



# Driving Effective Application Security in the Enterprise: An End-to-End Approach to Addressing One of the Biggest Threats to a Business

*Steven "Schmidty" Schmidt  
Application Security Technical Specialist  
IBM Security Systems*

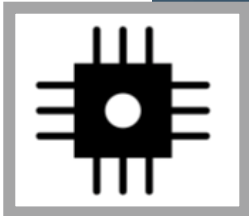
## **Pulse**2012

Meet the Experts. Optimise your infrastructure.

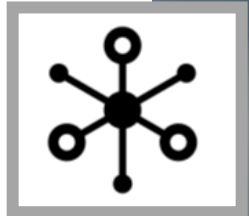
**May 31 – June 1**

Sheraton on the Park Hotel, Sydney

# The Smarter Planet



Our world is getting  
**Instrumented**



Our world is getting  
**Interconnected**



Our world is getting  
**Intelligent**



# Challenges we face on a smarter planet

## Key drivers for security projects

### Increasing Complexity



Soon, there will be **1 trillion** connected devices in the world, constituting an “internet of things”

### Rising Costs



Spending by U.S. companies on governance, risk and compliance will grow to **\$29.8 billion** in 2010

### Ensuring Compliance

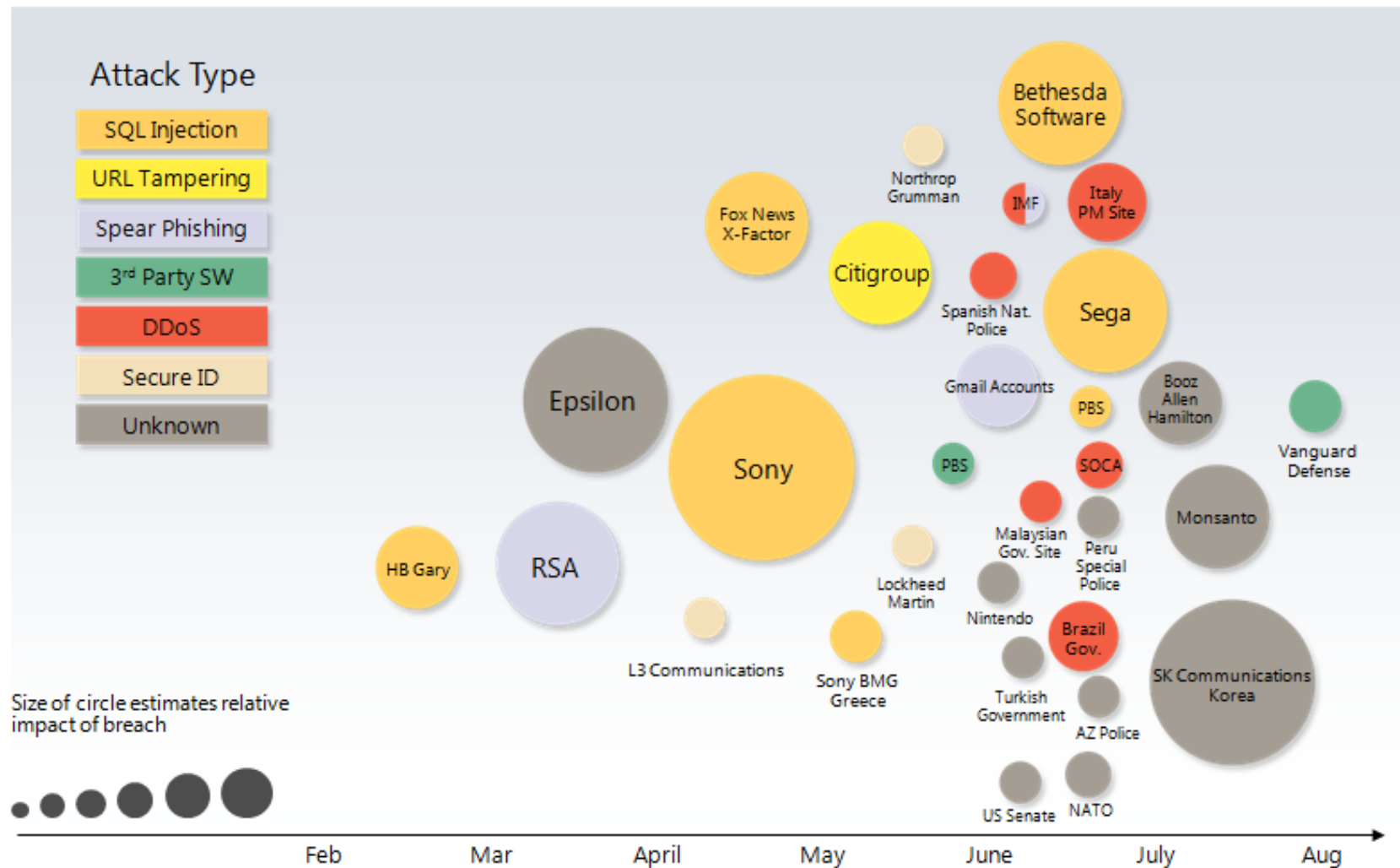


The cost of a data breach increased to **\$214** per compromised customer record

Source [http://searchcompliance.techtarget.com/news/article/0,289142,sid195\\_gci1375707,00.html](http://searchcompliance.techtarget.com/news/article/0,289142,sid195_gci1375707,00.html)

# Story Time!

# Targeted Attacks Shake Businesses and Governments



IBM Security X-Force© 2011 Midyear Trend and Risk Report September 2011

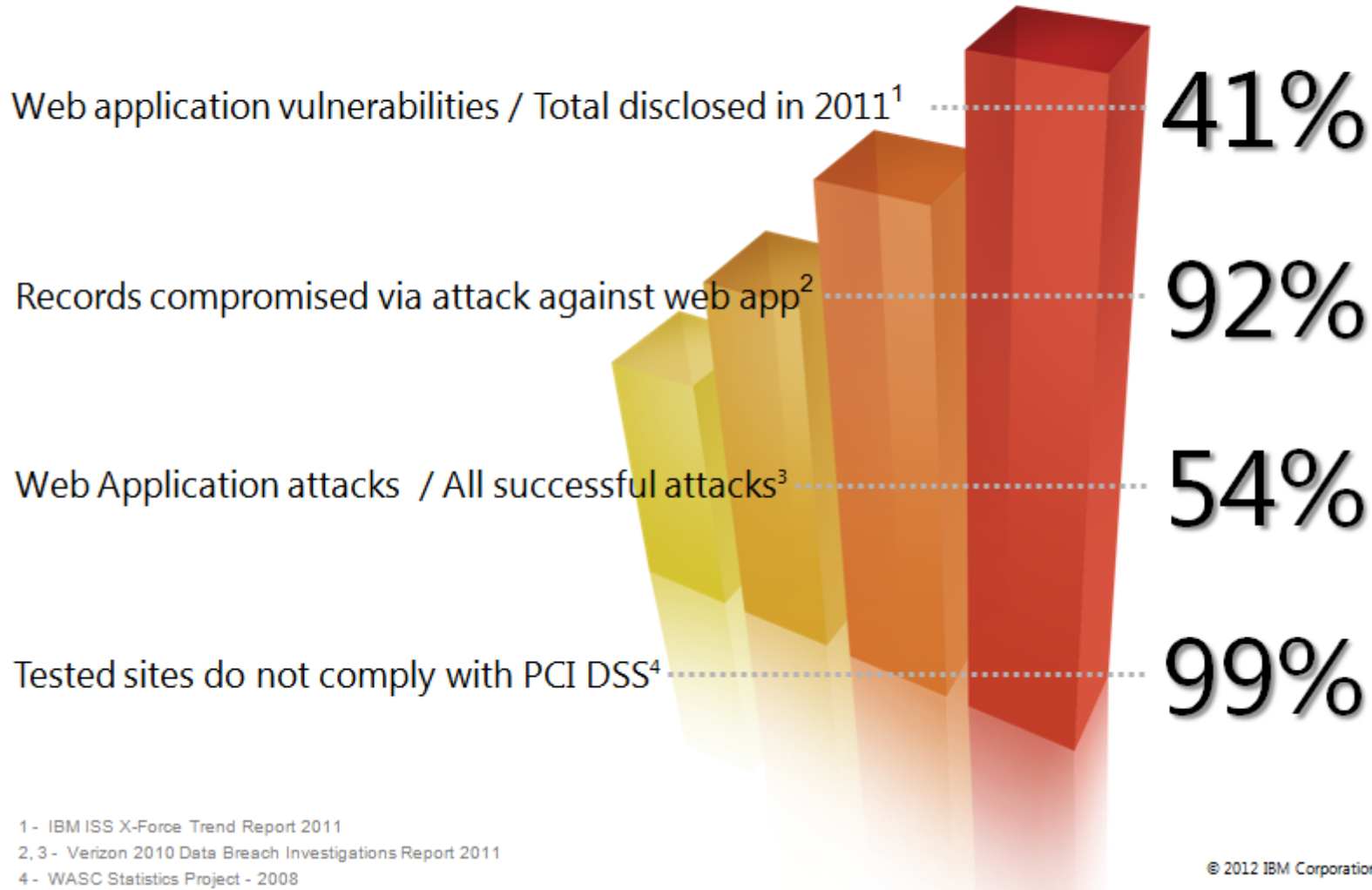
© 2012 IBM Corporation

# Web Application Vulnerabilities are still the greatest source of risk for organizations



IBM Security Systems - Application Security

## Application Security Statistics



1 - IBM ISS X-Force Trend Report 2011

2, 3 - Verizon 2010 Data Breach Investigations Report 2011

4 - WASC Statistics Project - 2008

# Application Security Market Drivers

- **Regulatory & Standards Compliance**

- eCommerce: PCI-DSS, PA-DSS
- Financial Services: GLBA
- Energy: NERC / FERC
- Government: FISMA

- **User demand Increasing Risk**

- Transformation of business processes to web applications & services
- Rich application demand is pushing development to advanced code techniques – Web 2.0 introducing more exposures

- **Cost efficiencies**

- Mitigate organizational risk with positive return on investment



"As attackers identify new ways to gain access to sensitive data, managing application security has become a big problem for our clients, and companies need solutions to proactively identify and fix vulnerabilities in their applications and comply with more and more regulations,"

***Joey Peloquin, Director, Application Security,  
Fishnet Security.***

# Why Are Applications So Vulnerable?



Time to market, priorities



Lack of security education



Complexity



Interconnectivity



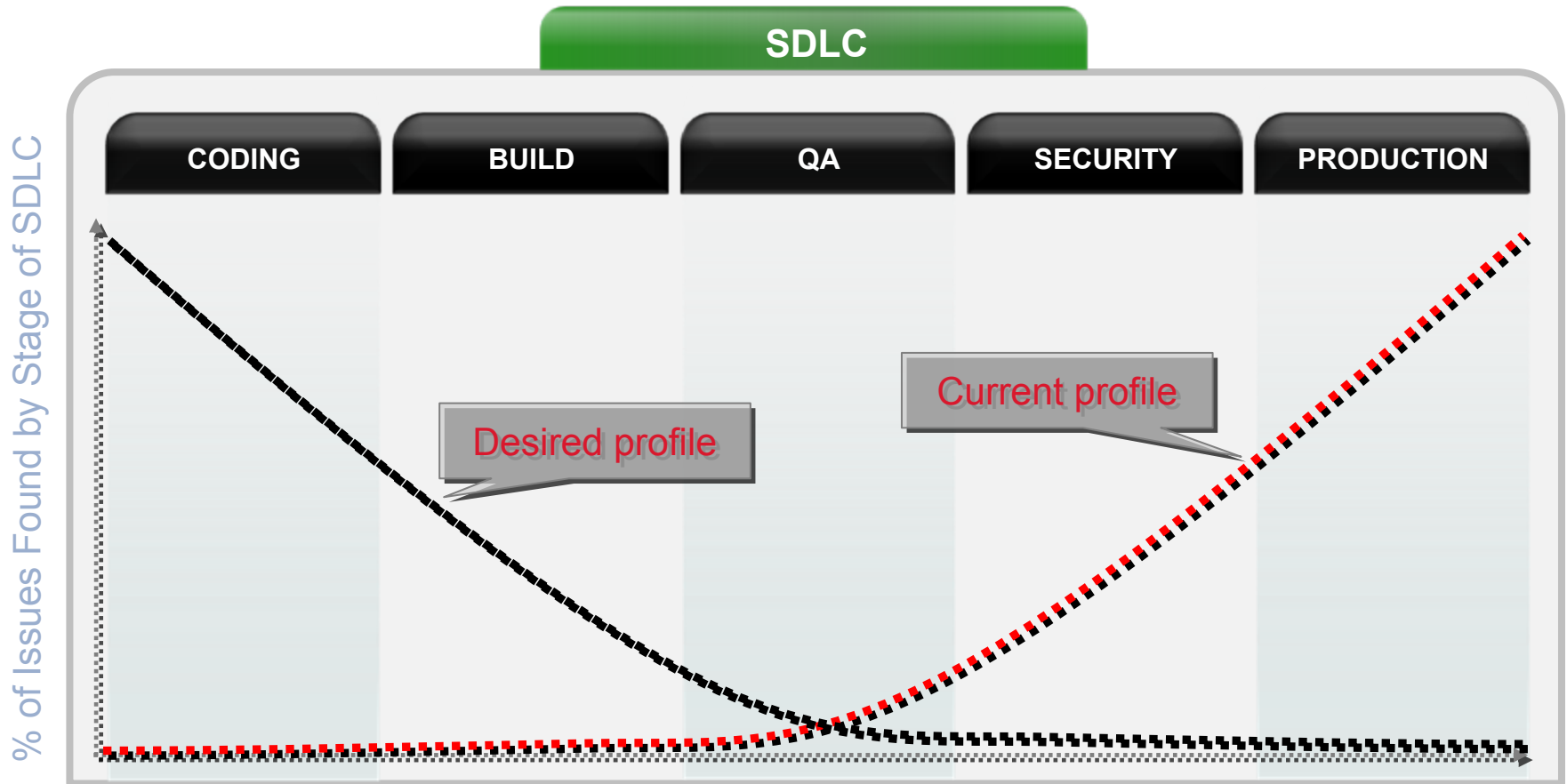
Network protections are not enough



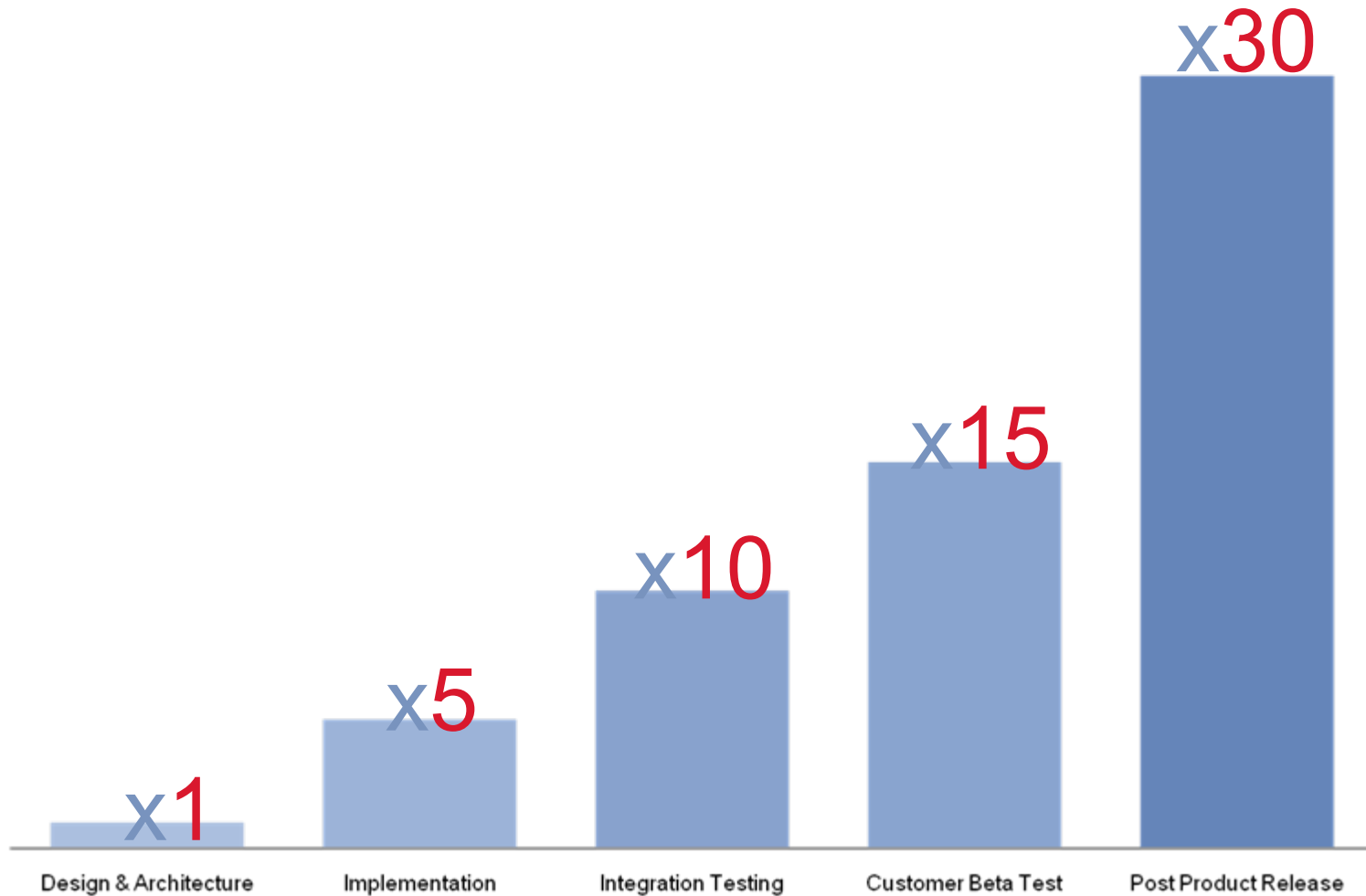


**More Story Time!**

# Security Testing Within the App Lifecycle



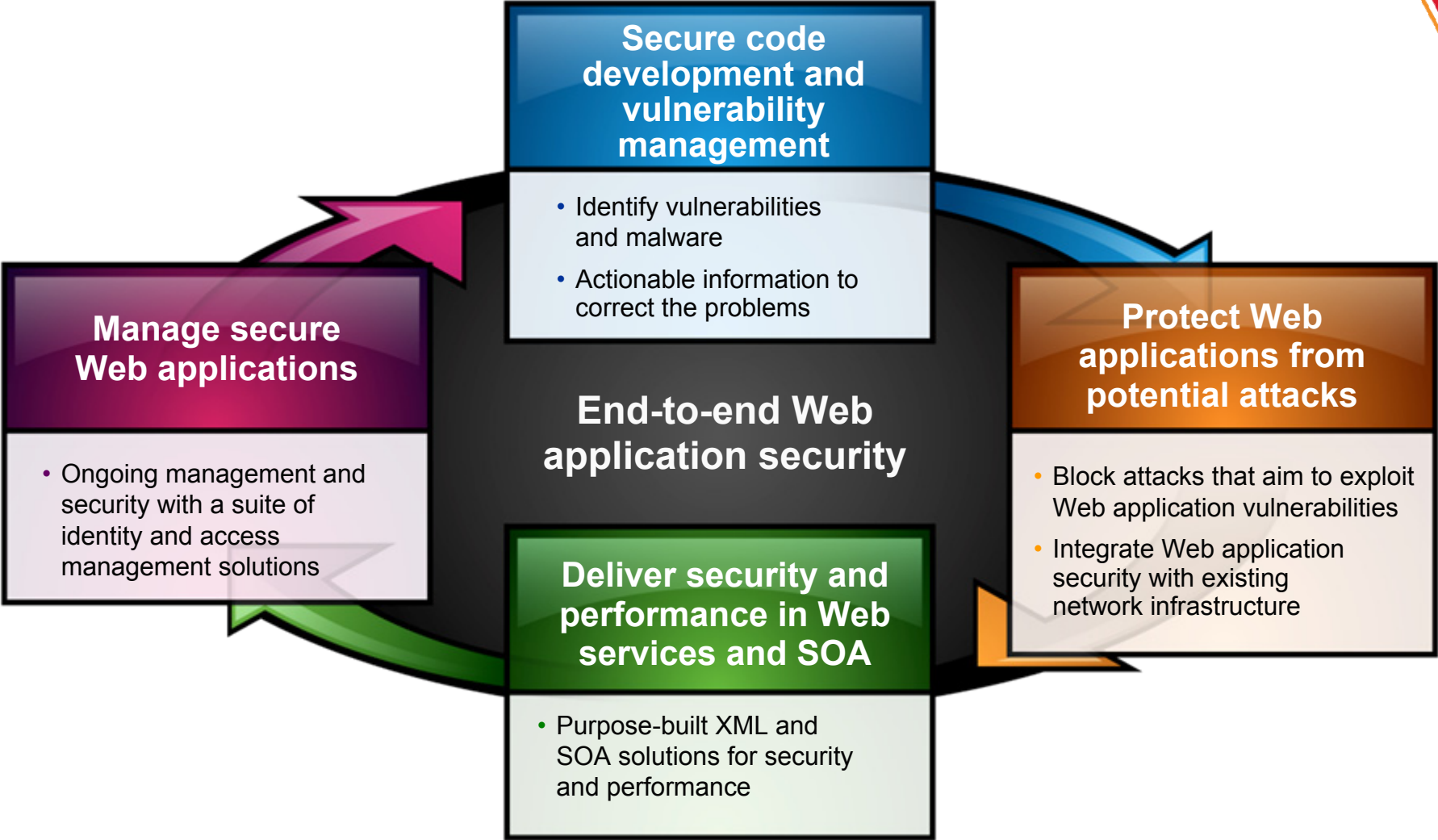
# Cost of fixing software defects: The Artist formerly known as Security Issues



The Economic Impacts of Inadequate Infrastructure for Software Testing (NIST, 2002)



# Application Safety – Protect Valuable Assets



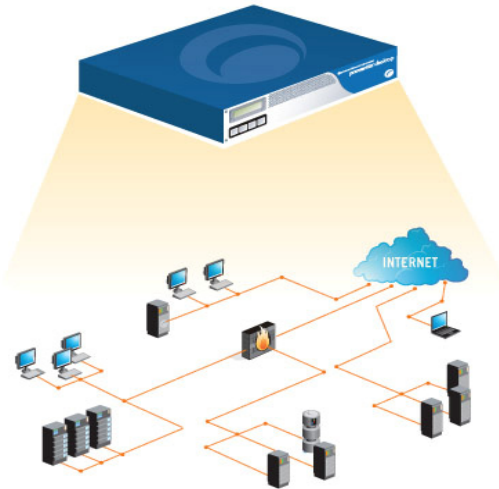


# How does IBM Security AppScan work?

## Automates Application Security Testing Same process for whitebox & blackbox

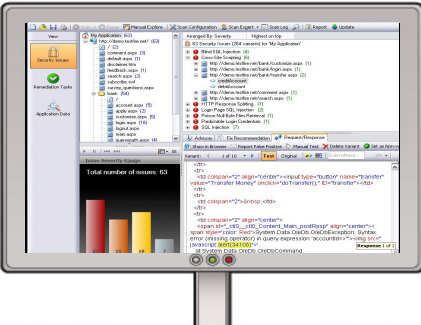
1

Scan applications



2

Analyze  
(identify issues)



Virtual-SOC Portal

3

Report  
(detailed & actionable)





# Security Testing Technologies...

## Combination Drives Greater Solution Accuracy

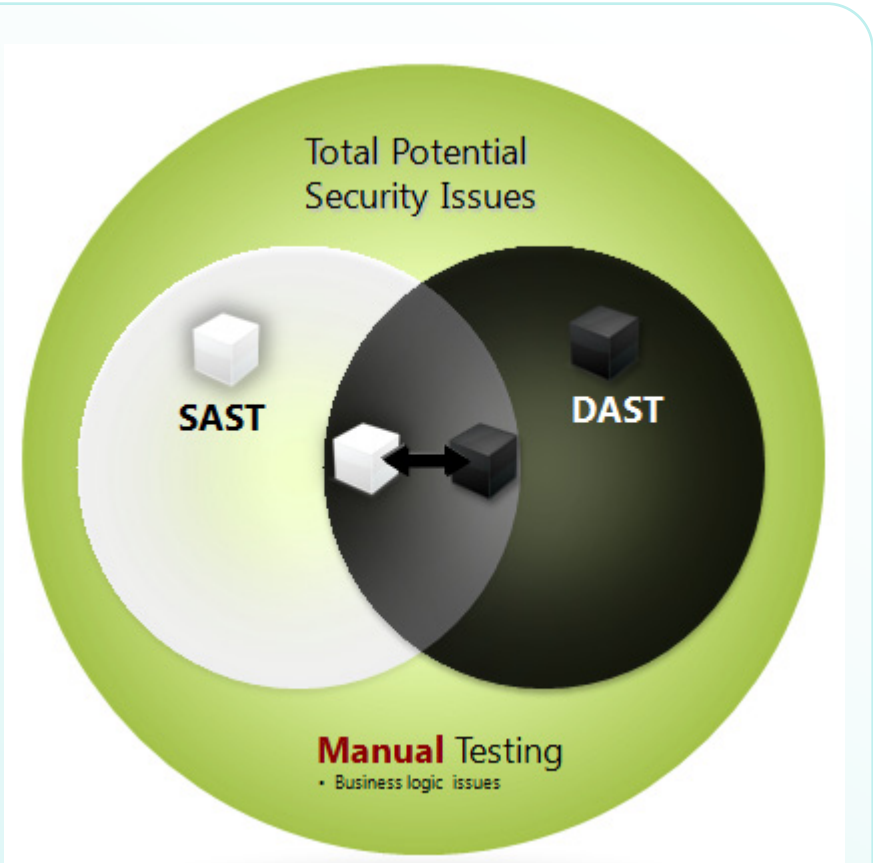
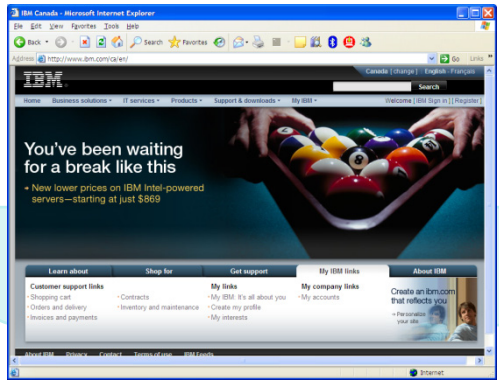
### Static Code Analysis (Whitebox )

- Scanning source code for security

```
104 /
105 /
106 /
107 /
108 /
109 /
110 /
111 /
112 /
113 /
114 /
115 /
116 /
117 /
118 /
119 /
120 /
121 /
122 /
123 /
124 /
125 /
126 /
127 /
128 /
129 /
130 /
131 /
132 /
133 /
134 /
135 /
136 /
137 /
138 /
139 /
140 /
141 /
142 /
143 /
144 /
145 /
146 /
147 /
148 /
149 /
150 /
151 /
152 /
153 /
154 /
155 /
156 /
157 /
158 /
159 /
160 /
161 /
162 /
163 /
164 /
165 /
166 /
167 /
168 /
169 /
170 /
171 /
172 /
173 /
174 /
175 /
176 /
177 /
178 /
179 /
180 /
181 /
182 /
183 /
184 /
185 /
186 /
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 /
```

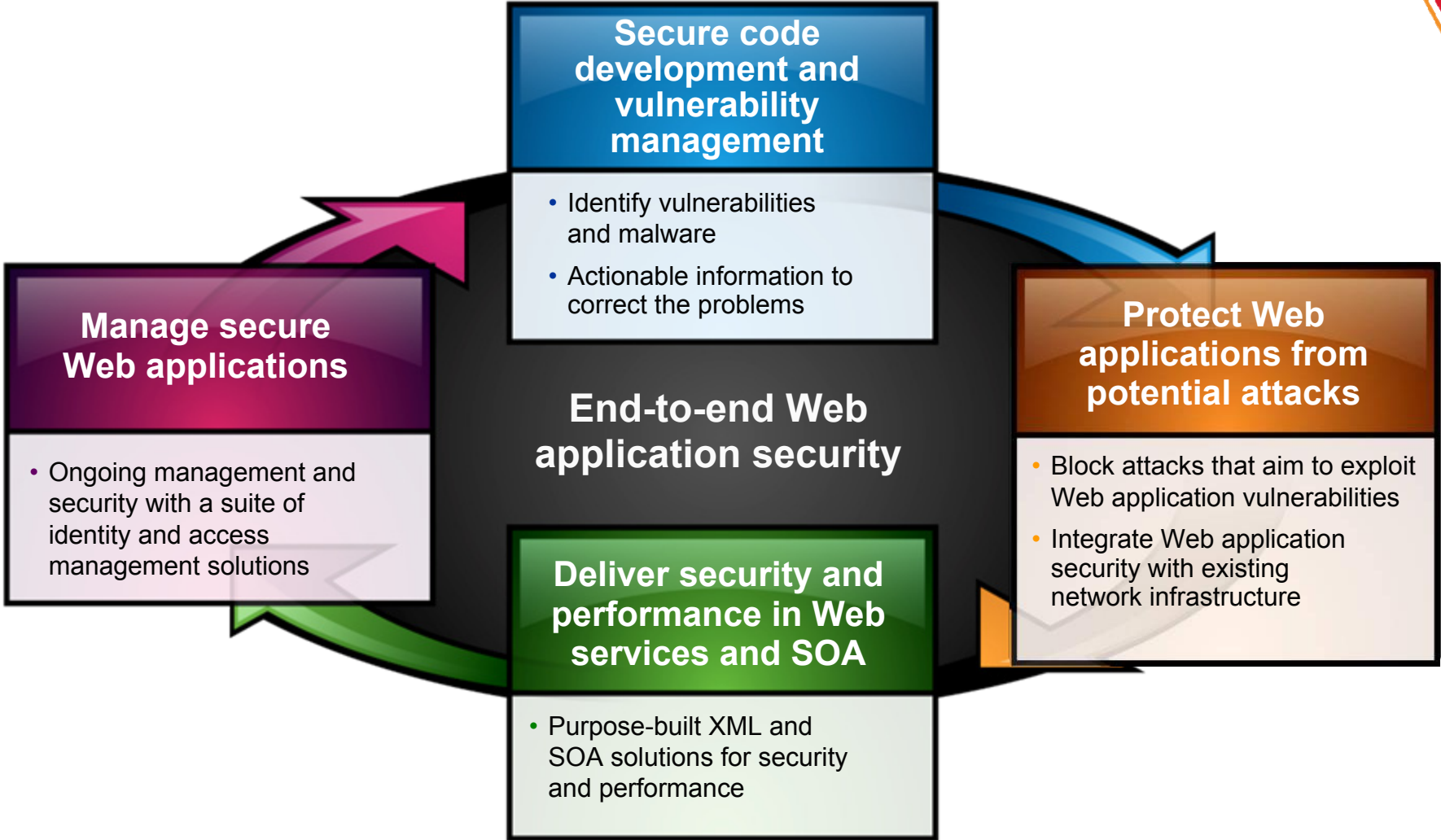
### Dynamic Analysis (Blackbox)

- Performing security analysis of a compiled application





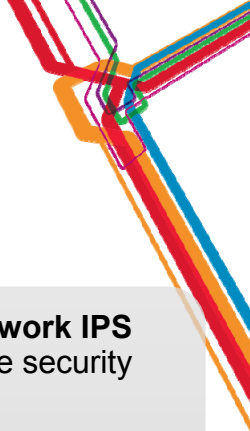
# Protecting Deployed Applications in Real-time





**Yep, another story...**





# IBM Security Network Intrusion Prevention System



**Beyond traditional network IPS** to deliver comprehensive security including:

- Web application protection
- Protection from client-side attacks
- Data Loss Prevention (DLP)
- Granular policy control for virtual environments
- Application control
- Virtual Patch technology

**Unmatched Performance** through PAM 2.0 delivering 20Gbps+ of throughput and 10GbE connectivity without compromising breadth and depth of security

**Evolving protection** powered by world renowned X-Force research to stay “ahead of the threat”

**Reduced cost and complexity** through consolidation of point solutions and integrations with other security tools

Virtual Patch

Client-side Application Protection

Web Application Protection

Threat Detection and Prevention

Data Security

Application Control



# Evolving Security: The Protocol Analysis Module

### How it Works

- Deep inspection of network traffic
- Identifies & analyzes >200 network and application layer protocols and data file formats

### What it Prevents

- Worms
- Spyware
- P2P
- DoS/DDoS
- Cross-site Scripting
- SQL Injection
- Buffer Overflow
- Web Directory Traversal

### Protocol Analysis Module (PAM)

Vulnerability Modeling & Algorithms	RFC Compliance
Stateful Packet Inspection	TCP Reassembly & Flow Reassembly
Protocol Anomaly Detection	Statistical Analysis
Port Variability	Host Response Analysis
Port Assignment	IPv6 Native Traffic Analysis
Port Following	IPv6 Tunnel Analysis
Protocol Tunneling	SIT Tunnel Analysis
Application-Layer Pre-Processing	Port Probe Detection
Shellcode Heuristics	Pattern Matching
Context Field Analysis	Custom Signatures
Proventia Content Analyzer	Injection Logic Engine

### NEW - Introducing PAM 2.0

- Takes advantage of next generation hardware
- Provides multi-threaded security inspection
- Delivers unprecedented levels of performance without compromising security

# Maintaining High Levels of Pre-emptive Protection

IBM X-Force®

Research and Development Team

- Research and evaluate threat and protection issues
- Deliver security protection for today's security problems
- Develop new technology for tomorrow's security challenges
- Educate the media and user communities



**14B** analyzed Web pages & images

**40M** spam & phishing attacks

**54K** documented vulnerabilities

**Billions** of intrusion attempts daily

**Millions** of unique malware samples

Provides Specific Analysis of:

- Vulnerabilities/Exploits
- Malicious/Unwanted websites
- Spam and Phishing
- Malware
- Other emerging trends

# A Look at IBM's Web Protection Module



- Detects/blocks wide range of Web application attacks
- Critical such as SQL Injection and Cross-site Scripting/CSRF
- Path Traversal, Brute Force, and many more

Web Protection Shared Tuning

Protection Domain: Global

Web Protection Categories:

	Enabled	Category
<input type="checkbox"/>	<input type="checkbox"/>	Client-side Attacks
<input type="checkbox"/>	<input type="checkbox"/>	Injection Attacks
<input type="checkbox"/>	<input type="checkbox"/>	Malicious File Execution
<input type="checkbox"/>	<input type="checkbox"/>	Cross-site Request Forgery (CSRF)
<input type="checkbox"/>	<input type="checkbox"/>	Information Disclosure
<input type="checkbox"/>	<input type="checkbox"/>	Path Traversal
<input type="checkbox"/>	<input type="checkbox"/>	Authentication
<input type="checkbox"/>	<input type="checkbox"/>	Buffer Overflow
<input type="checkbox"/>	<input type="checkbox"/>	Brute Force
<input type="checkbox"/>	<input type="checkbox"/>	Directory Indexing
<input type="checkbox"/>	<input type="checkbox"/>	Miscellaneous Attacks

Rolling Packet Capture Settings

Client-side Attacks

Show Security Events...

Enabled

Attack techniques that exploit the trust relationship between a user and the Web sites they visit, such as

Ignore Event

Display:

Block

Log Evidence

Responses:

Email Quarantine

Security Events for 'Client-side Attacks'

- Cross\_Site\_Scripting
- HTTP\_Apache\_Expect\_XSS
- HTTP\_Apache\_OnError\_XSS
- HTTP\_Cross\_Site\_Scripting
- HTTP\_GETscript
- HTTP\_HTML\_Tag\_Injection
- HTTP\_Html\_In\_Ref
- HTTP\_IFRAME\_Tag\_Injection
- HTTP\_MCMS\_CrossSiteScripting
- HTTP\_MSIS\_Script
- HTTP\_Nfuse\_Script
- HTTP\_POST\_Script
- HTTP\_Share\_Point\_XSS

Close

Home Appliance Dashboard Monitor Health and S

Security Modules

- Data Loss Prevention
- **Web Application Protection**
- X-Force Virtual Patch

Advanced IPS

- Security Events
- User Defined Events
- Open Signatures
- Protection Domains
- Connection Events
- Tuning Parameters



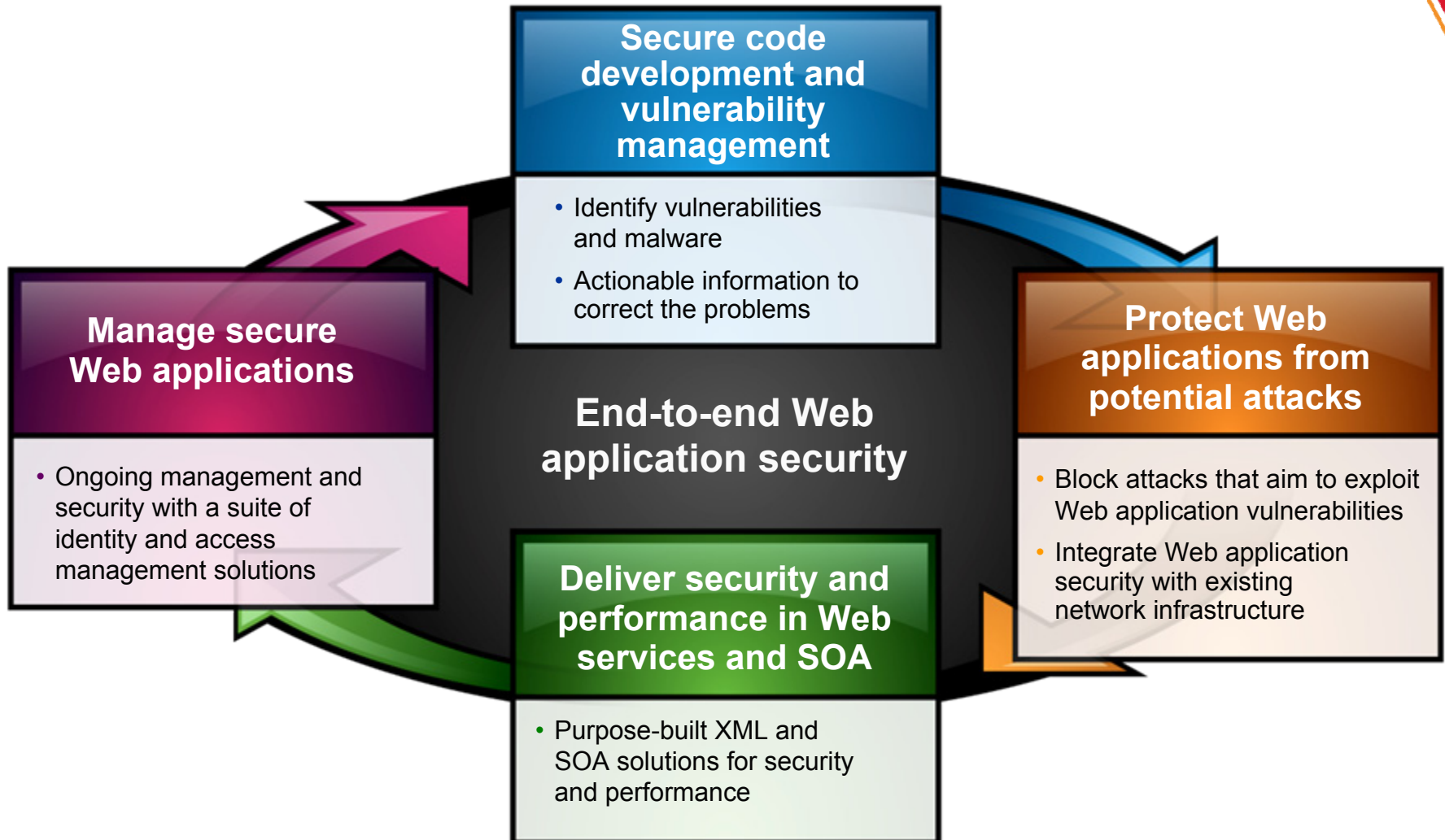
# More Intelligent Insight into Web Application Threats

- Correlates vulnerability data with actual attacks
- Understand which attacks have a high probability of success
- Increased insight helps in tuning IPS Web protection module
- Prioritize vulnerability remediation efforts based exposure

The screenshot shows the SiteProtector Event Analysis interface. The left pane displays a tree view of 'My Sites' with a folder structure including '65.196.147.50', 'SP2001', 'Geographical', 'Organizational', 'Protection Solutions', 'ES-Series', 'G-Series', 'M-Series', 'PSL', 'Rational AppScan', and 'SiteProtector'. The main pane shows 'Event Analysis - Event Name (Agent)' with filters for 'Last Week', 'Tag Name Filter', and 'Source IP Filter'. A table of events is displayed below, with two rows highlighted in blue and red:

Tag Name	Status
HTTP_POST_SQL_UnionSelect	Detected event
SQL_Injection	Attack likely successful (vulnerable)
XPath_Injection	Attack likely successful (vulnerable)
1.1.1.1 - 255.255.255.254	Detected event
192.168.1.0 - 192.168.1.255	Detected attack (vuln not scanned recently)
localhost	Detected attack (vuln not scanned recently)
HTTP_Server_ID	Detected event
HTTP_Share_Point_XSS	Detected attack (vuln not scanned recently)
HTTP_Shells_Perl_Exe	Detected attack (vuln not scanned recently)
HTTP_testcgi	Attack failure (blocked by Proventia appliance)
HTTP_Translate_F_SourceRead	Attack failure (blocked by Proventia appliance)
HTTP_Twiki_Image_Include_CmdExec	Attack failure (blocked by Proventia appliance)
HTTP_Unify_UploadServlet	Attack failure (blocked by Proventia appliance)
HTTP_Unix_Passwords	Detected event
HTTP_URL_BackslashDotDot	Detected attack (vuln not scanned recently)
HTTP_URL_dotpath	Detected event
HTTP_URL_Many_Slashes	Attack failure (blocked by Proventia appliance)
HTTP_URL_repeated_char	Detected event
HTTP_URL_Repeated_Dot	Detected attack (vuln not scanned recently)
HTTP_URLscan	Detected event
HTTP_Webplus	Attack failure (blocked by Proventia appliance)
HTTP_Windows_Executable	Attack failure (blocked by Proventia appliance)
SQL_Injection	Attack likely successful (vulnerable)
XPath_Injection	Attack likely successful (vulnerable)

# IBM can Help Protect your Valuable Assets





# QUESTIONS

[www.ibm.com/security](http://www.ibm.com/security)



# Acknowledgements, disclaimers and trademarks

© Copyright IBM Corporation 2012. All rights reserved.

The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication 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 this publication to IBM products, programs or services do not imply that they will be made available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation 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. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth, savings or other results. All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information concerning non-IBM products and services was obtained from a supplier of those products and services. IBM has not tested these products or services and cannot confirm the accuracy of performance, compatibility, or any other claims related to non-IBM products and services. Questions on the capabilities of non-IBM products and services should be addressed to the supplier of those products and services.

All customer examples cited or described are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer and will vary depending on individual customer configurations and conditions. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

IBM, the IBM logo, ibm.com, Tivoli, the Tivoli logo, Tivoli Enterprise Console, Tivoli Storage Manager FastBack, and other IBM products and services are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at [ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml)