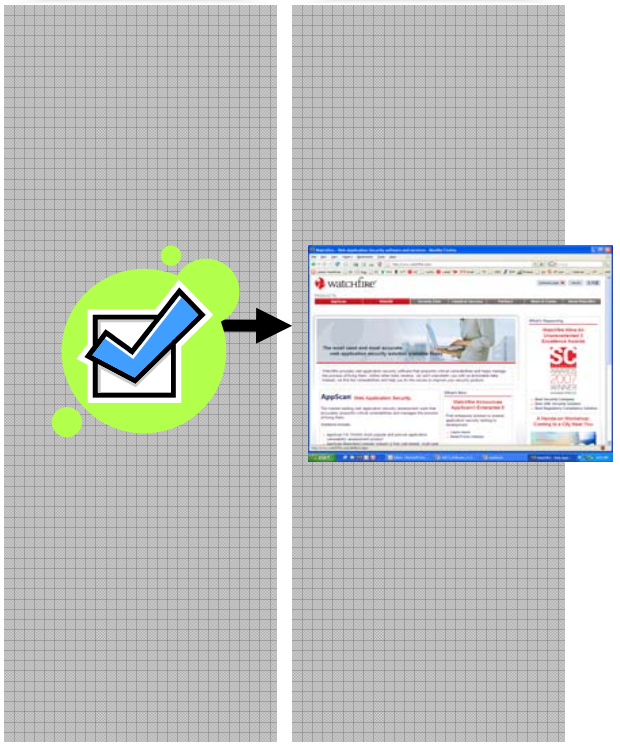
Security Testing Within the Software Lifecycle

Software Development Lifecycle

Security | Production

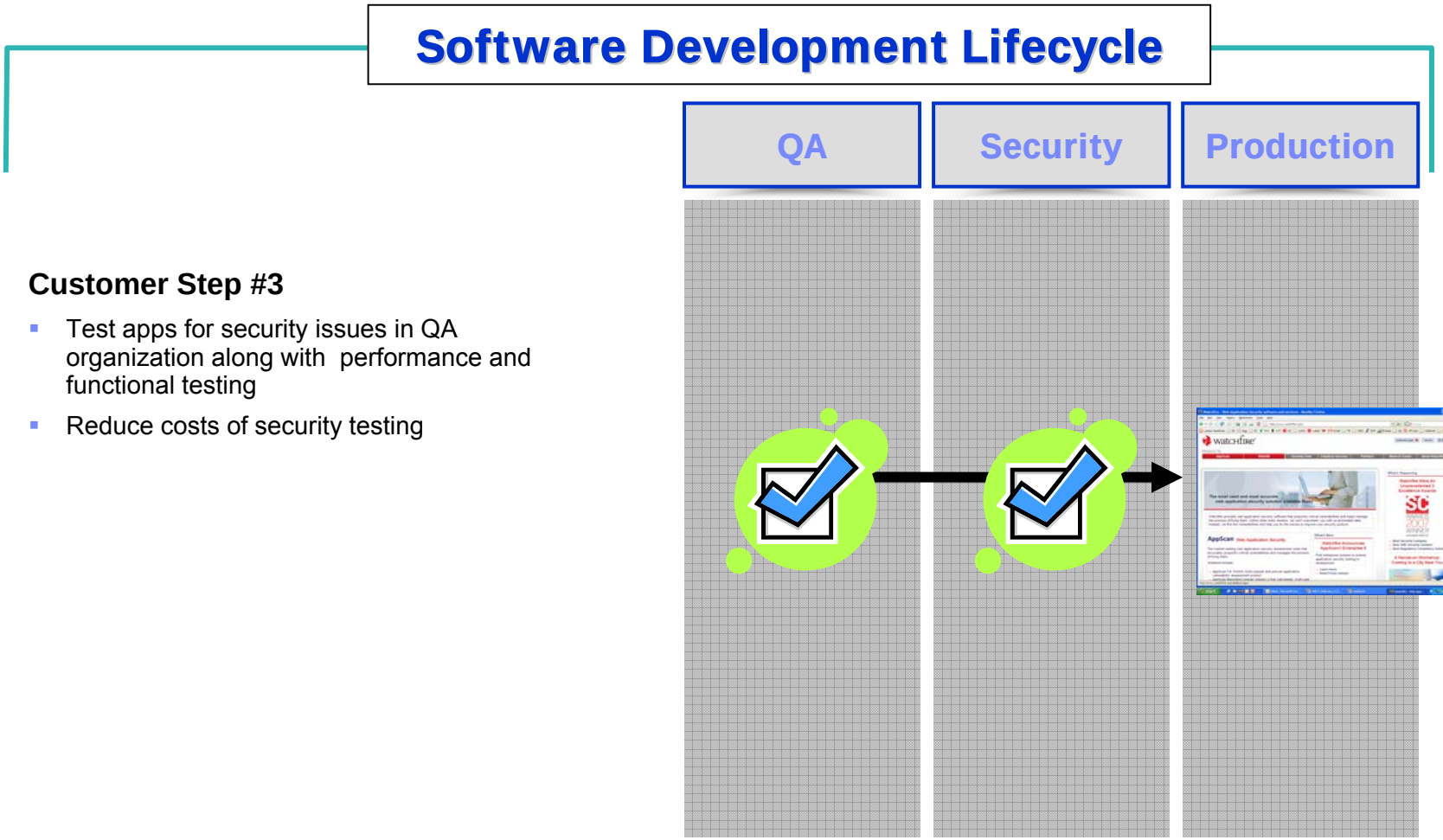
Customer Step #2

- Test apps **before** going to production
- Deploy secure web applications



Application Security Testing Maturity

Security Testing Within the Software Lifecycle

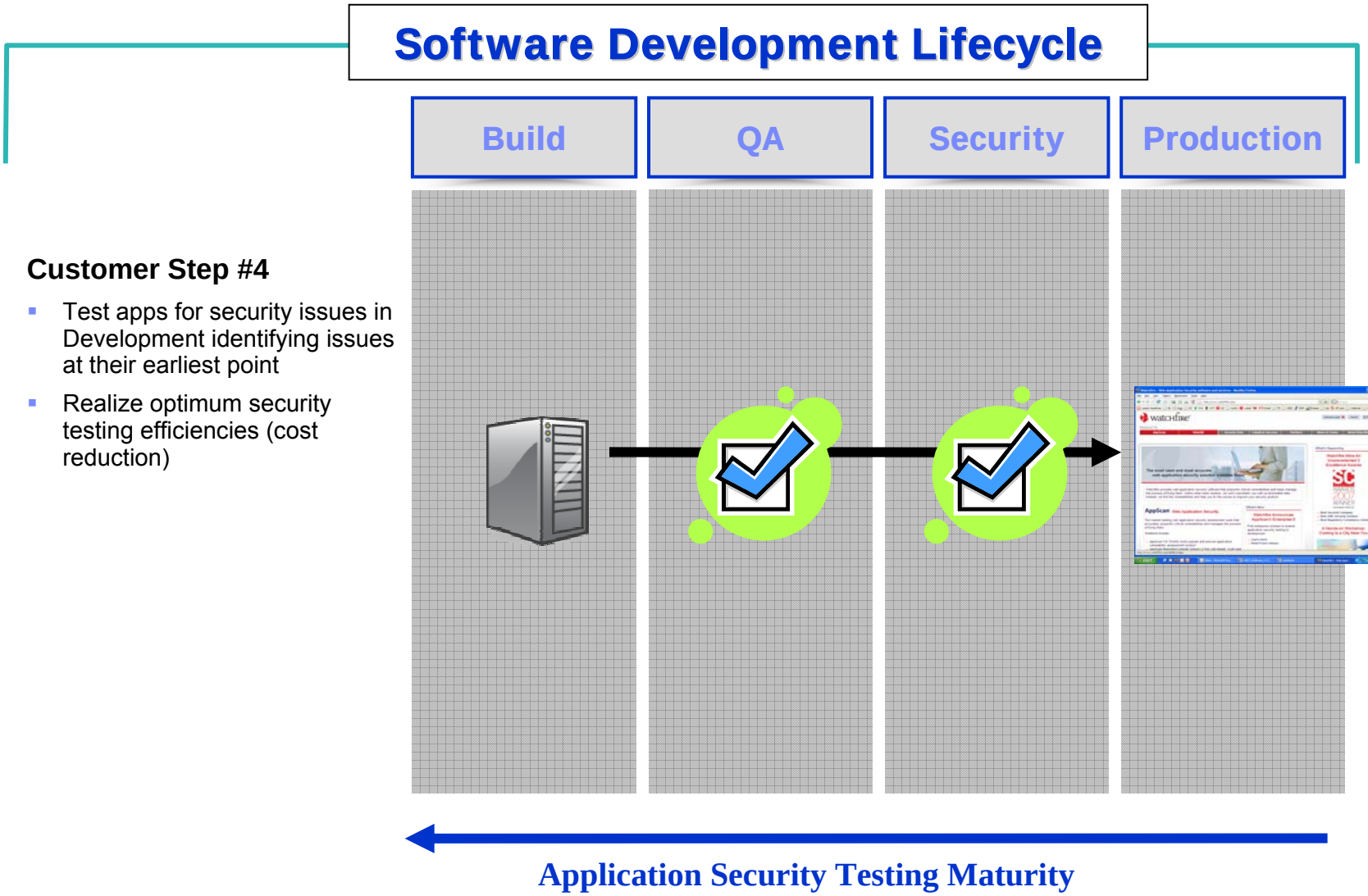


Customer Step #3

- Test apps for security issues in QA organization along with performance and functional testing
- Reduce costs of security testing

Application Security Testing Maturity

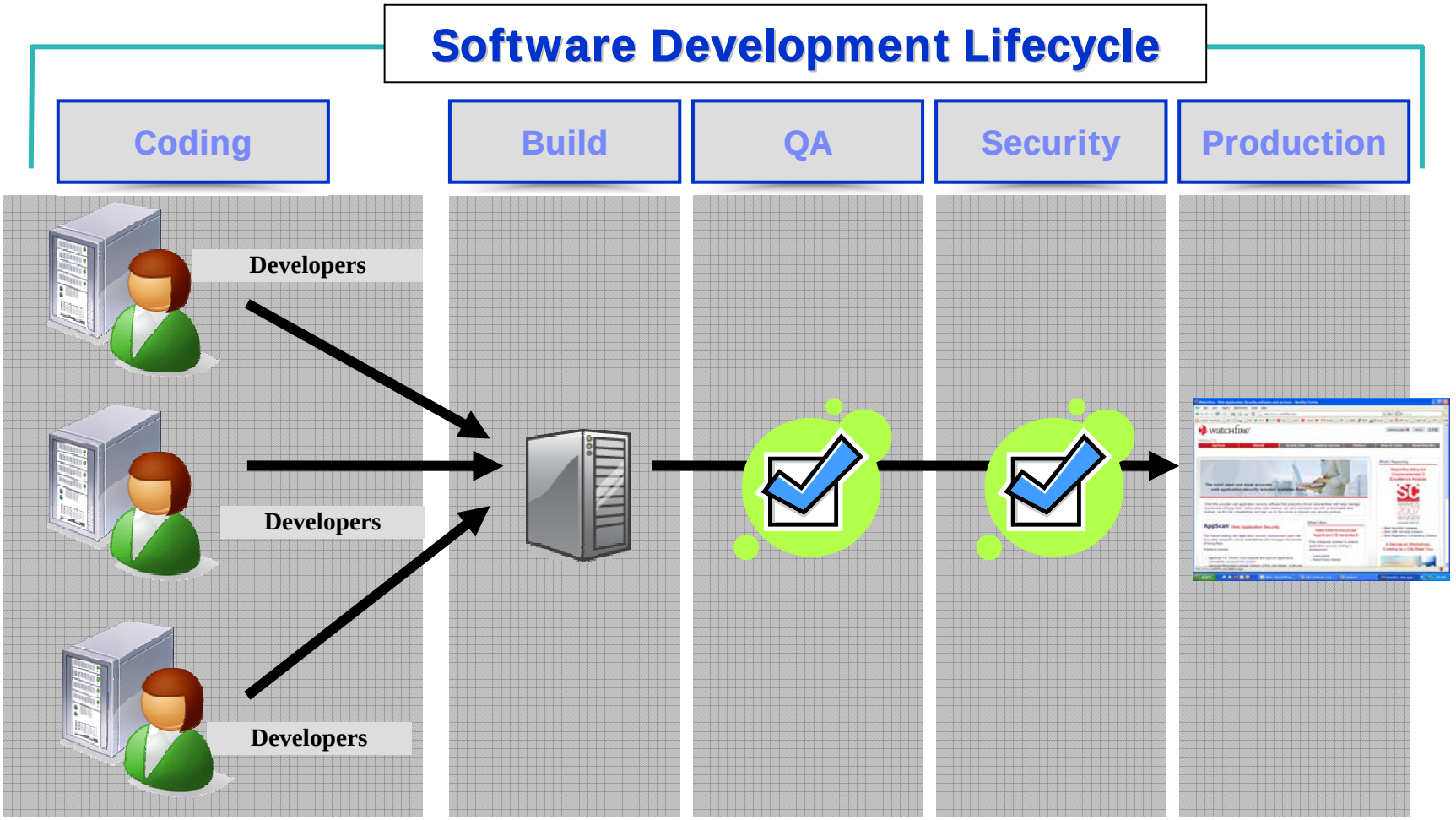
Security Testing Within the Software Lifecycle



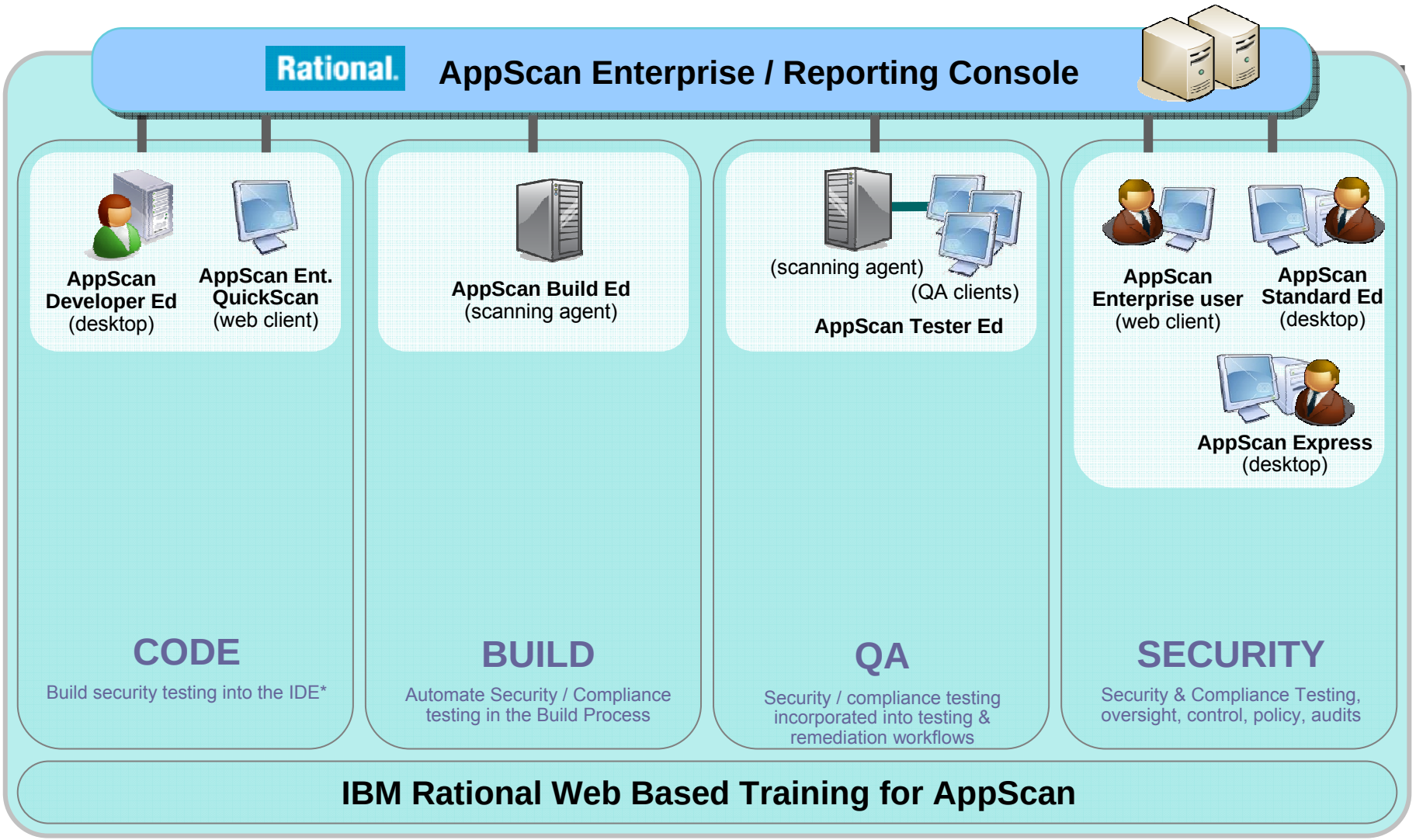
Customer Step #4

- Test apps for security issues in Development identifying issues at their earliest point
- Realize optimum security testing efficiencies (cost reduction)

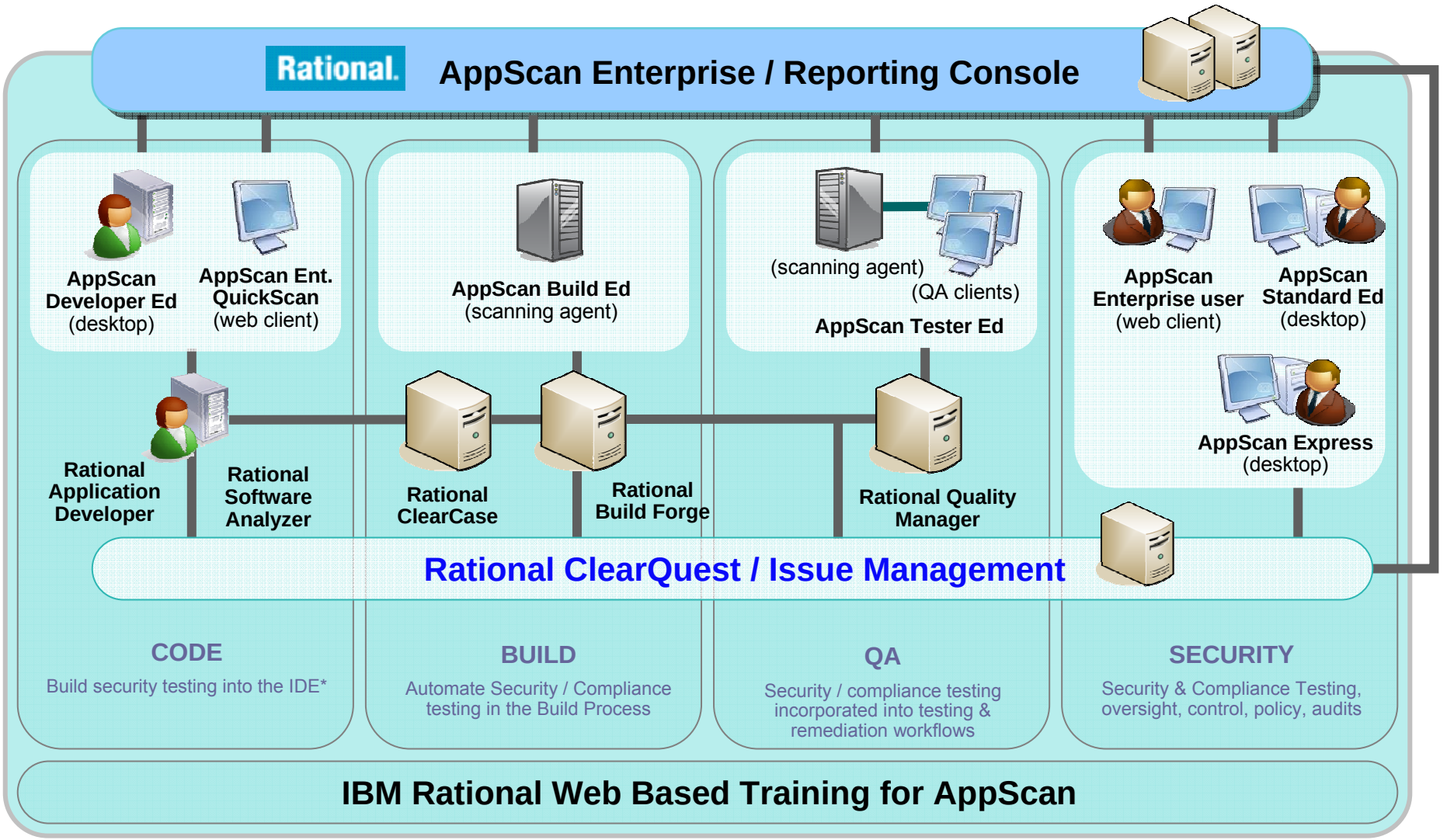
Security Testing Within the Software Lifecycle



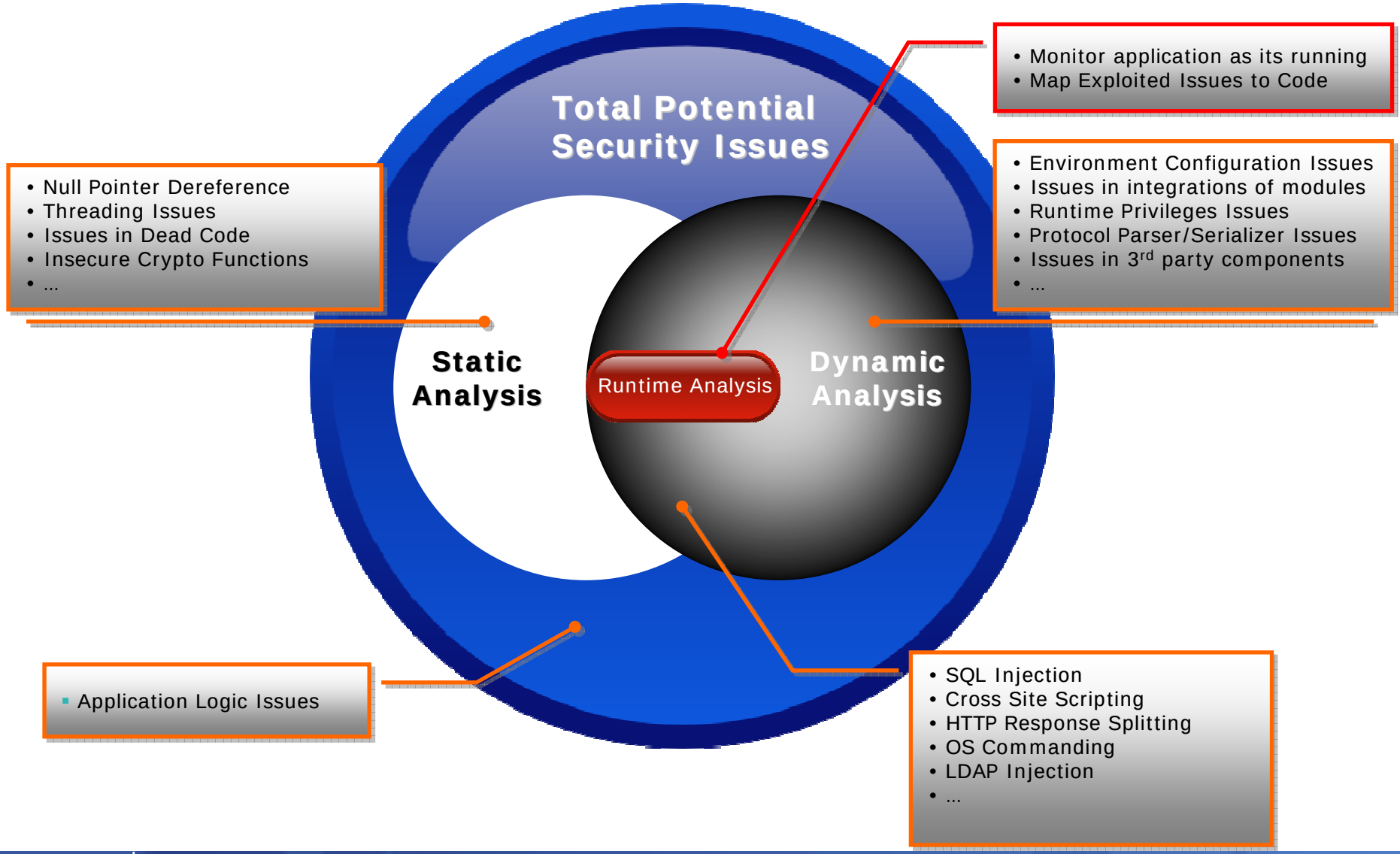
IBM Rational AppScan Ecosystem



IBM Rational AppScan Ecosystem



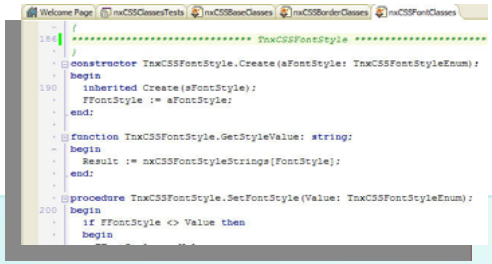
Security Issues Coverage



Analysis Techniques Used

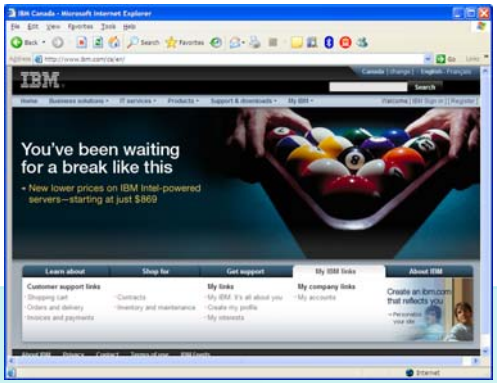
Static Code Analysis <> Whitebox

- Looking at the code for issues (code-level scanning)



Dynamic Analysis <> Blackbox

- Sending tests to a functioning application



Composite Analysis

- Blend of all testing techniques for improved accuracy of reporting
- Leverage strengths and overcomes weaknesses of each individual technique

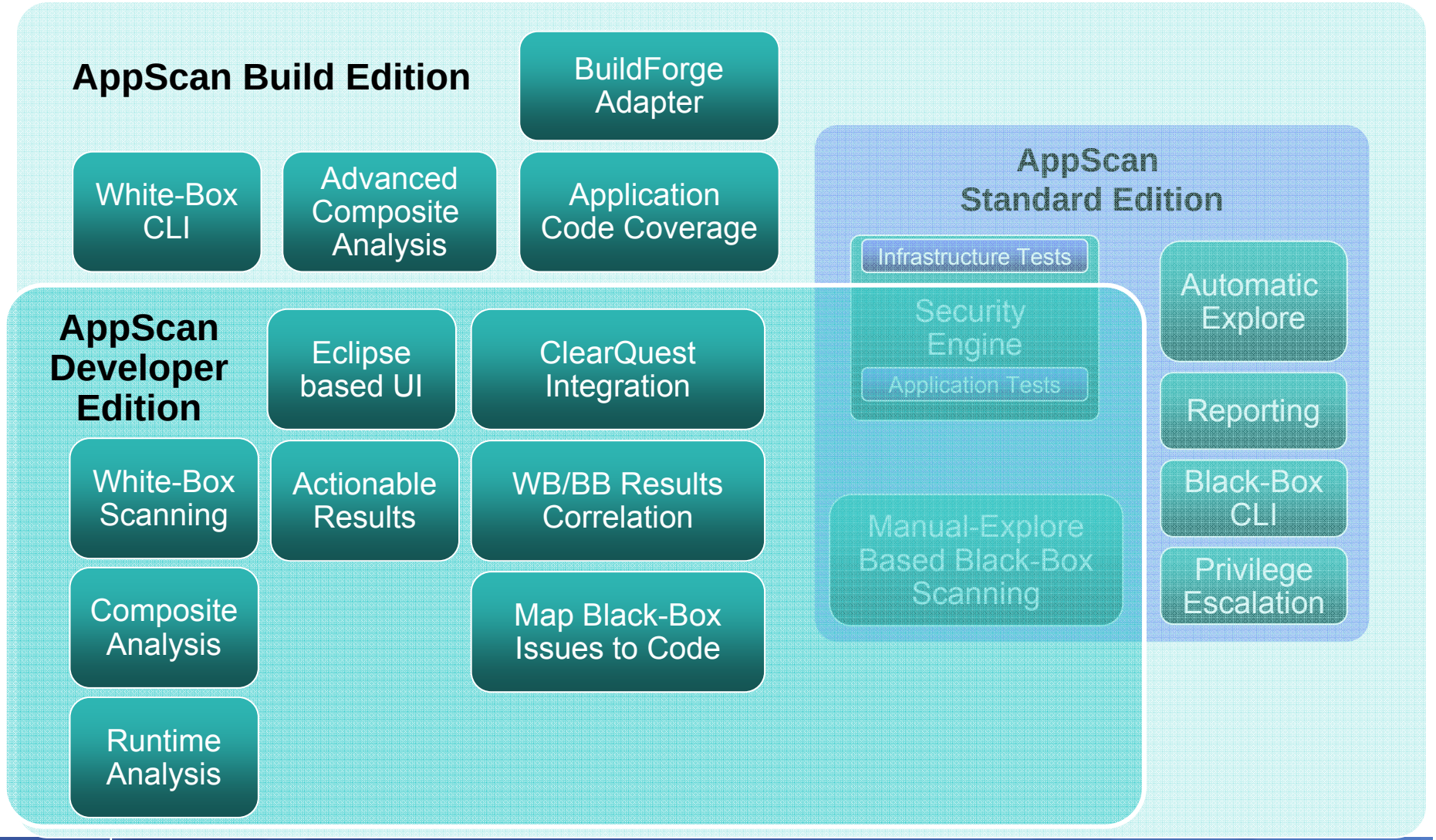
String Analysis

- IBM patent pending code analysis technique
- Code analysis version of “Scan Expert” for efficient configuration of scan to enable accurate results

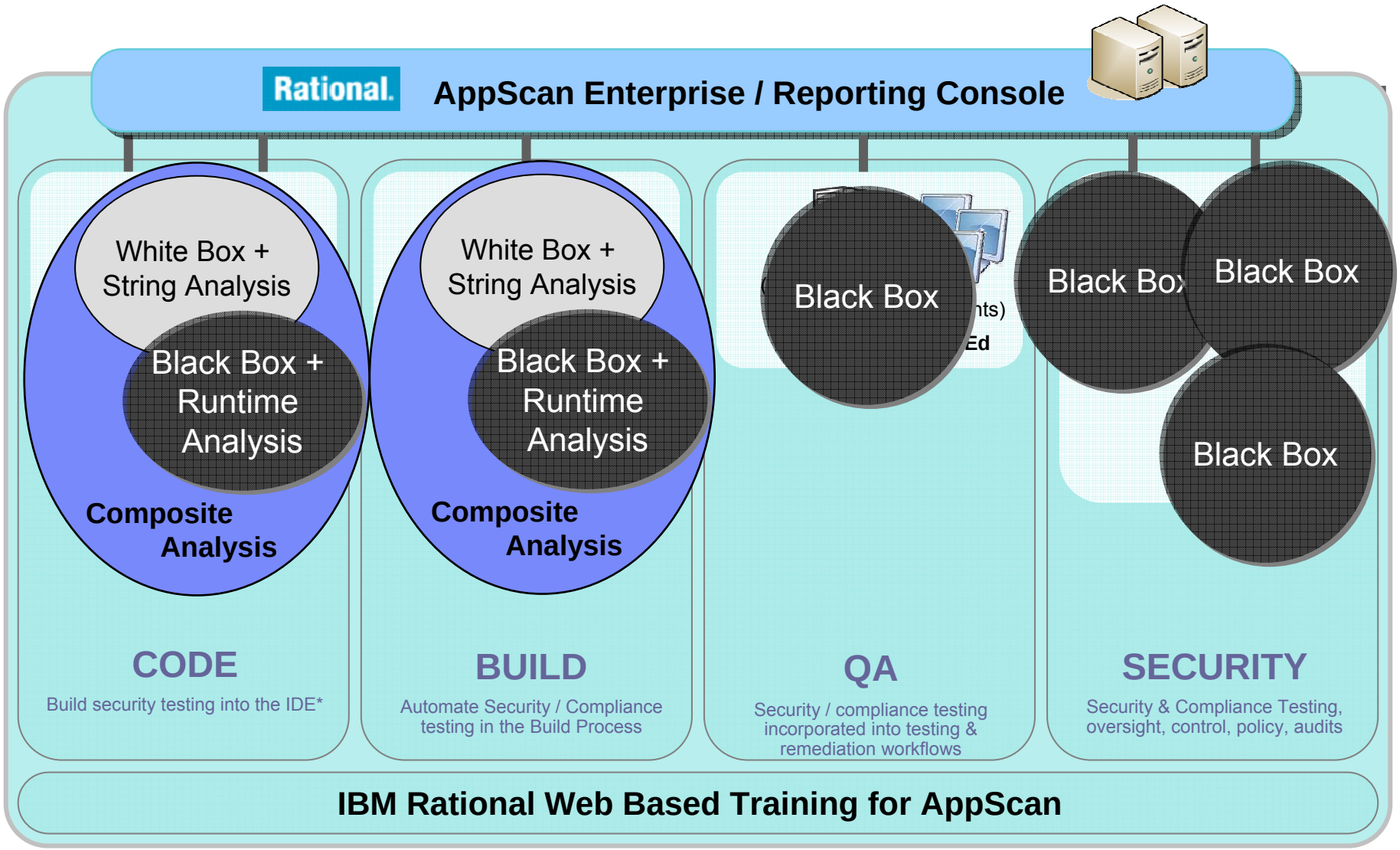
Runtime Analysis

- Monitoring behavior for feedback while application is running at a detailed level to tell where a vulnerability exists in the execution code

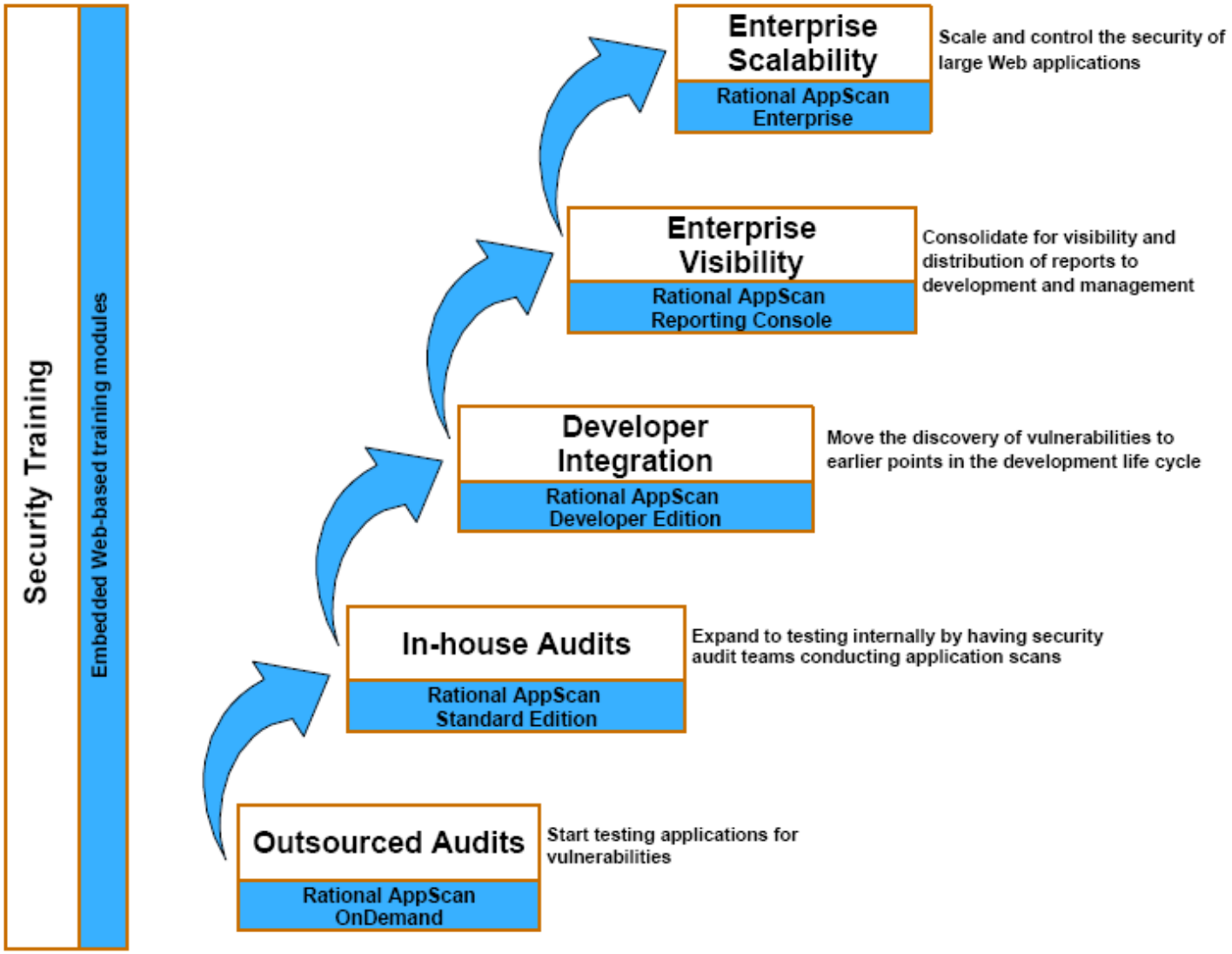
Functionality Diagram



IBM Rational AppScan Ecosystem



Scale-out and up



New Malware-Plug-in for AppScan

Malware ist ein ernstes Problem für alle Kunden, die Daten über das Internet übertragen. Im Rahmen der RSA Security Conference 2009 kündigte IBM Rational eine neue Funktion im Rational AppScan-Produktportfolio an, mit der Malware auf Websites erkannt und durchsucht werden kann. **Malware ist Software, die ohne Einverständnis des Eigentümers in Computersysteme eindringt oder diese beschädigt**.

Weitere Informationen hierzu erhalten Sie in einem Webseminar und einer Präsentation im AppScan Playbook. Diese Materialien befinden sich unter "Identify" und sind mit "Business Partner enablement materials on Malware" gekennzeichnet. **Das Webseminar richtet sich insbesondere an Business Partner und darf nicht beim Kunden vorgestellt werden**.

http://www.ibm.com/vrm/newsletter_10255_5579_122792_email_DYN_1IN/xuvqeh110464599

AppScan's HTTP-Based Malware Scanning

1. **Discover all content and links in a Web Application**
   - Execute JavaScript & Flash
   - Fill forms and login sequences
   - Analyze secure pages
   - …
2. **Analyze all content for malicious behavior indicators**
3. **Compare all links to comprehensive black-lists**

Malware Scanning Summary

- **A New Approach - An HTTP-Based Malware Scanner (AppScan)**
  - Advantages:
    - Has visibility to all content and links (shares victim's point of view)
    - Has time to perform deep analysis content
    - Able to analyze links to determine if they lead to unwanted content
    - Can flag "Suspicious" behavior, less need for 100% confidence

- **The IBM Advantage**
  - Leverages best-of-breed security technology
    - AppScan's Web Application Auditing capabilities
    - ISS's Malware Detection capabilities
  - Supports product or SaaS based monitoring
  - A natural addition to Security Monitoring of Production Environments

Weitere Informationen finden Sie:

auf der IBM Rational AppScan Kundenseite:
http://www.ibm.com/software/de/rational/appscan/index.html

im aktuellen Fachbeitrag auf www.itseccity.de (Juni 2009):
http://www.itseccity.de/?url=/content/fachbeitraege/grundlagen/090622_fac_gru_isc2.html

in der IBM Partnerworld:
https://www-304.ibm.com/jct01005c/partnerworld/mem/mkt/mkt_rational_webapp_playbook.html

im aktuellen Redbook (Juni 2009):
http://www.redbooks.ibm.com/abstracts/redp4530.html?Open

auf der Developerworks Produktseite:
http://www.ibm.com/developerworks/rational/products/appscan/

oder bei Ihrem lokalen IBM Team: **AppScan@de.ibm.com**

Kontaktdaten:

Thomas Neudert

Product Sales Specialist – Rational AppScan
Tel: 0151-11755765
Email: Thomas_Neudert@de.ibm.com

Vielen Dank für Ihre Aufmerksamkeit!