



IBM Software Partner Academy Program

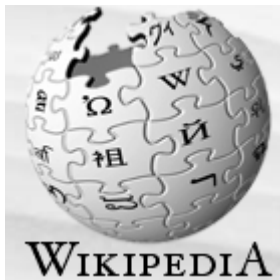
## Telefonkonferenz am 24.07.09

„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  
through spokesm

Like ChoicePoint  
Security numbers  
"Multistate Anti-



Time Frame:  Analytical charting

### Last 5 days quote

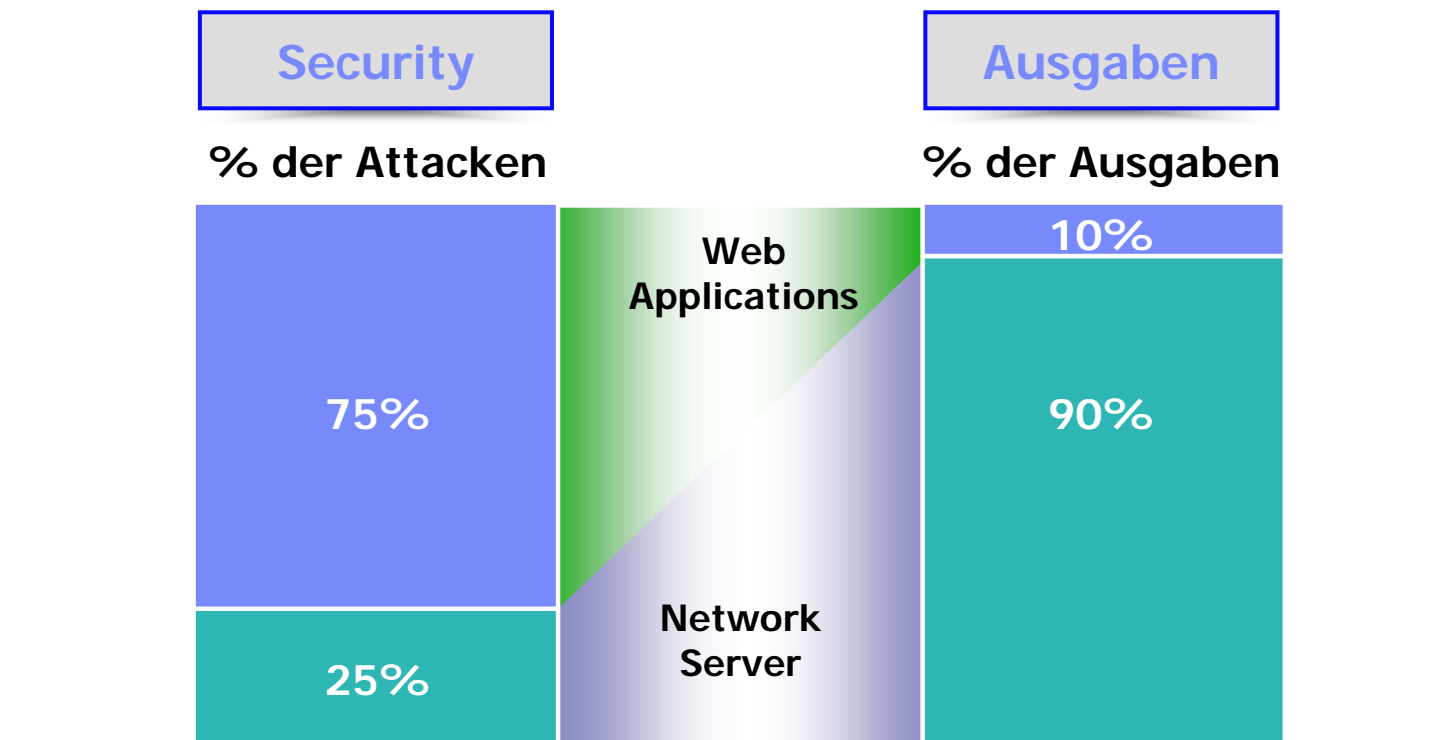
| Date     | Close | Net Change | % Change ** |
|----------|-------|------------|-------------|
| 9Mar2005 | 538   | ▼ -8.75    | -1.60%      |

- **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

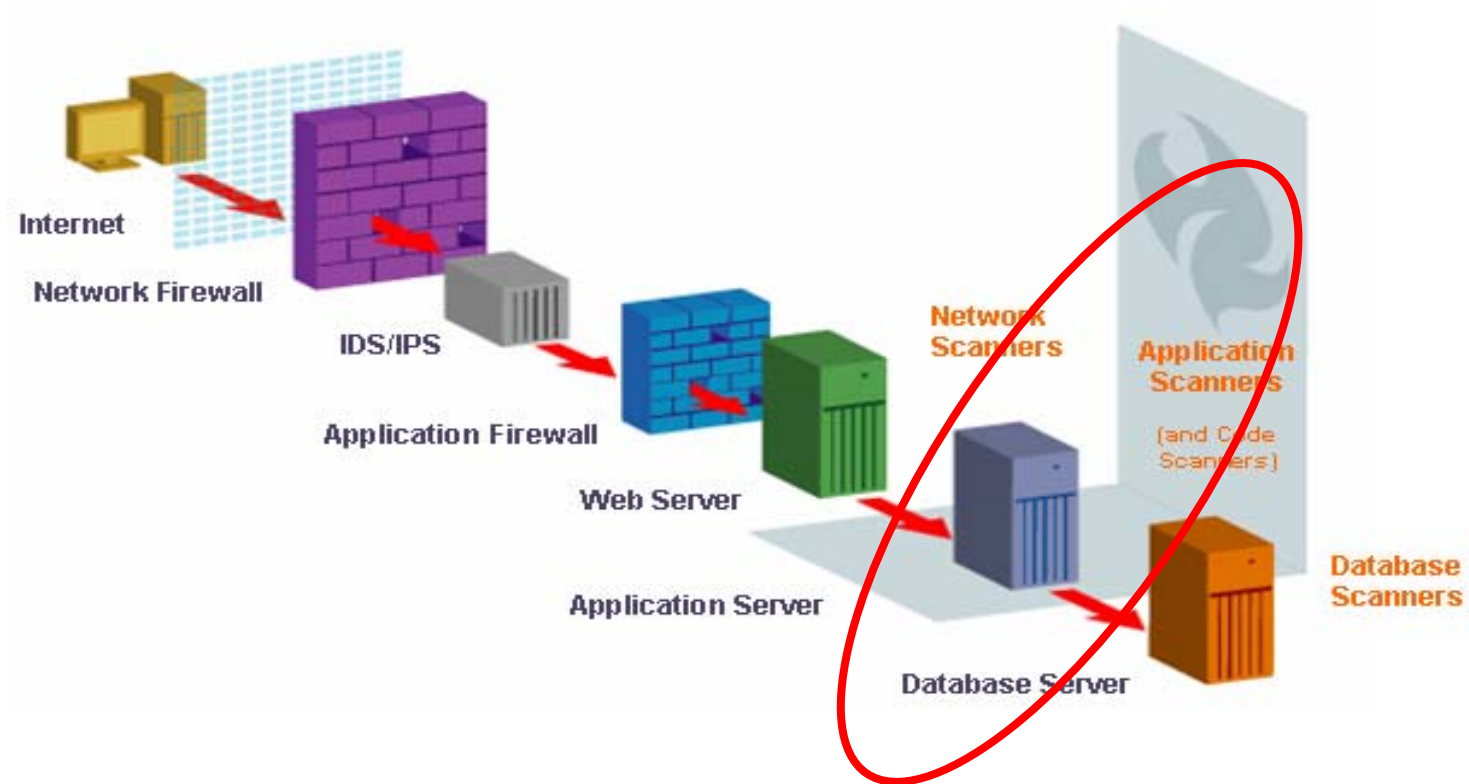


**75%** aller Attacken auf Informationssicherheit finden im Web Application Layer statt

**2/3** aller Web Applicationen sind gefährdet.

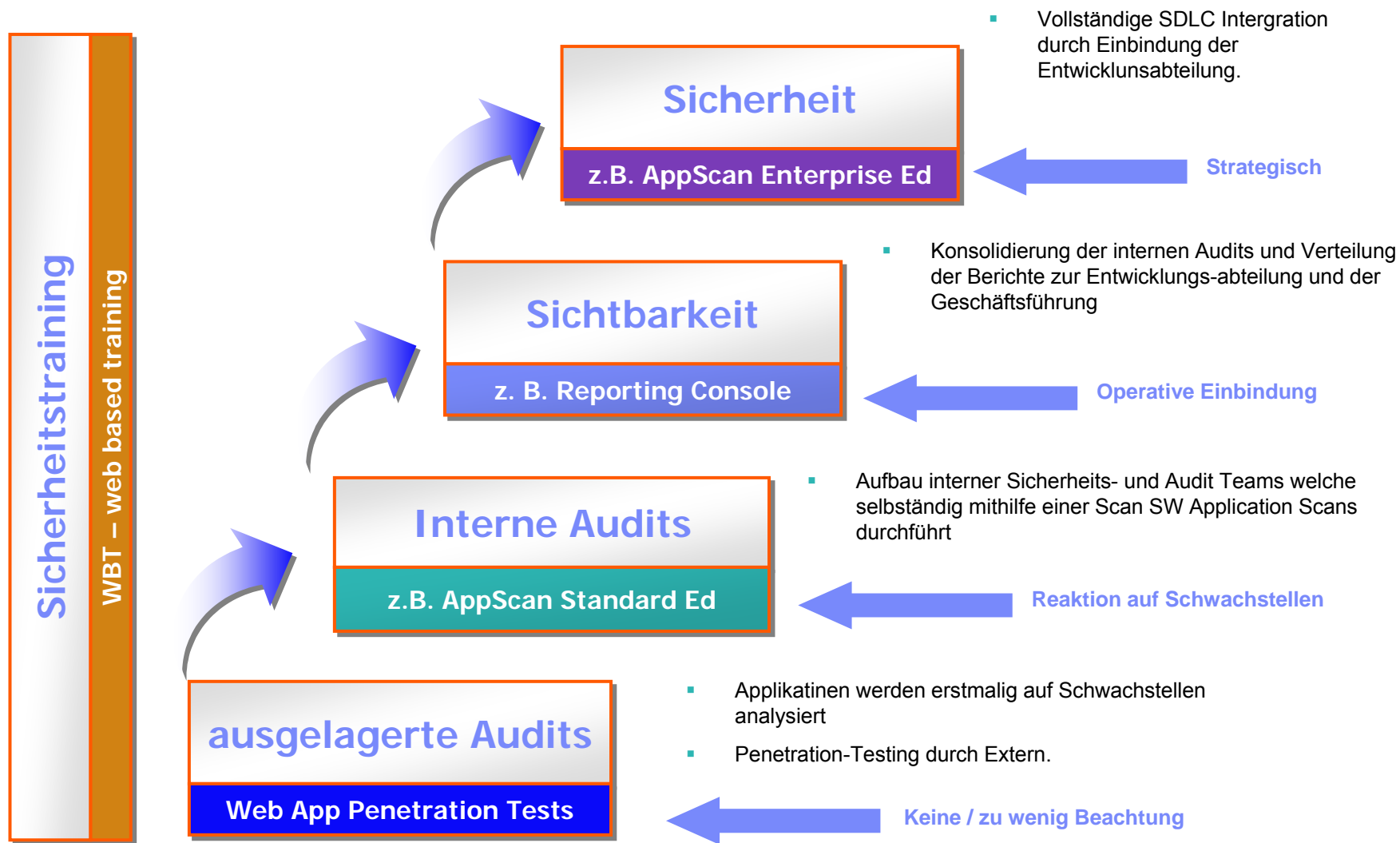
Gartner

# Einordnung der „Web Application Security“



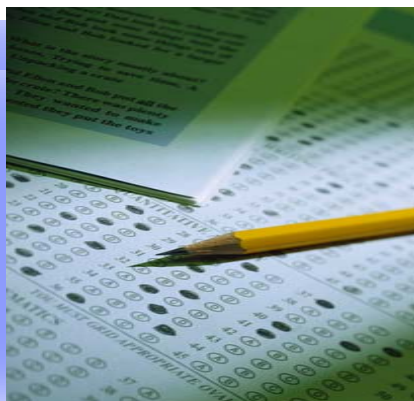


# Web Application Security – Lösungsansätze



## 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

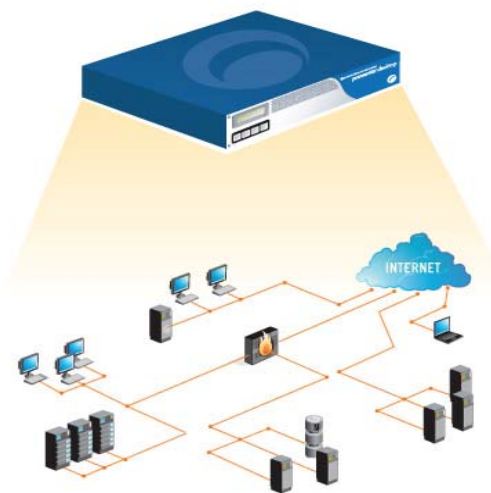
je später ein Fehler beseitigt wird, umso teurer wird es

# Was macht ein Webapplication Scanner?

## Automatisiertes Testen von Web Applikationen auf Sicherheitsschwachstellen

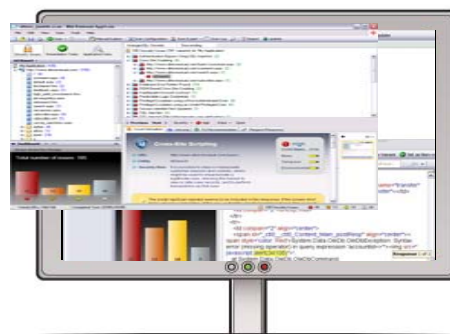
1

Analyse der Struktur und Komplexität der Web Site / Applikation



2

Identifizierung der Sicherheits-Schwachstellen, Berichtserstellung priorisiert nach Relevanz.



3

Konkrete Lösungsvorschläge und weiterführende Unterstützung. Nachverfolgung und Compliance Unterstützung



# Beispiel eines Scans

The screenshot shows the IBM Rational AppScan interface for a scan named 'altoro.jsmith.scan'. The main window displays a list of 105 security issues, sorted by severity in descending order. The issues include:

- Authentication Bypass Using SQL Injection (2)
- Cross-Site Scripting (6)
  - http://www.althoromutual.com/bank/customize.aspx (2)
  - http://www.althoromutual.com/comment.aspx (2)
  - http://www.althoromutual.com/search.aspx (1)
  - txtSearch
  - http://www.althoromutual.com/subscribe.aspx (1)
- Database Error Pattern Found (10)
- DOM Based Cross-Site Scripting (2)
- Inadequate Account Lockout (1)
- Predictable Login Credentials (1)
- Privilege Escalation using a Non-Authenticated User (8)
- Privilege Escalation using an Under-Privileged User (4)
- Session Identifier Not Updated (1)
- SQL Injection (6)
- SQL Injection File Write (requires user verification) (1)

The detailed view of a Cross-Site Scripting issue is shown below:

- Issue Information:** Cross-Site Scripting
- Severity:** High
- CVSS Metric:** (7.5)
- URL:** http://www.althoromutual.com/search.aspx
- Entity:** txtSearch
- Security Risk:** It is possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user.

The dashboard at the bottom left shows an 'Issue Severity Gauge' with the following data:

| Severity | Count |
|----------|-------|
| Critical | 45    |
| High     | 13    |
| Medium   | 19    |
| Low      | 28    |

Additional dashboard information includes: Total number of issues: 105, Visited URLs: 166/166, Completed Tests: 25355/25355, and a summary of 105 Security Issues (45 High, 13 Medium, 19 Low, 28 Information).

## 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 & RESSOURCEN**

## Woher kommt AppScan? Was ist Watchfire?



#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



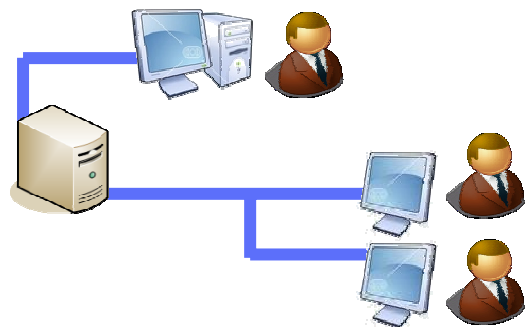
## AppScan Versionen (Black Box)



### Appscan Standard Edition (Desktop)

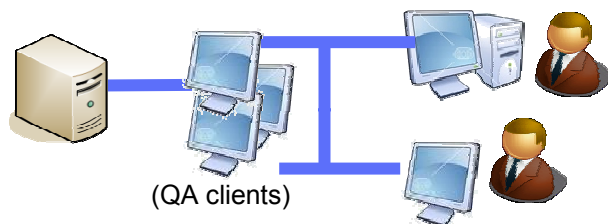
- Desktop basiertes Scanning
- **Einstiegslösung**

+



### Appscan Reporting Console (Server/Client)

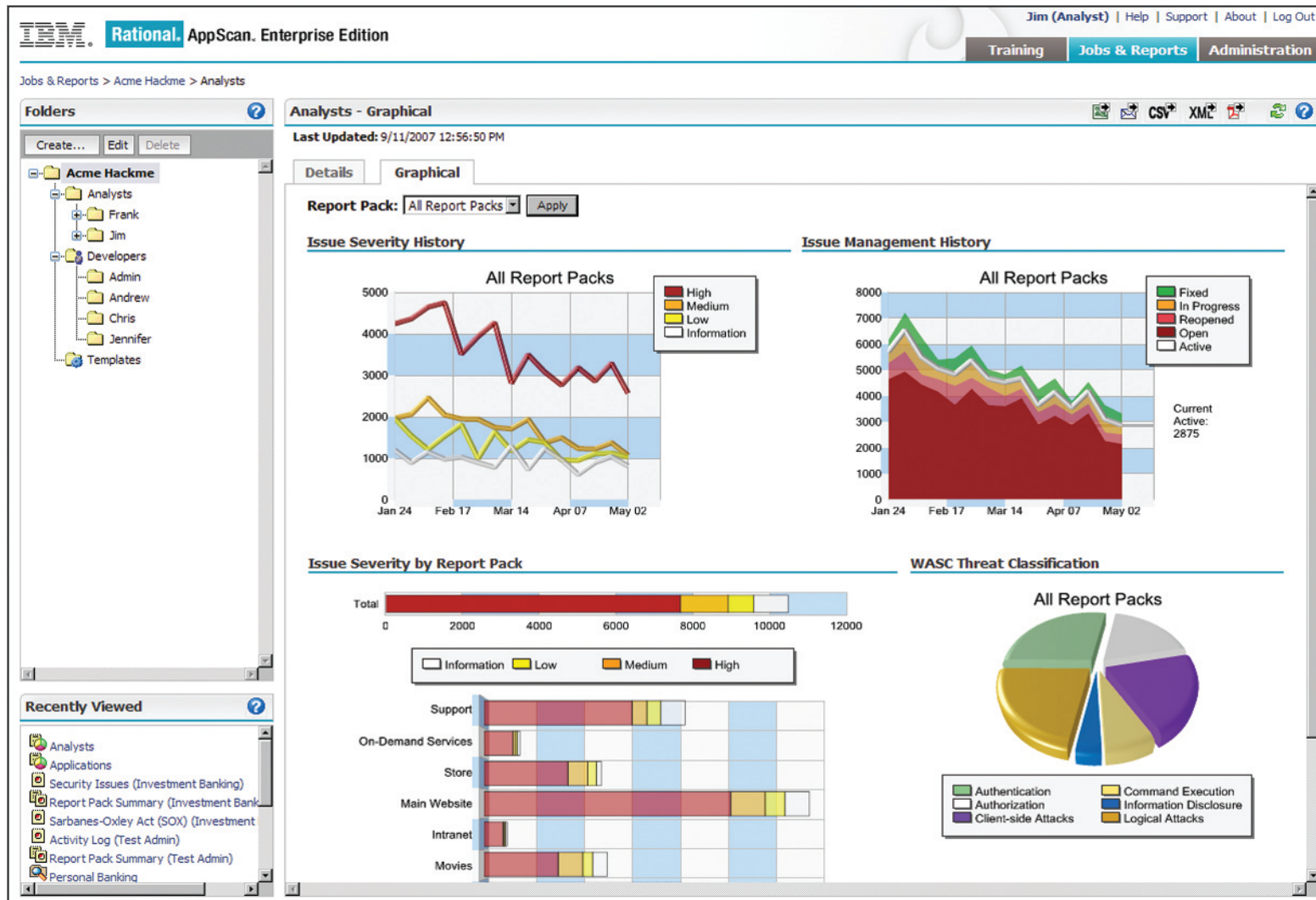
- Server & Rollen basierender SICHERER Austausch der Reports und Analyseergebnisse



### Appscan Enterprise Version (Server/Client)

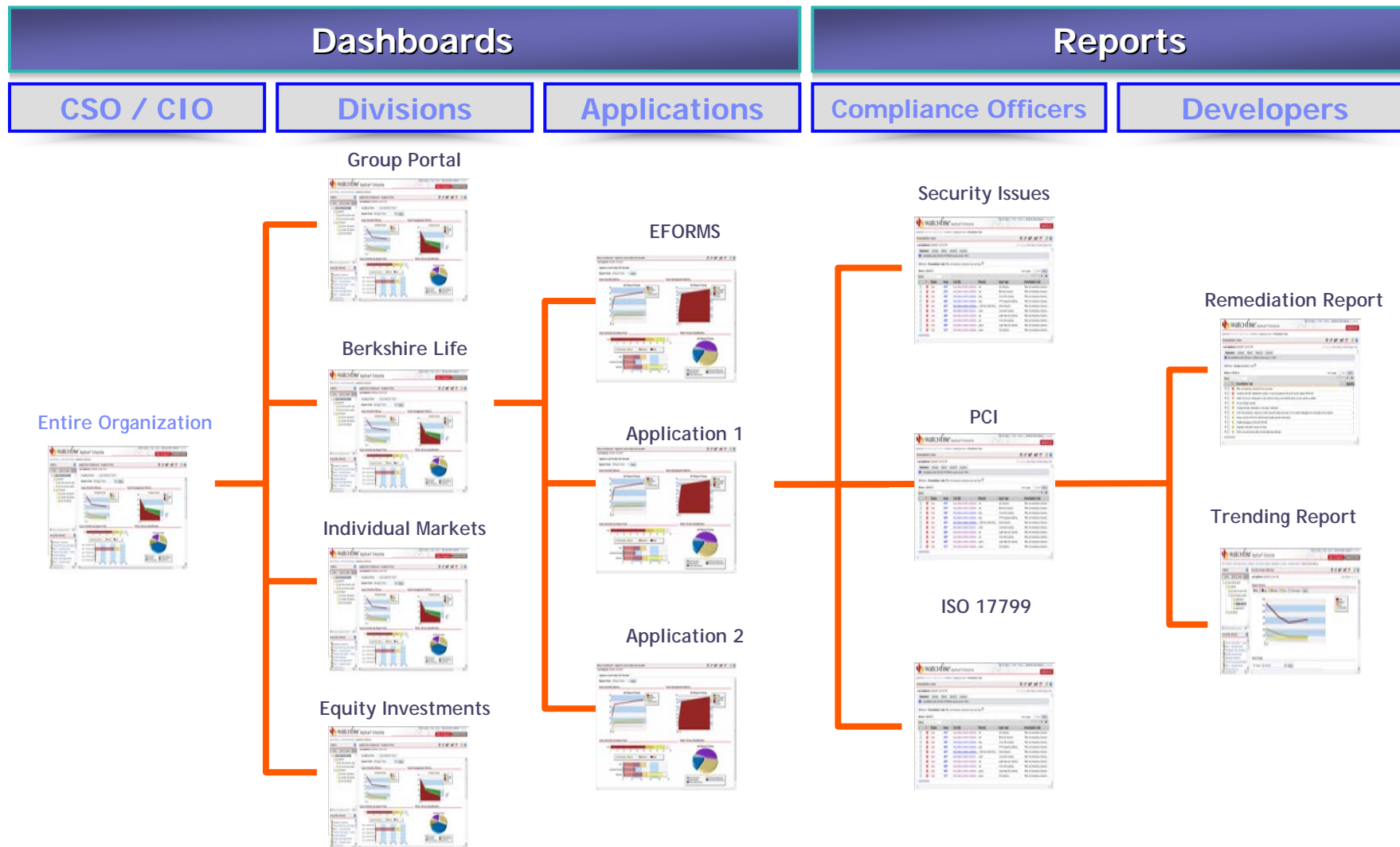
- Server basiertes Scanning im gesamten SDLC / zentrale Steuerung, Workflow, Web-based

# Beispiel Management Dashboards





# Sichtbarkeit im gesamten Unternehmen



# AppScan Einstiegslösung - Listpreise

## AppScan Standard Edition

Floating User



|              |        |
|--------------|--------|
| User Licence | 31.394 |
| Renewal      | 6.279  |

## AppScan Express Edition

Authorized User



|              |        |
|--------------|--------|
| User Licence | 17.387 |
| Renewal      | 3.477  |

oder

|                      |        |
|----------------------|--------|
| „Consulting Licence“ | 27.627 |
| Renewal              | 5.525  |

entspricht Rabattstufe D  
der Standard Edition

## Was heißt „Ganzheitliche Sicherheit“ ?

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



# Entdecke die Welt neuer Möglichkeiten

Globalisierung schafft Zugang zu weltweiten Ressourcen

Milliarden mobile Geräte bekommen Zugang zum World Wide Web

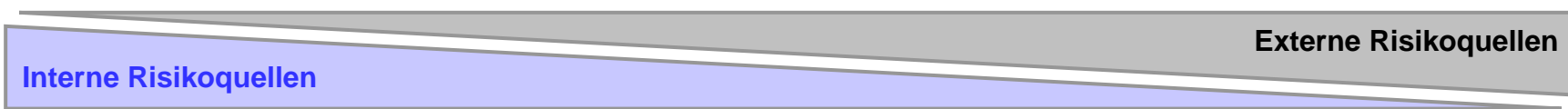
Zugang zu Informationen ohne zeitliche Verzögerung



**Neue Möglichkeiten**  
**Neue Komplexität**  
**Neue Risiken**

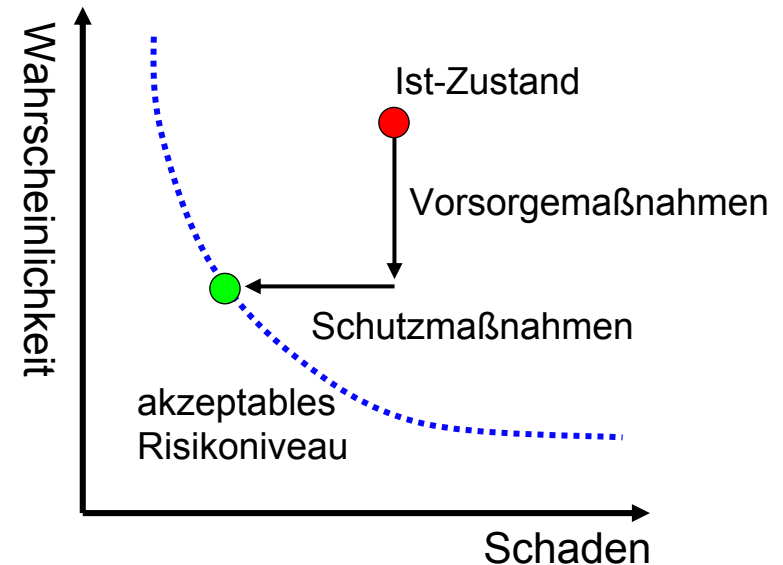
# Gesamtheitliche Bewertung von Risiken

| Interne Verfahren  | Systeme   | Menschen   |   | Externe Ereignisse   |  |
|--|---|--|---|--|--|
|  |   | Mitarbeiter  | Externe   | Direktes Umfeld  | Katastrophen   |
| <ul style="list-style-type: none"> <li>▪ Falsche Strategie</li> <li>▪ Fehlende Zielausrichtung</li> <li>▪ <b>Unklare Verantwortlichkeiten</b></li> <li>▪ <b>Schlechte Prozessdefinition und -umsetzung</b></li> <li>▪ Mangelnde Anpassungsfähigkeit an neue Anforderungen</li> </ul> | <ul style="list-style-type: none"> <li>▪ Hardwaredefekte</li> <li>▪ <b>Softwarefehler</b></li> <li>▪ Schlechte Administration</li> <li>▪ Mangelhafte Benutzerfreundlichkeit</li> <li>▪ Anfälligkeit gegen Würmer und Viren</li> <li>▪ Inadäquate Architekturen</li> <li>▪ Stromausfall</li> </ul> | <ul style="list-style-type: none"> <li>▪ Missbrauch</li> <li>▪ <b>Diebstahl</b></li> <li>▪ <b>Unachtsamkeit, Unwissenheit</b></li> <li>▪ Menschliches Versagen</li> <li>▪ Bestechung</li> <li>▪ Fluktuation</li> </ul> | <ul style="list-style-type: none"> <li>▪ Computerviren und Würmer</li> <li>▪ <b>Hacking</b></li> <li>▪ Einbruch</li> <li>▪ Betrug</li> <li>▪ Vandalismus</li> <li>▪ Raub, Diebstahl</li> <li>▪ Sabotage</li> <li>▪ Spionage</li> <li>▪ Terrorismus</li> </ul> | <ul style="list-style-type: none"> <li>▪ Ausfall der Kommunikationsverbindungen (Telefon, Mail, Web)</li> <li>▪ Änderung der regulatorischen Anforderungen</li> <li>▪ Verlust der Verkehrsverbindungen</li> <li>▪ Extreme Nachfrageschwankungen</li> </ul> | <ul style="list-style-type: none"> <li>▪ Erdbeben</li> <li>▪ Hochwasser</li> <li>▪ Sturm</li> <li>▪ Frost</li> <li>▪ Feuer</li> <li>▪ Explosion</li> <li>▪ Chemieunfälle</li> <li>▪ Flugzeugabsturz, Verkehrsunfälle</li> <li>▪ Krieg</li> </ul> |

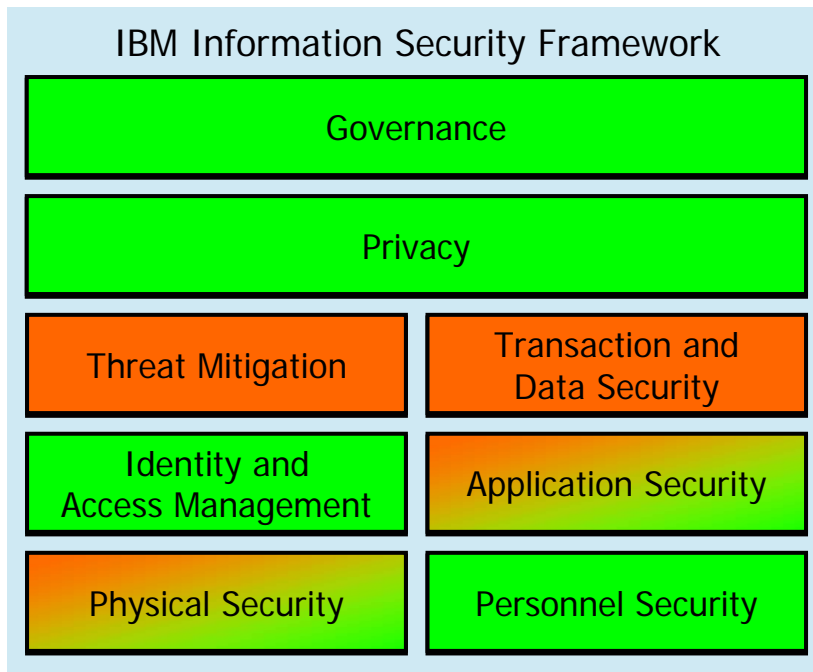


## Ganzheitliches Vorgehen

- 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



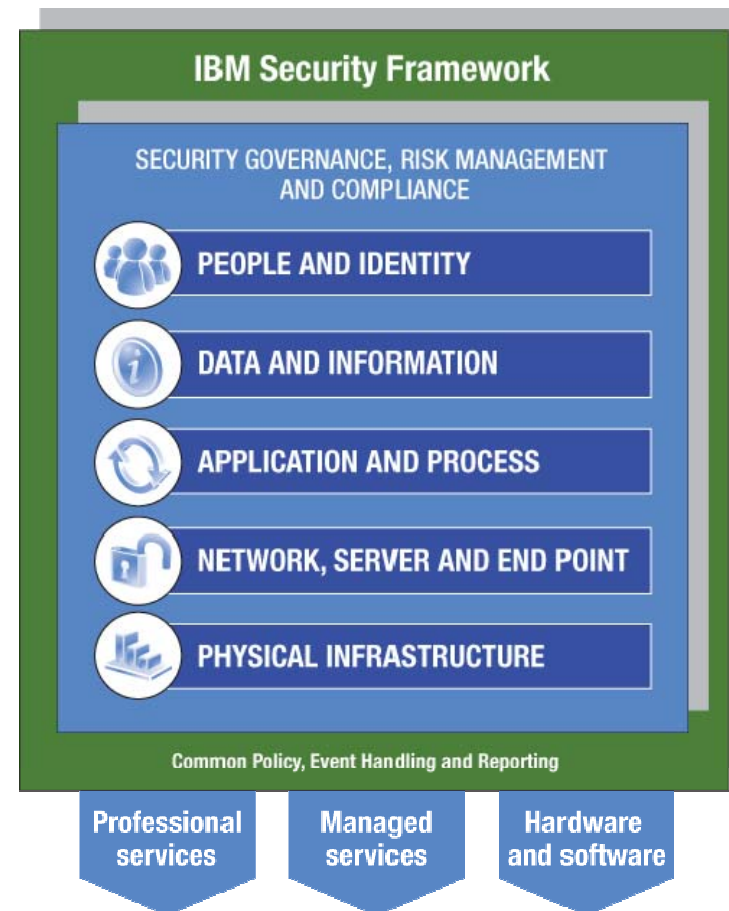
- Überblick über die gesamte Breite von Sicherheitsthemen
- Definition des notwendigen Sicherheitsniveaus
- Identifizierung von Geschäftsrisiken
- Ermittlung des Reifegrads der etablierten Sicherheitsmechanismen und Prozesse im Marktvergleich
- Maßnahmendefinition auf Basis von Best Practices
- Bereitstellungen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

← Schutzmaßnahmen

↳ Vorsorgemaßnahmen

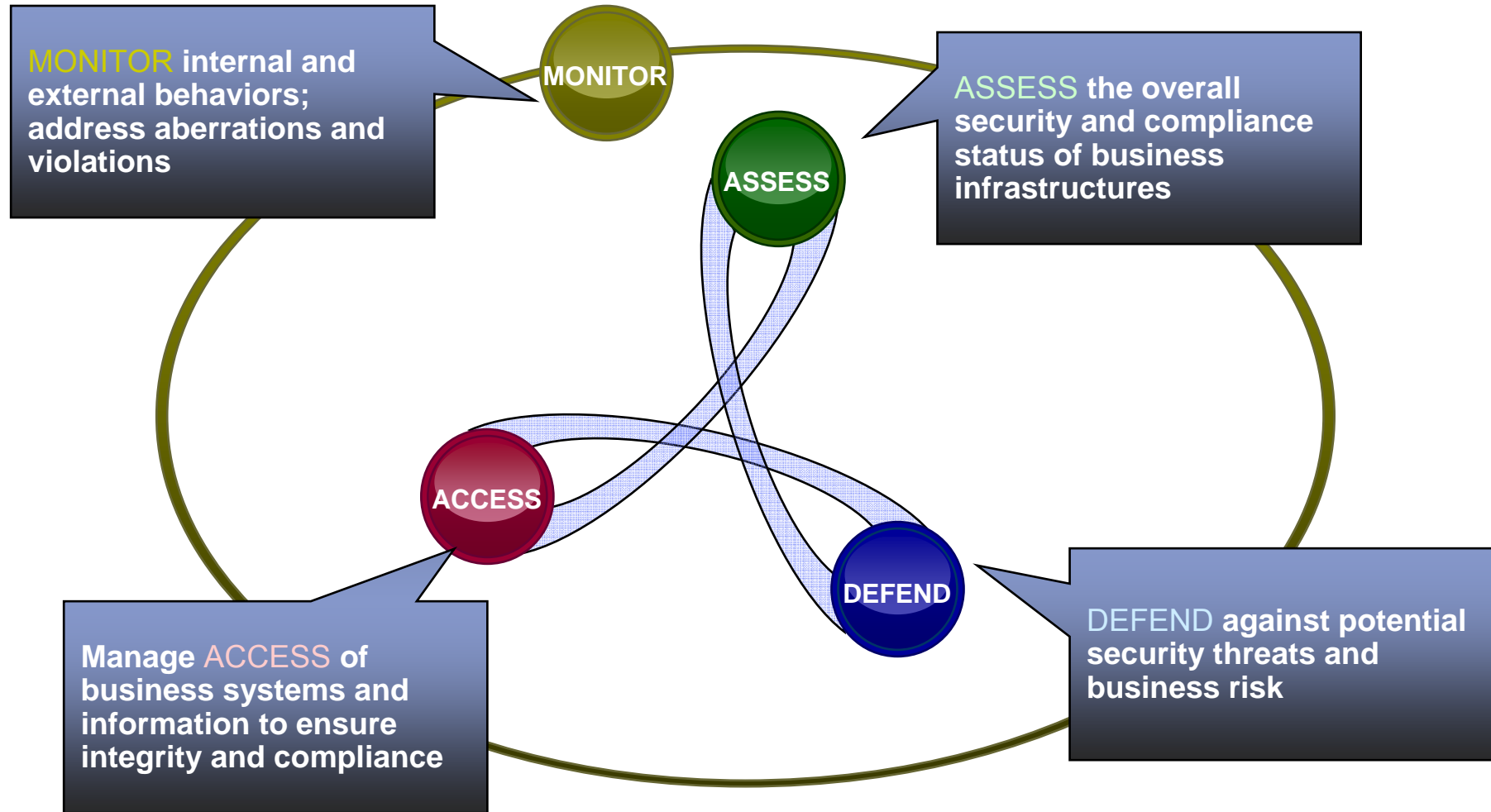
# IBM: Comprehensive Security Risk & Compliance Management

- 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

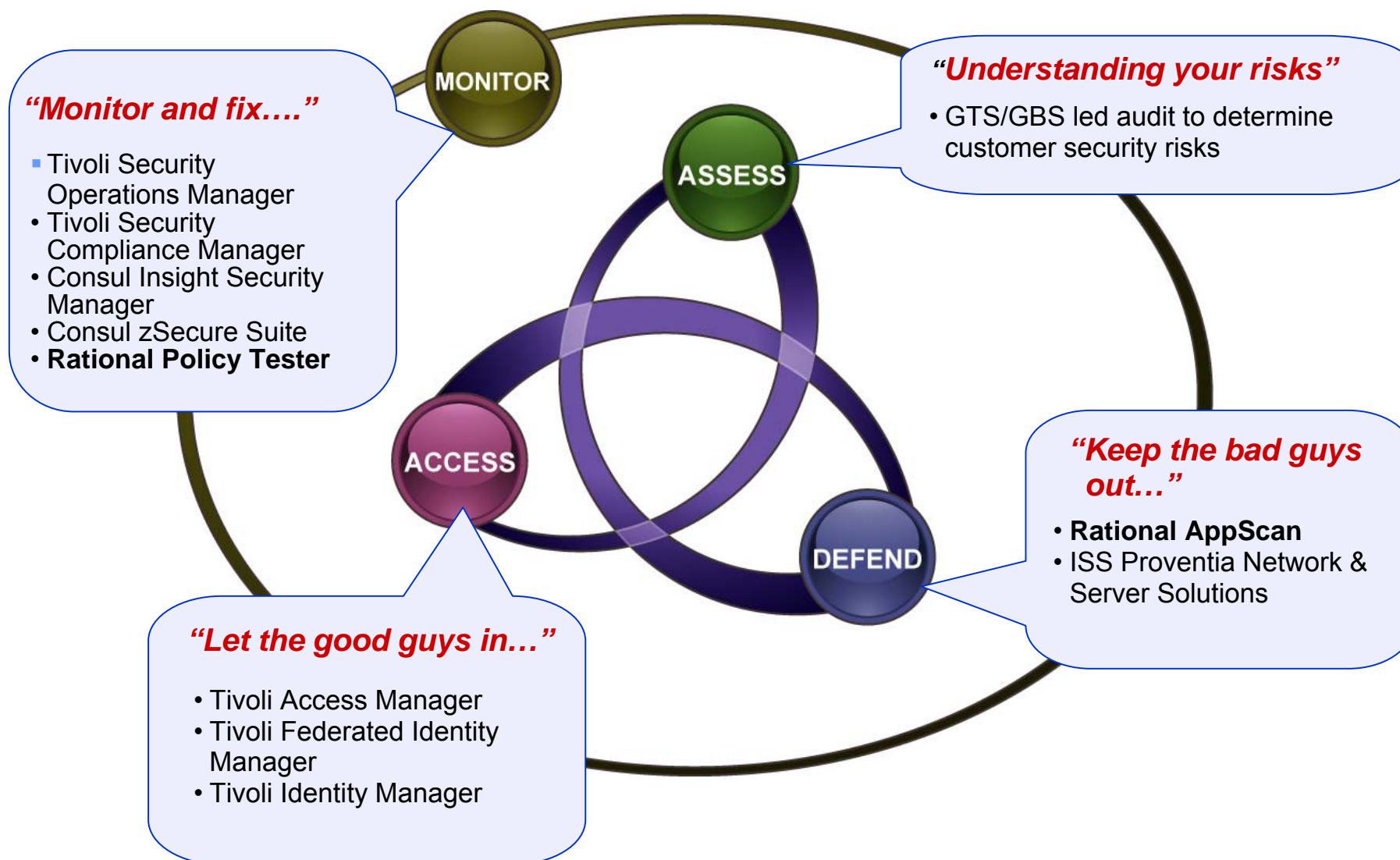




# IBM's Security Management Vision and Strategy



## 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



Security



Privacy



Quality



Standards



Compliance

## AppScan vs. Policy Tester

| IBM Rational AppScan   | IBM Rational Policy Tester   |
|--|--|
| <p>Web application and web service automated <b>Security</b> testing</p> <ul style="list-style-type: none"> <li>✓ Desktop and enterprise scalable solutions for assessing and remediating security vulnerabilities</li> <li>✓ Built for developers, testers, security professionals, and executives</li> <li>✓ Enterprise-wide reporting and tracking</li> </ul> | <p>Web Quality &amp; Compliance testing platform to monitor and manage website quality, privacy and compliance</p> <ul style="list-style-type: none"> <li>✓ Web <b>Quality</b> testing to ensure website functionality and a positive user experience</li> <li>✓ Web <b>Privacy</b> testing to meet regulatory compliance such as HIPPA, COPPA, &amp; Safe Harbor</li> <li>✓ Web <b>Accessibility</b> testing to ensure websites are available to those with disabilities and to meet compliance with Section 508 of the Rehabilitation Act</li> </ul> |

# Operationalization of Security Testing

*Customers are addressing Web Application Security in three ways:*

## 1 Enable Security Specialists

- AppScan Standard
- AppScan Enterprise

## 2 Embed Security into Development

- AppScan Developer / Build
- AppScan Tester

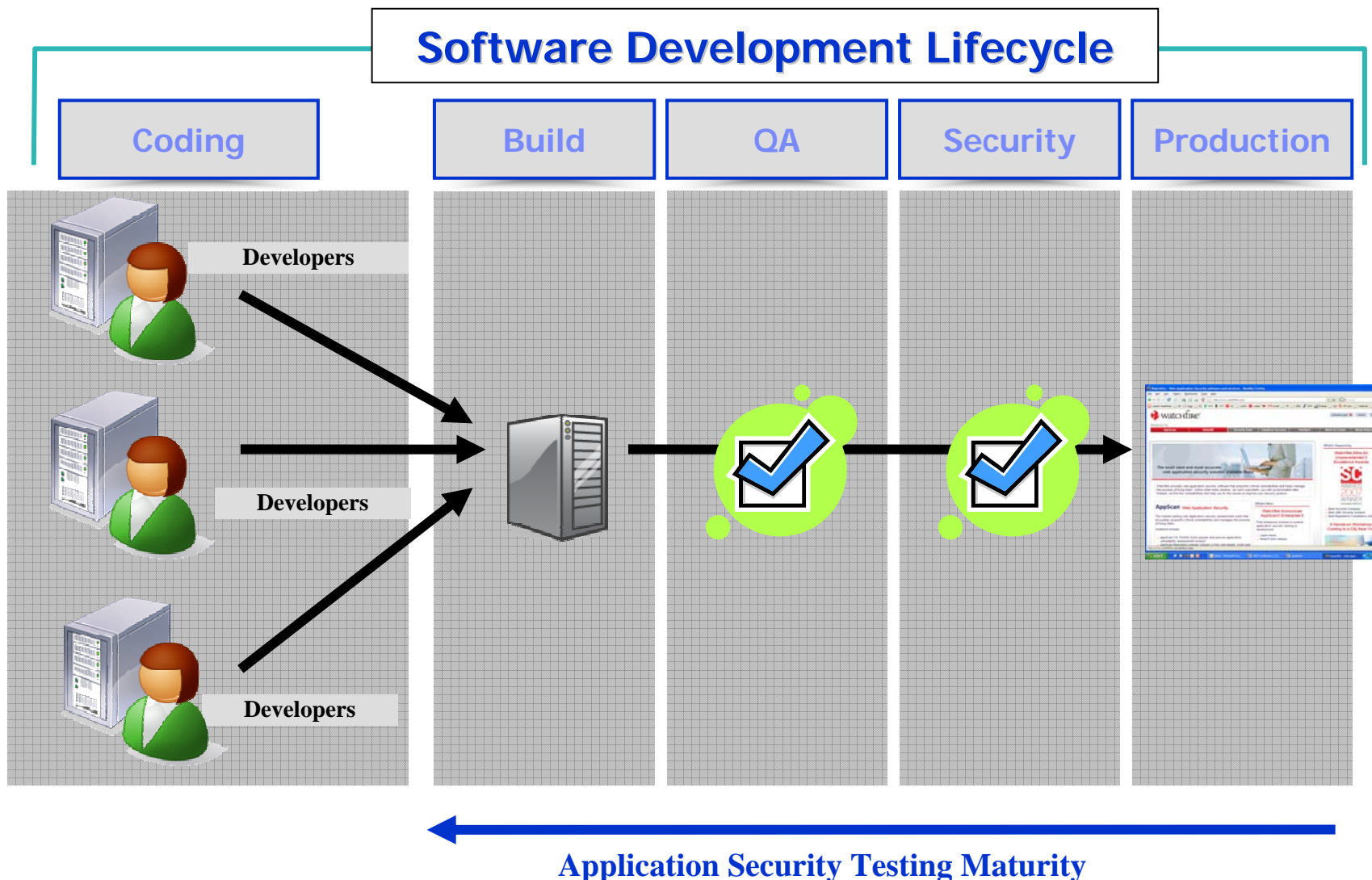
## 3 Outsource Security Testing

- AppScan OnDemand
- AppScan Security Consulting

### *Control, Monitor, Collaborate & Report Web Application Security Testing*

- AppScan Reporting Console

# Security Testing Within the Software Lifecycle



# Security Testing Within the Software Lifecycle

## Software Development Lifecycle

Production

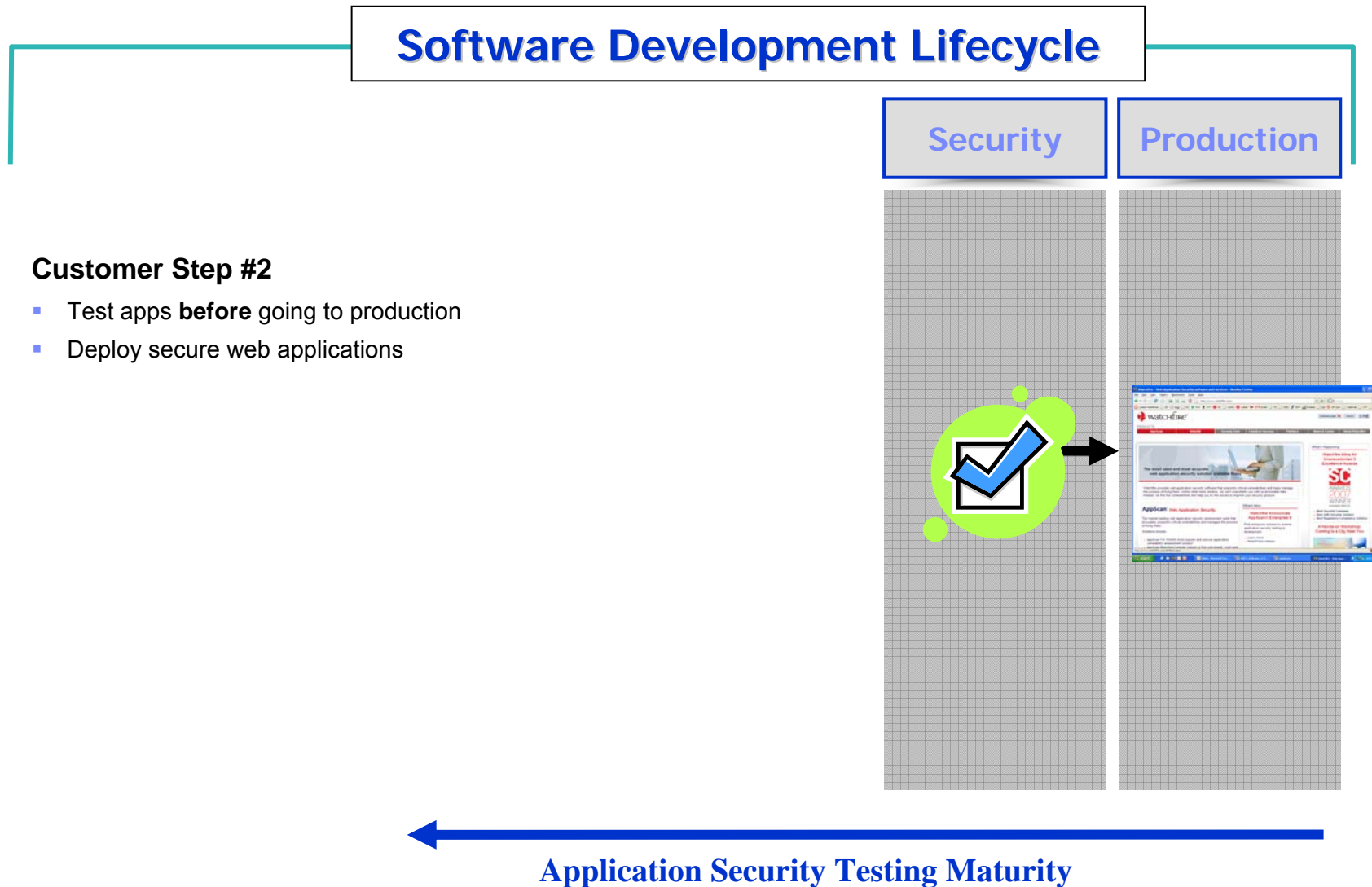
### Customer Step #1

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



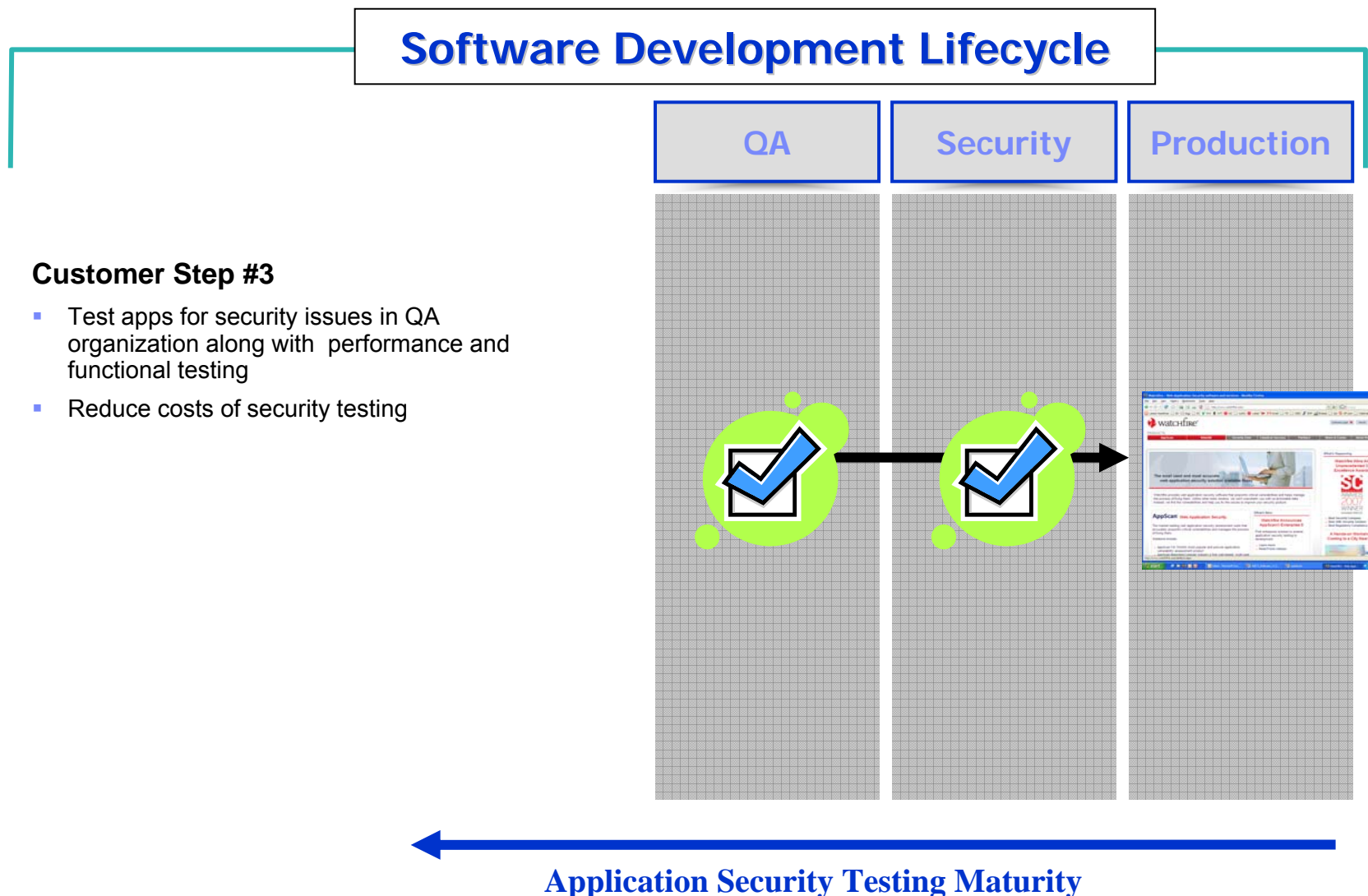
Application Security Testing Maturity

# Security Testing Within the Software Lifecycle

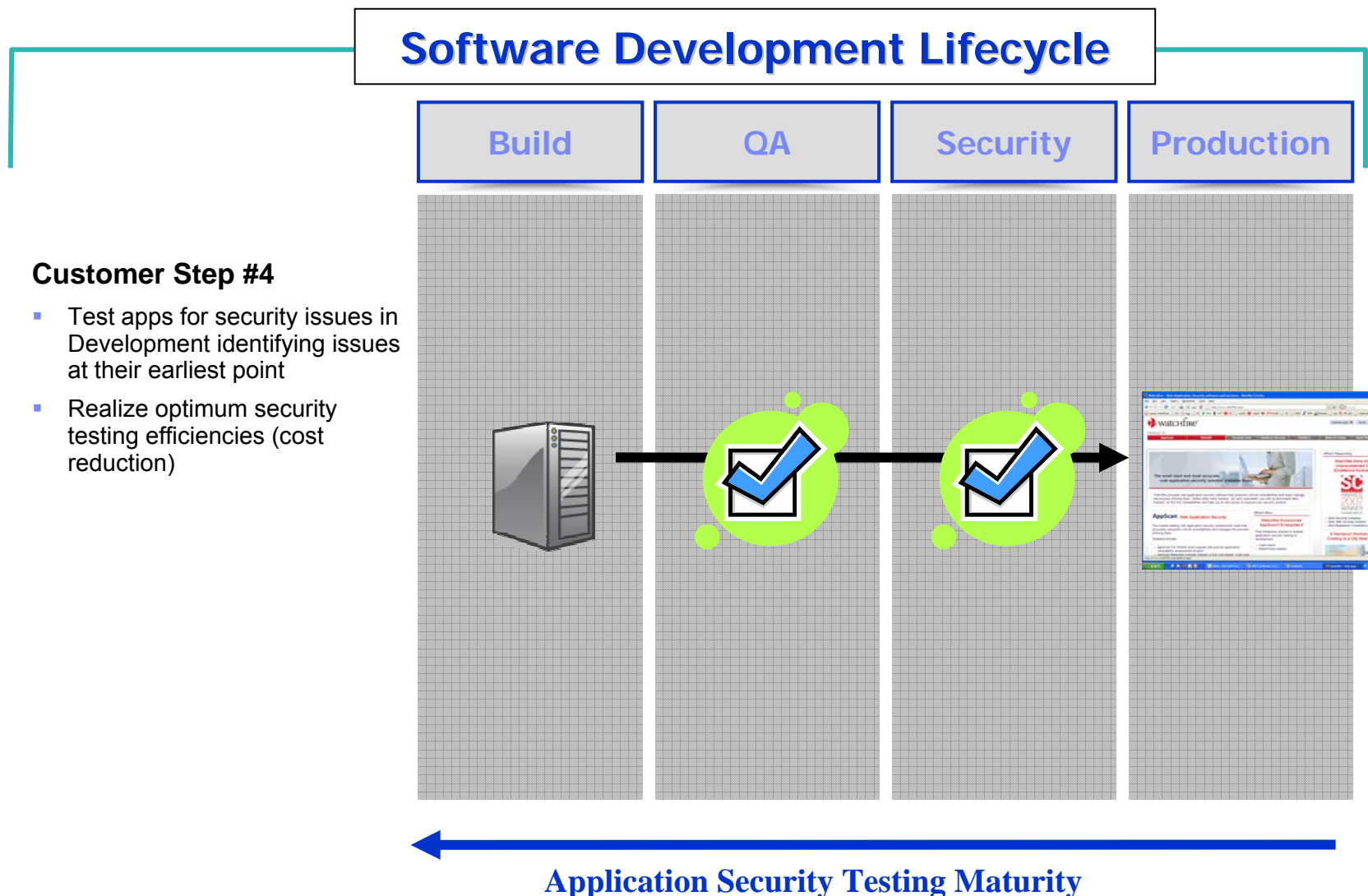




# Security Testing Within the Software Lifecycle



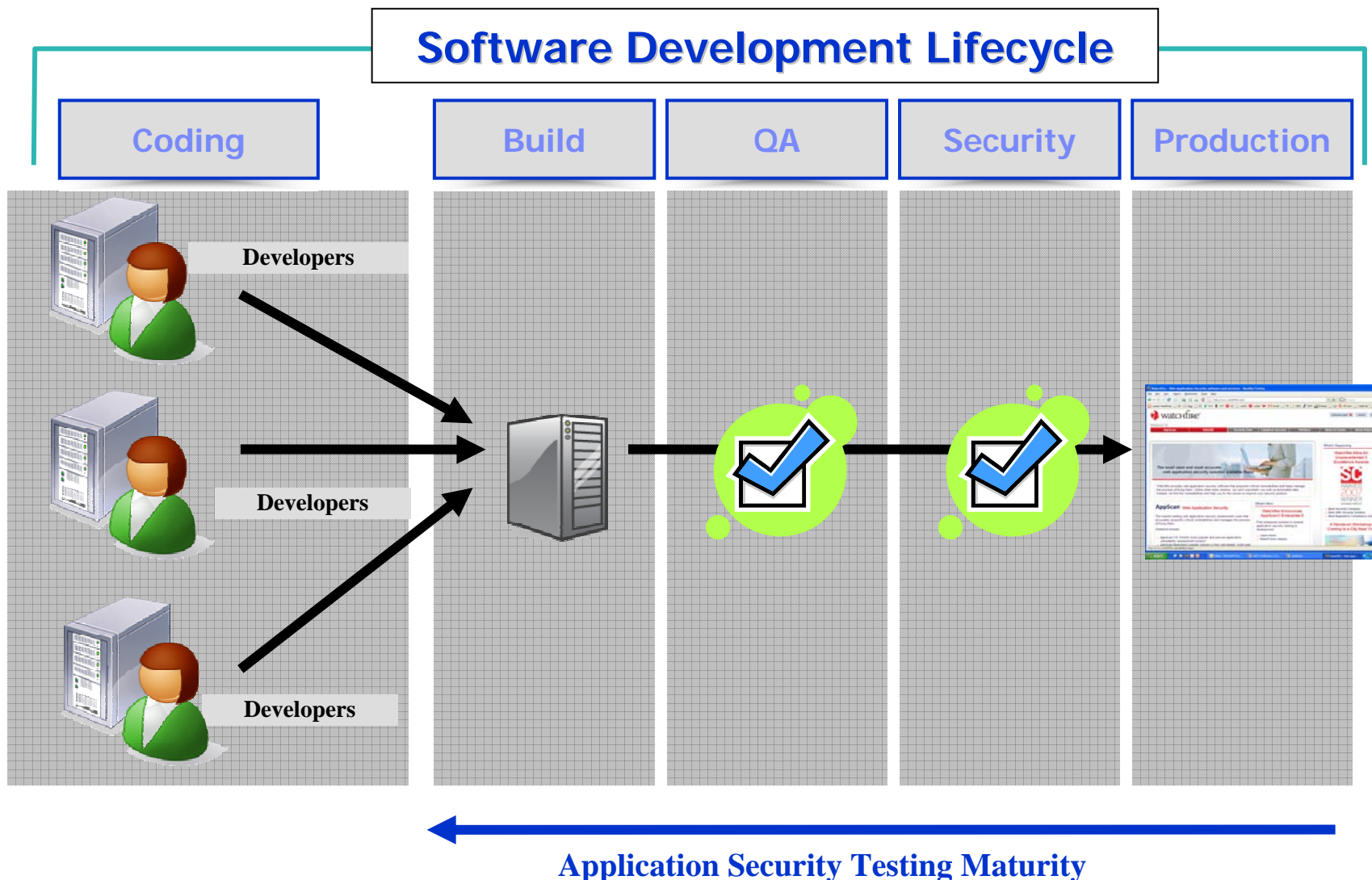
# Security Testing Within the Software Lifecycle



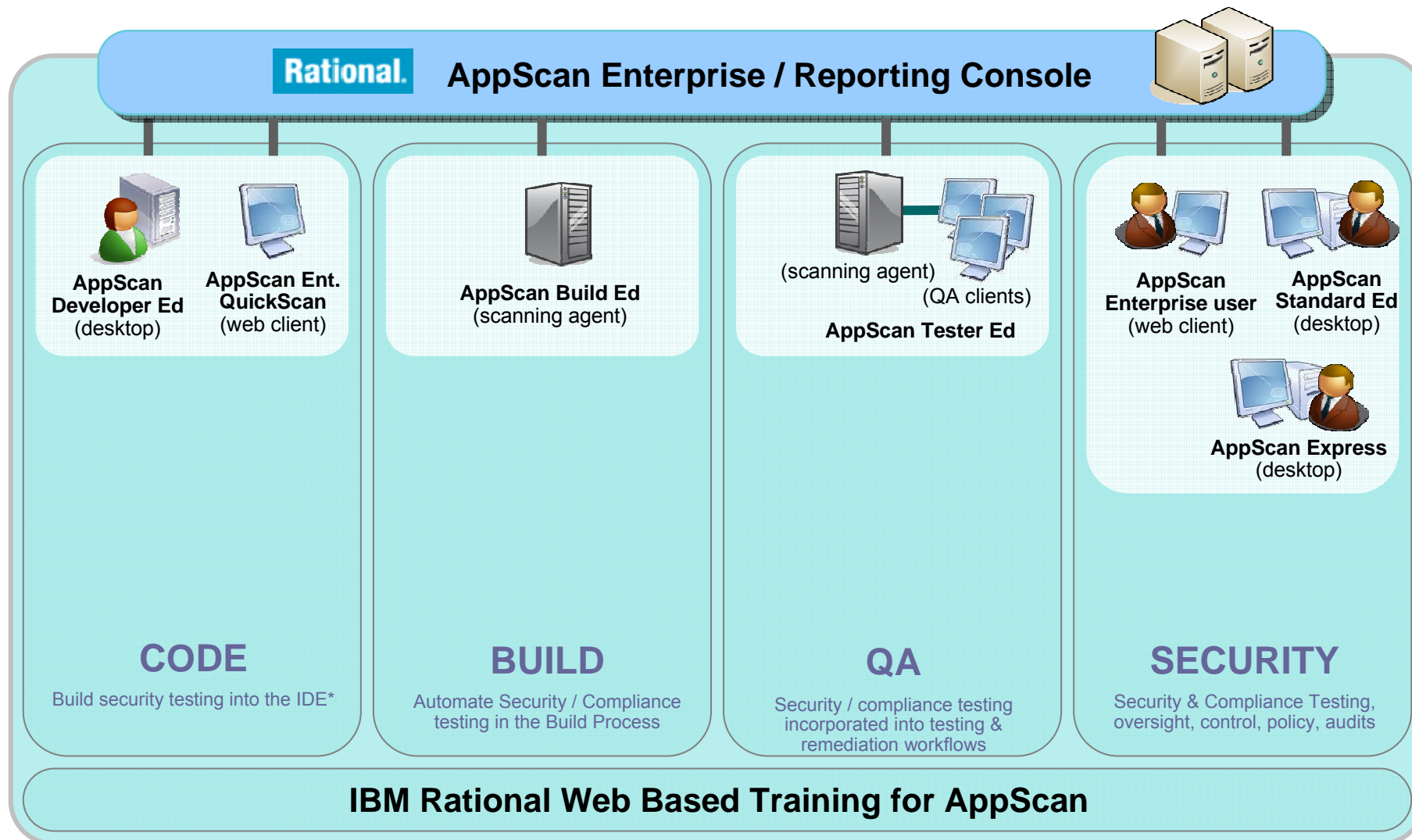
**Customer Step #4**

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

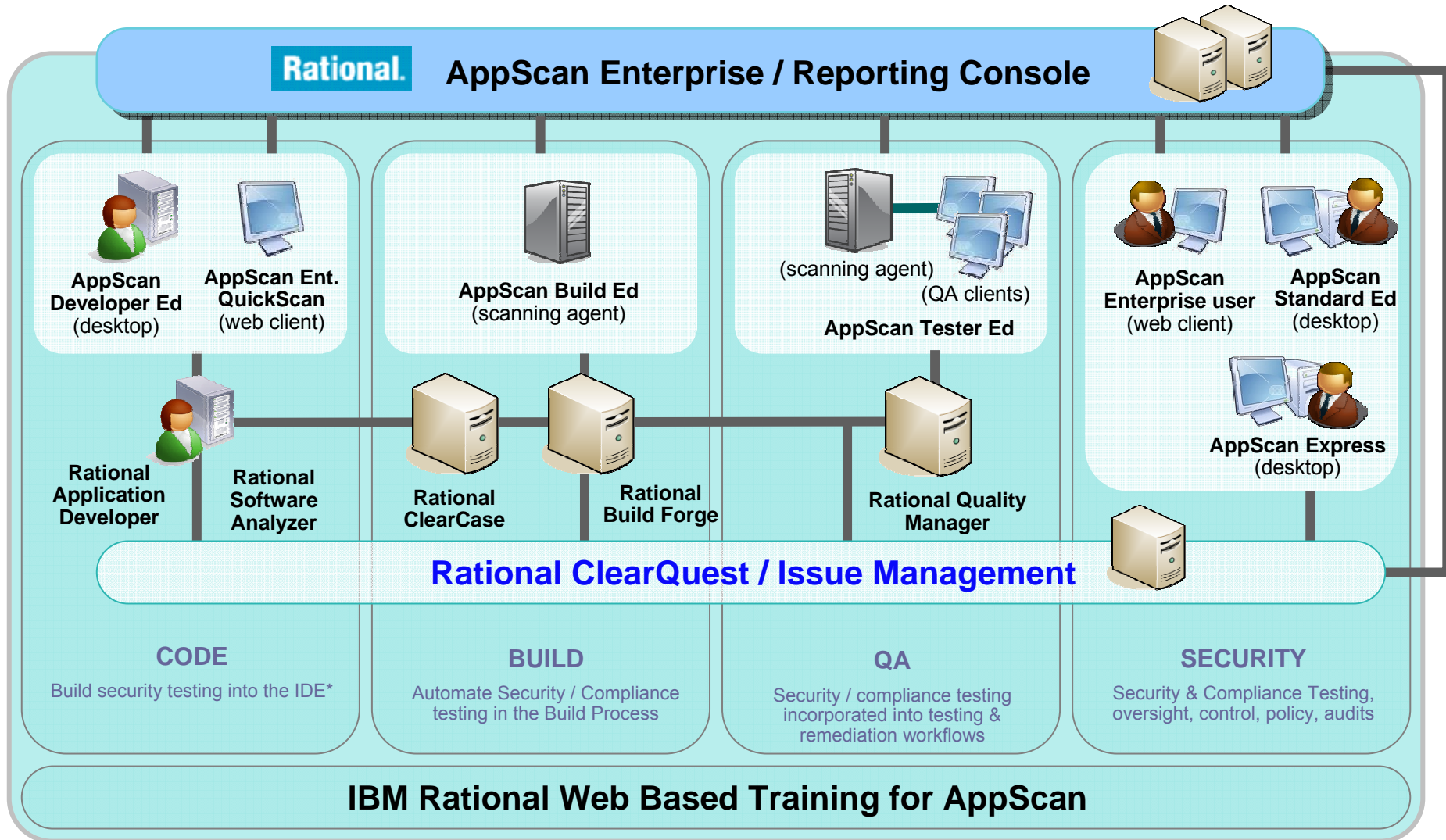
# Security Testing Within the Software Lifecycle



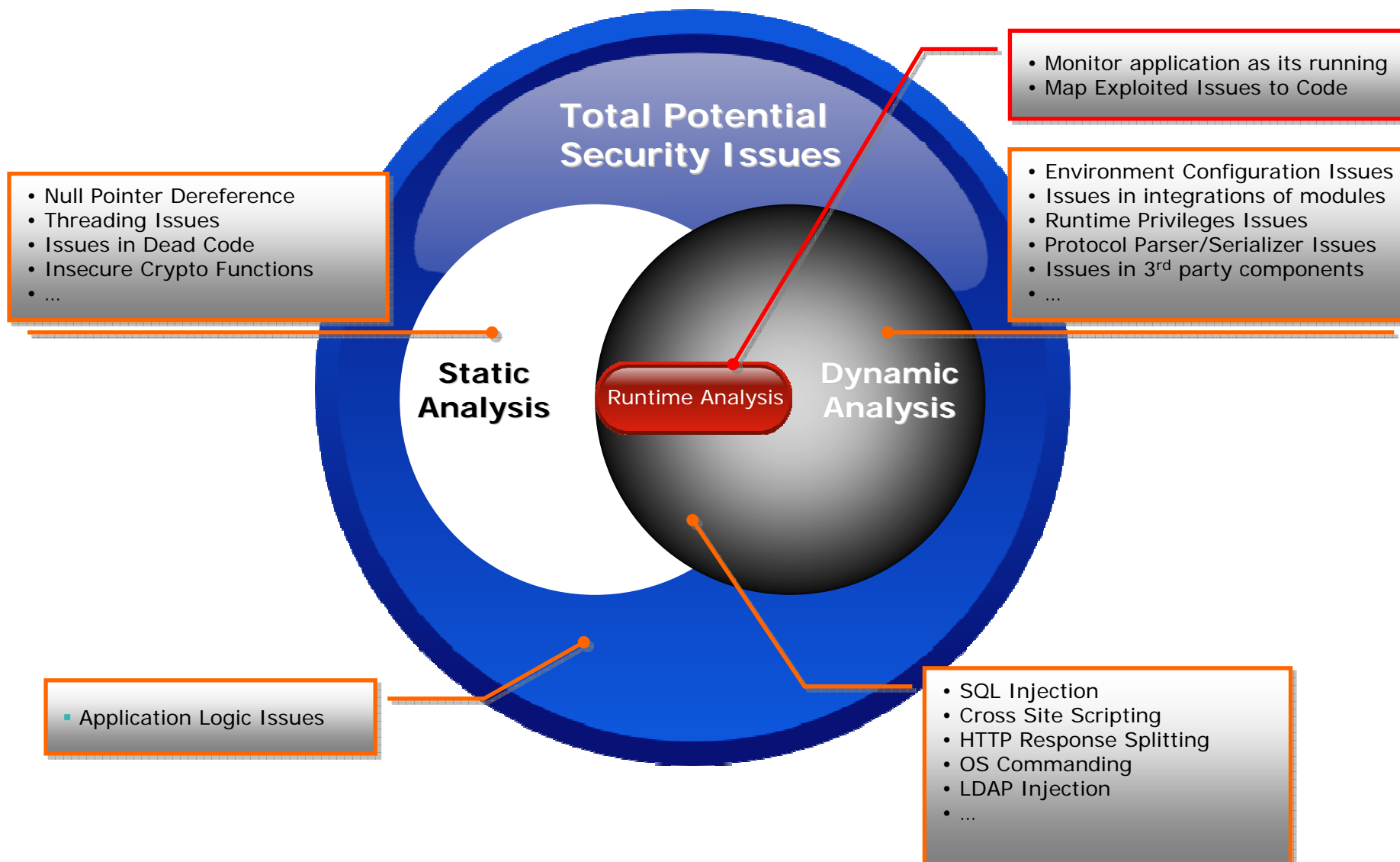
# IBM Rational AppScan Ecosystem



# IBM Rational AppScan Ecosystem



# Security Issues Coverage



# Analysis Techniques Used

## Static Code Analysis <> Whitebox

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

```

187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
    
```

## Composite Analysis

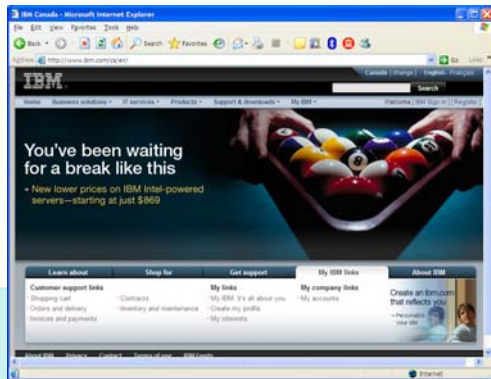
- Blend of all testing techniques for improved accuracy of reporting
- Leverage strengths and overcomes weaknesses of each individual technique

## String Analysis

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

## Dynamic Analysis <> Blackbox

- Sending tests to a functioning application

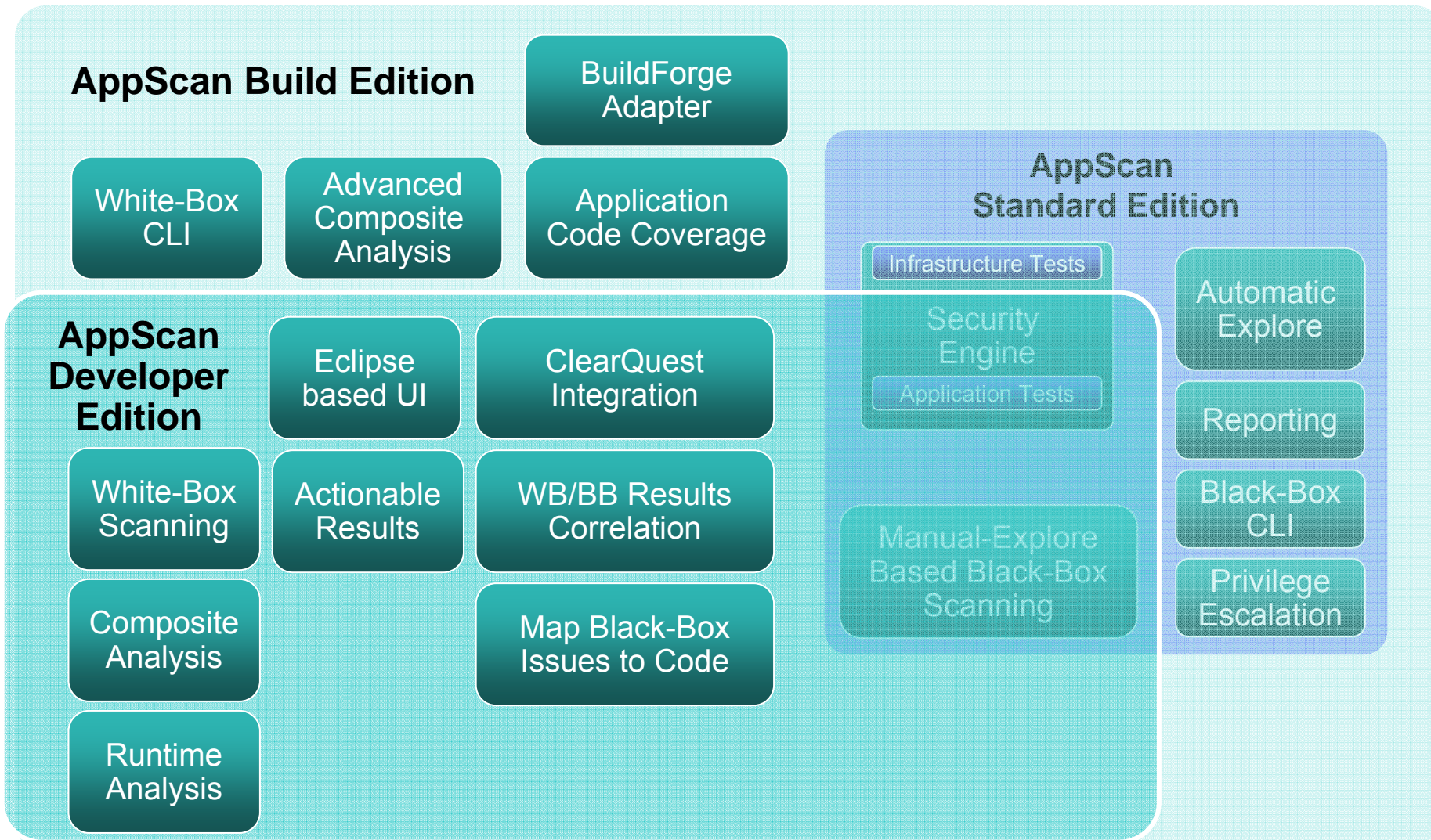


## Runtime Analysis

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

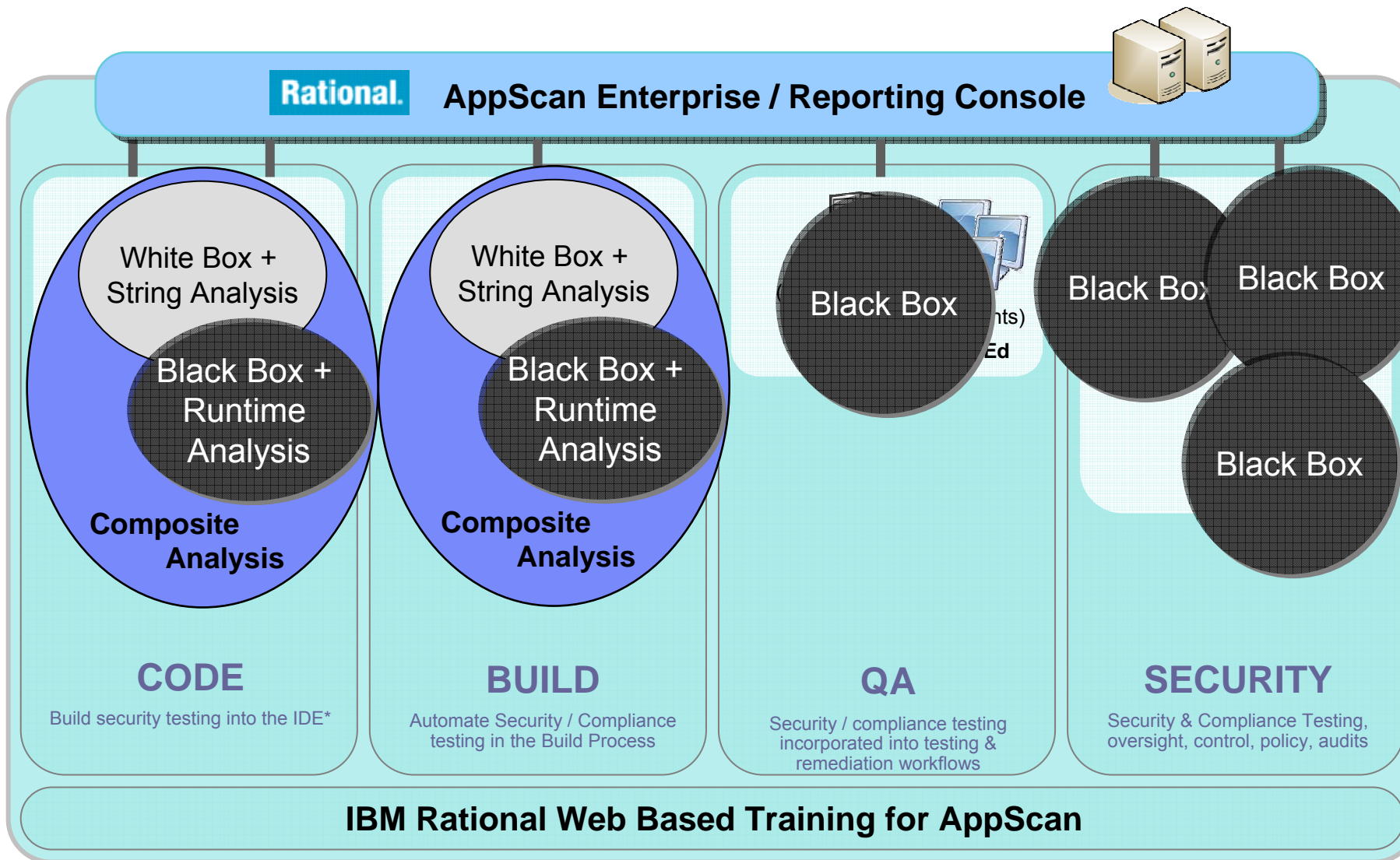


# Functionality Diagram

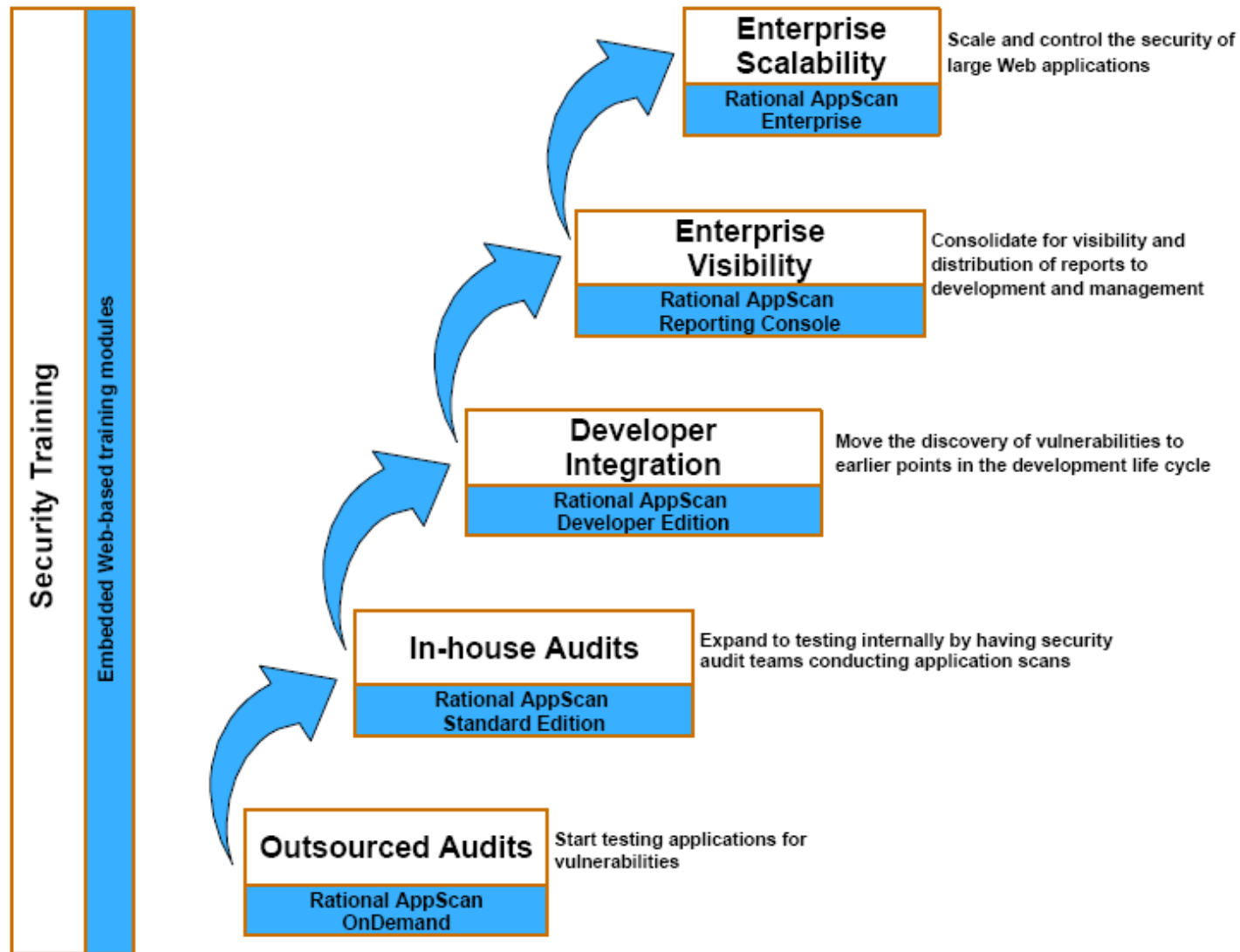




# IBM Rational AppScan Ecosystem



# 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](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](http://www.itseccity.de) (Juni 2009):

[http://www.itseccity.de/?url=/content/fachbeitraege/grundlagen/090622\\_fac\\_gru\\_isc2.html](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](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**



| IBM Software Partner Academy Program

Kontakt Daten:

**Thomas Neudert**

**Product Sales Specialist – Rational AppScan**

**Tel: 0151-11755765**

**Email: [Thomas\\_Neudert@de.ibm.com](mailto:Thomas_Neudert@de.ibm.com)**

**Vielen Dank für Ihre Aufmerksamkeit!**