# Protect Data & Client Trust:

## An end to end approach to protecting web applications and your organization

**Deepa Nadig**
*IT Specialist*
*deenadig@in.ibm.com*
*+91-9845296929*

**Innovate2010**
The Rational Software Conference

**Let's build a smarter planet.**

The premiere software and product delivery event.
**Aug 16th-19th India**

# Smarter planet opportunities driven by Web-enabled applications

## The Opportunity – smarter planet

INTERNET
facebook
myspace a place for friends
iTunes
Google

Globalization and Globally Available Resources

Access to streams of information in the Realtime

Billions of mobile devices accessing the Web

New Forms of Collaboration

# Smarter planet opportunities driven by Web-enabled applications

## The Driver – Web-enabled Applications

### Web Applications

Intuitive interfaces for business processes, client interaction, integration with business partners

### Web 2.0 and SOA

Collaboration among peers and partners

### Databases

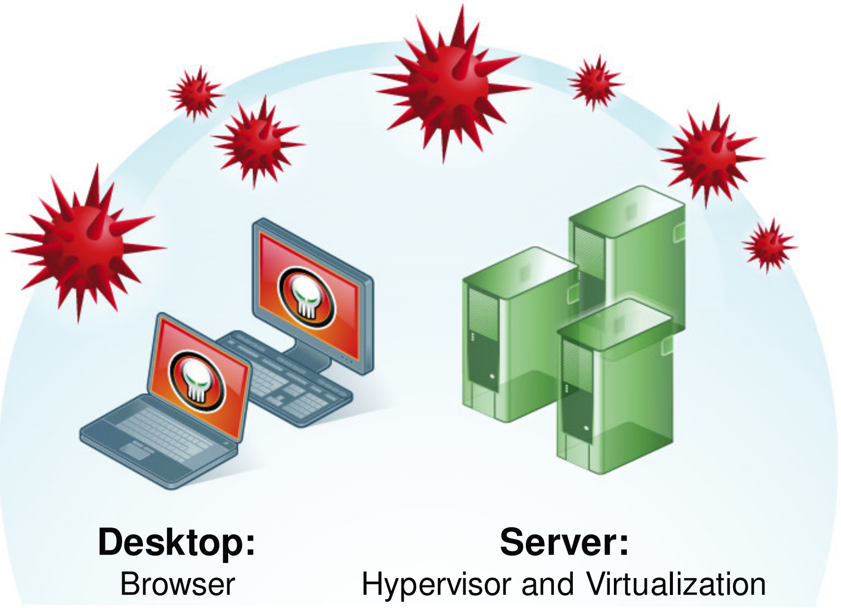
Backend of every Web application

**How do I secure the new Web without significantly Increasing my costs?**

# Changing security landscape creates complex threats

**Web-enabled applications drive the need for security**

- New applications are increasing the attack surface
- Complex Web applications create complex security risks
- Making applications more available to “good” users, makes them more available to “bad” users
- Web attacks are evolving to blended attacks (i.e. planting of malware on legitimate Web sites)



**Desktop:**
Browser

**Server:**
Hypervisor and Virtualization
Web Applications

# Unprotected Web applications risk sensitive data and compliance

## Risks and Threats

Stealing Sensitive Information is one of the highest motivation for Web application attacks

## Costs of Security Breaches

- Average cost of a security breach is $6.6 million
- Client notification ($202 per record)
- Fines (as high as $15 million)
- Brand loss and lawsuits
- Disruption to business operations

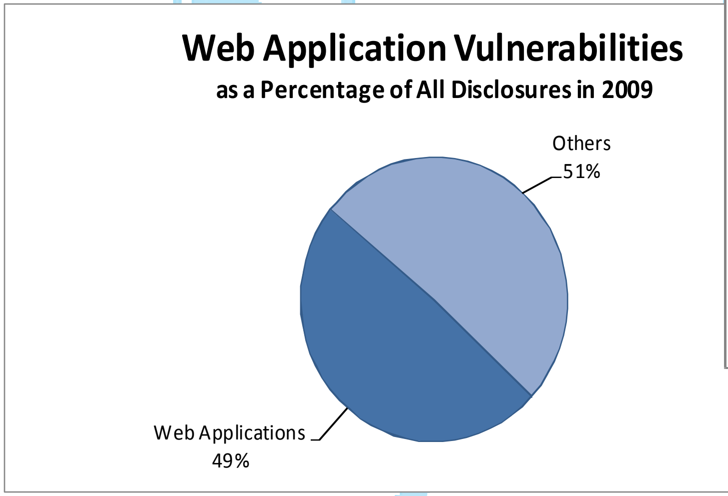
## Compliance Demands

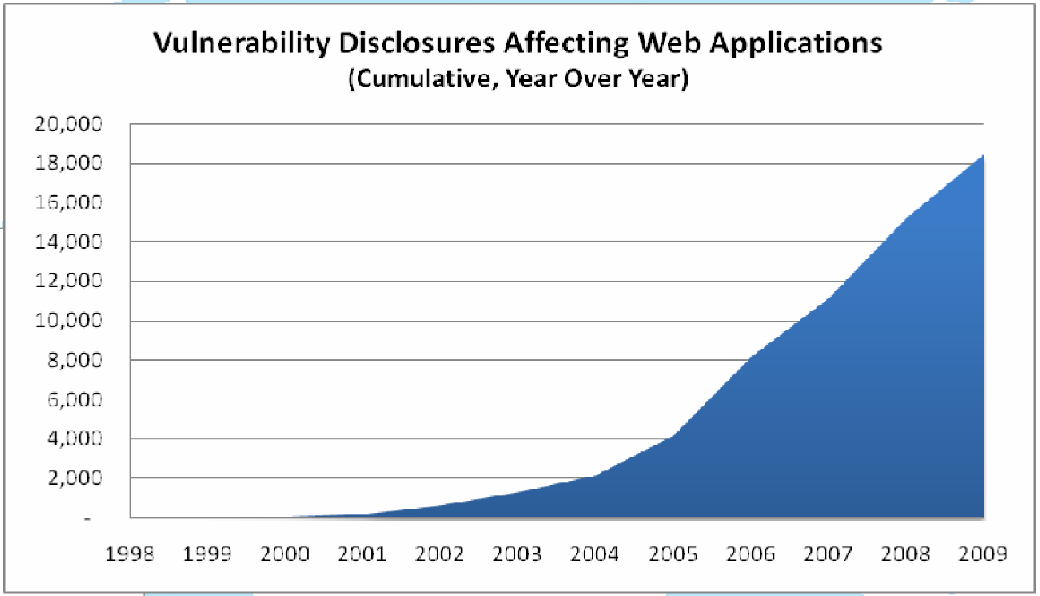
PCI DSS non-compliance costs clients hundreds of thousands in fines a month

Source: Web Incidents Hacking Database 2008 Annual report

# COTS Application Vulnerabilities Continue to Grow

- In 2009, 49% of all vulnerabilities are Web application vulnerabilities
- SQL injection and Cross-Site Scripting are neck and neck in a race for the top spot
- 67% of web application vulnerabilities had no patch by the end of the year

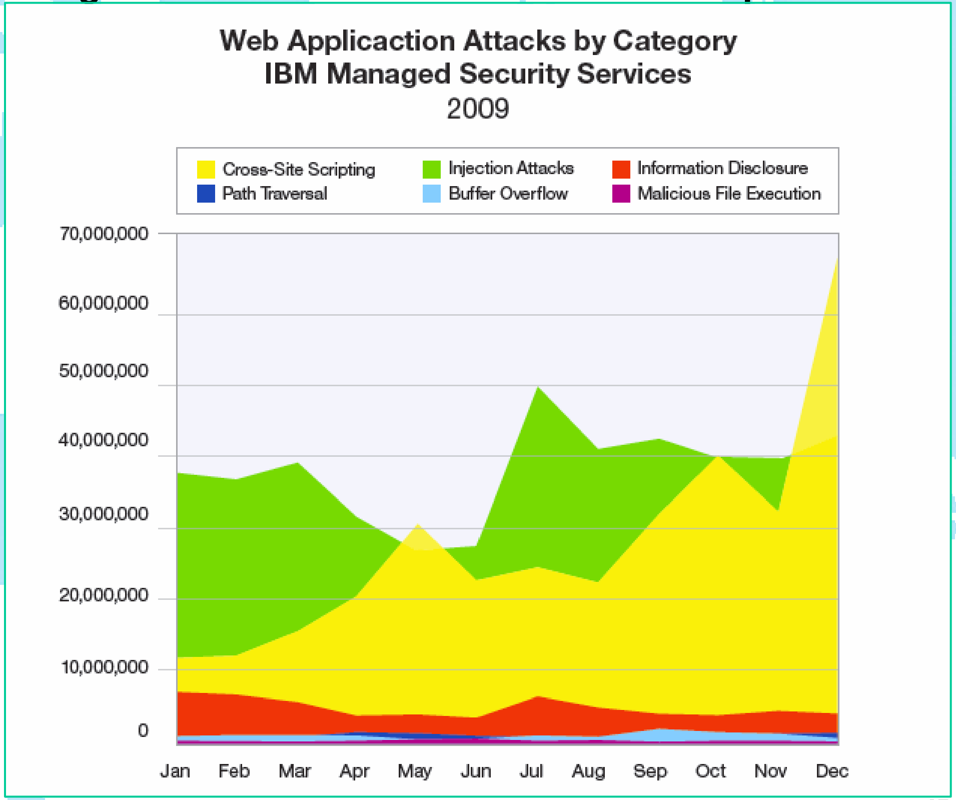




*IBM Internet Security Systems*
*2009 X-Force® Trend & Risk Report*

# Attacks are Both Plentiful and Trivial

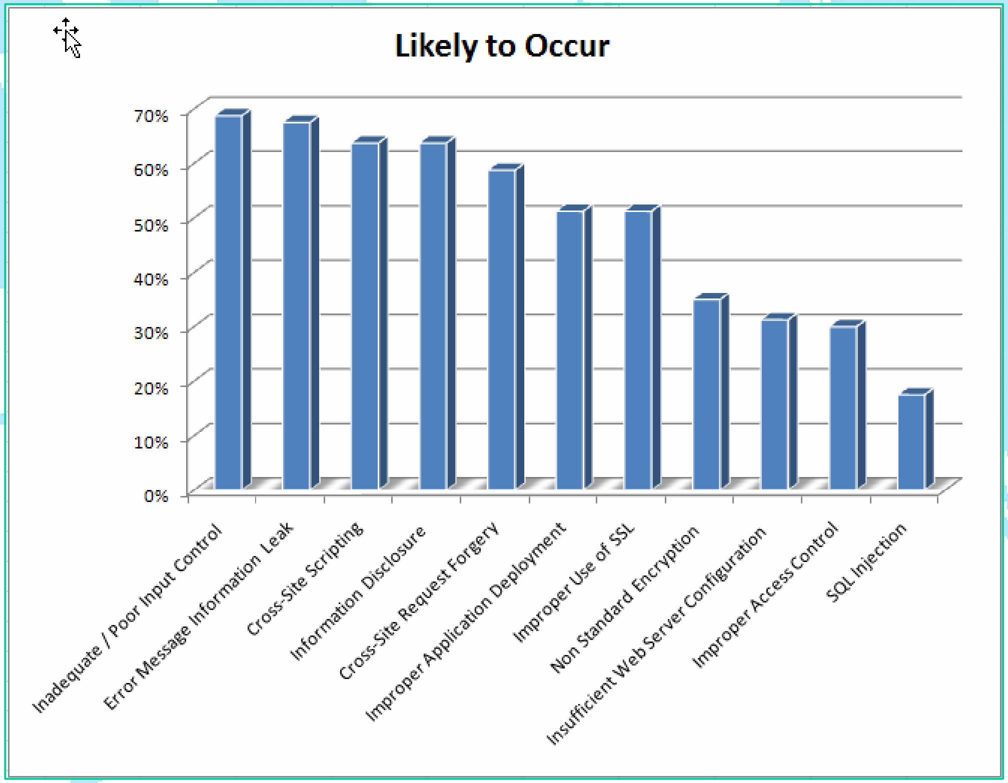
- Over **60 million XSS attacks** in December, 2009 alone
- An average of **30 million SQL injection attacks** observed every month
- Automated exploit engines continue to lower the cost of exploitation



*IBM Internet Security Systems*
*2009 X-Force® Trend & Risk Report*

# Over 90% of Custom Web Apps have Vulnerabilities

- **In 2009, over two thirds of custom applications contained XSS vulnerabilities**
- **In 2009, over 93% of custom web applications contained at least one high/medium vulnerability**



*IBM Rational AppScan OnDemand Statistics 2009*

# Breaches are Numerous and Significant

- Security forensics team investigated 90 confirmed security breaches in a single year*
  - Encompassed an astounding 285 million compromised data records
  - Vulnerable Web Applications (SQL Injection) accounted for 79% of compromised data records

Figure 4. Sources of breaches by percent of breaches

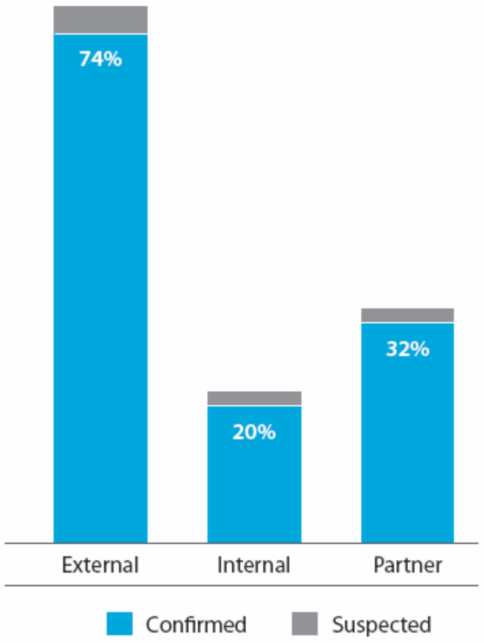
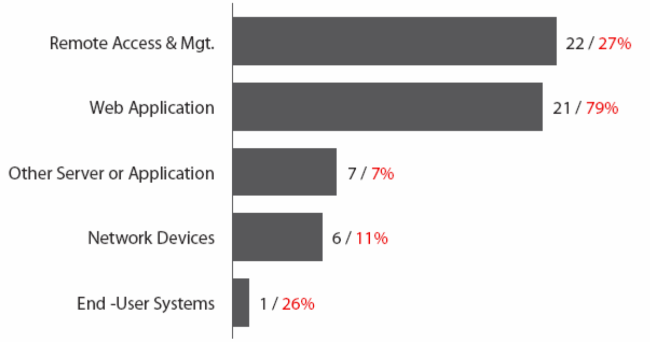


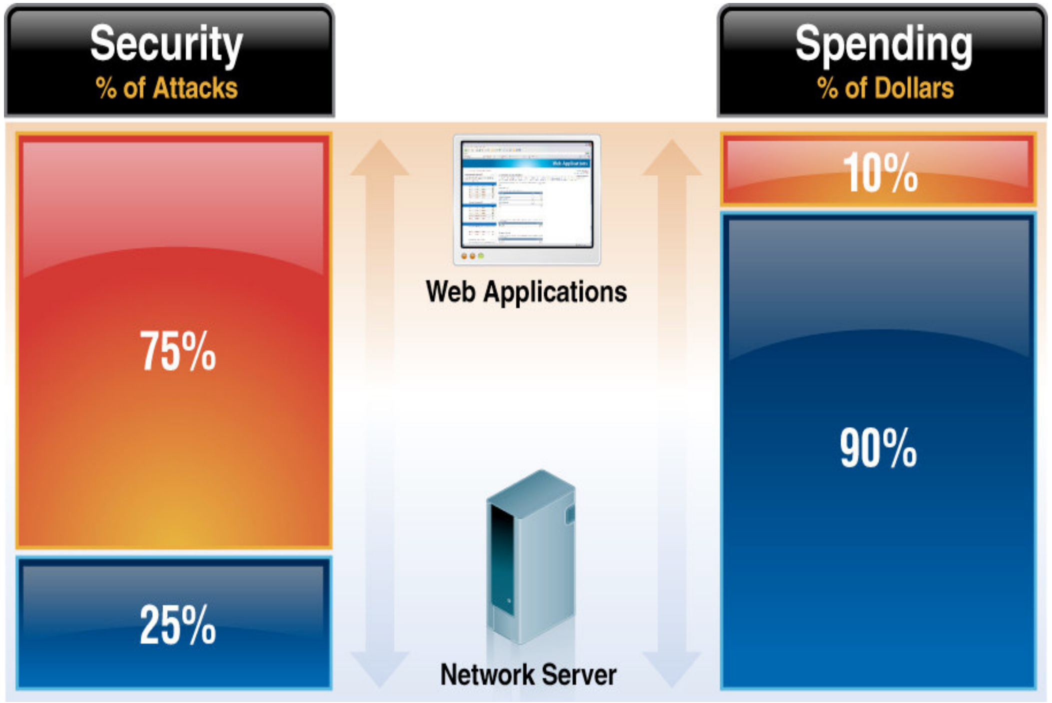
Figure 16. Attack pathways by number of breaches (black) and percent of records (red)



*2009 Verizon Data Breach Report*

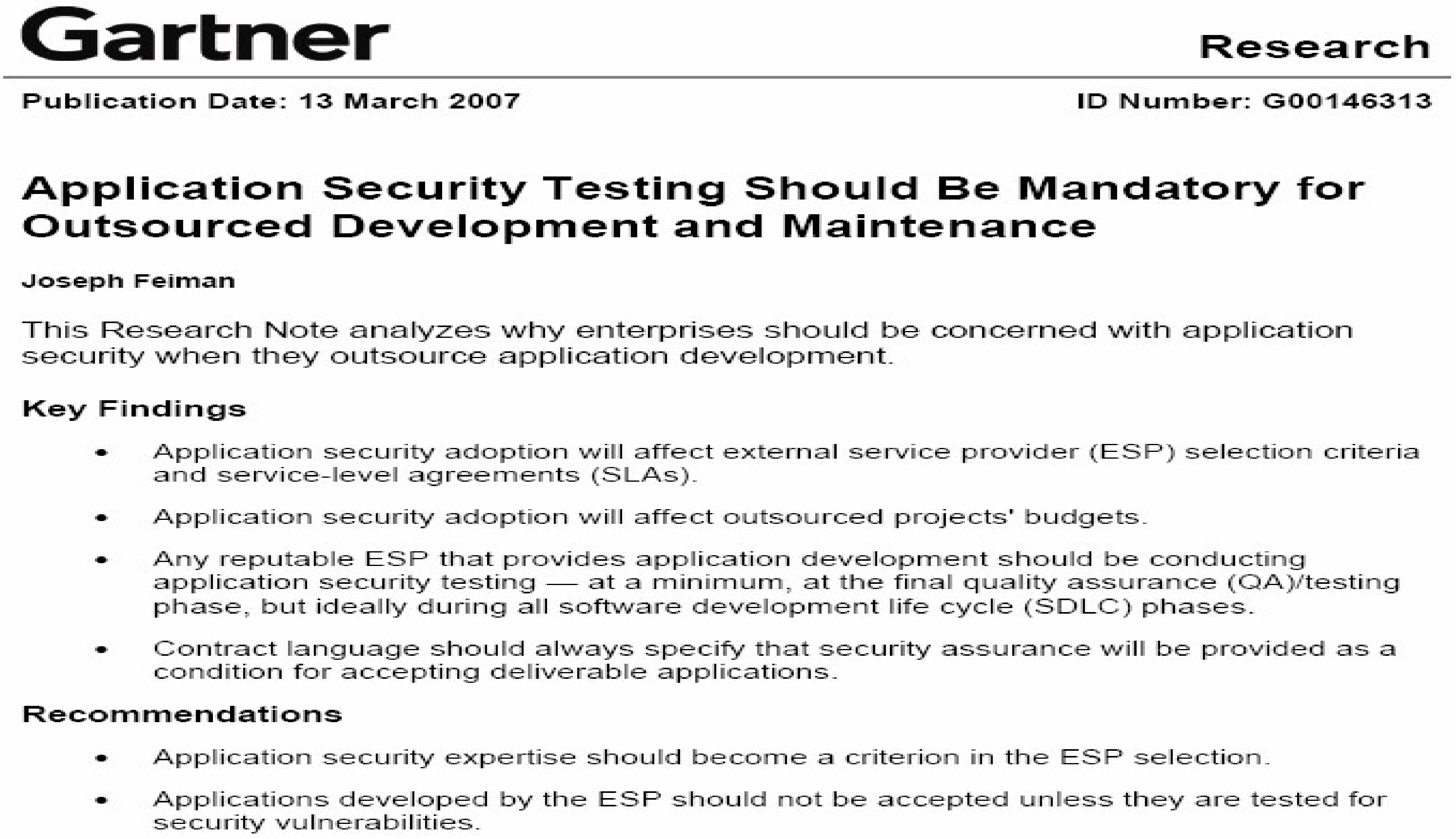
# Traditional point solutions throw money at the problem and can't address the full problem

- **Vulnerability scanners**
  - Traditional vulnerability scanners don't cover Web applications
- **Penetration testing**
  - Effective at finding vulnerabilities but not scalable for ongoing tests
  - Not focused on remediation
- **Network firewall and IPS**
  - Generic Web application protection (if any) so most custom Web applications not covered
  - Most IPS solutions focus on exploits as opposed to Web application vulnerabilities
- **Web application firewall**
  - Expensive point product to deploy and manage
  - Can be effective, but difficult to deploy, tune and manage
  - Building policies can be as time consuming as remediating the vulnerability



Source: Gartner

# Increasingly your End customers are demanding Secure Coding , non adherence might mean loss of valuable Customer.



Gartner Research

Publication Date: 13 March 2007 ID Number: G00146313

## Application Security Testing Should Be Mandatory for Outsourced Development and Maintenance

Joseph Feiman

This Research Note analyzes why enterprises should be concerned with application security when they outsource application development.

### Key Findings

- Application security adoption will affect external service provider (ESP) selection criteria and service-level agreements (SLAs).
- Application security adoption will affect outsourced projects' budgets.
- Any reputable ESP that provides application development should be conducting application security testing — at a minimum, at the final quality assurance (QA)/testing phase, but ideally during all software development life cycle (SDLC) phases.
- Contract language should always specify that security assurance will be provided as a condition for accepting deliverable applications.

### Recommendations

- Application security expertise should become a criterion in the ESP selection.
- Applications developed by the ESP should not be accepted unless they are tested for security vulnerabilities.

# Cost is a Significant Driver for Moving Security Testing in SDLC

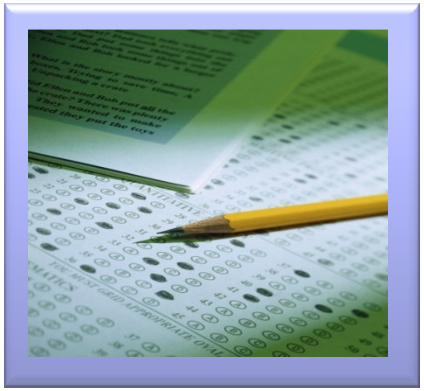
***80% of development costs are spent identifying and correcting defects!****

***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***

***+***

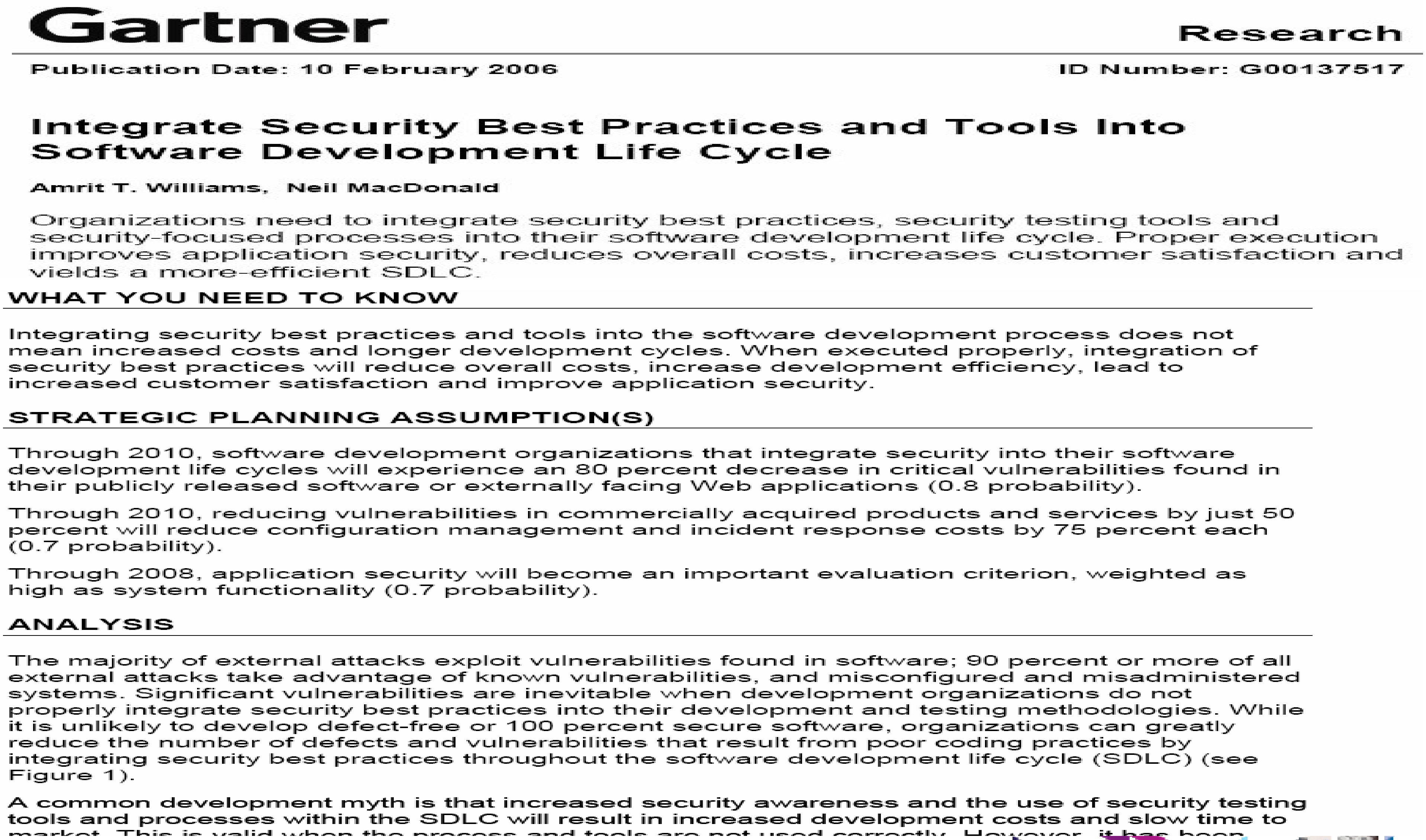
***Law suits, loss of customer trust, damage to brand***

***The increasing costs of fixing a defect….***

*Capers Jones, Applied Software Measurement, 1996*

** Source: NIST, 'Assesses Technical Needs of Industry to Improve Software Testing', June 28, 2002*

# Incorporating Security at coding is most efficient way of building secure Applications:



Gartner

Research

Publication Date: 10 February 2006

ID Number: G00137517

## Integrate Security Best Practices and Tools Into Software Development Life Cycle

Amrit T. Williams, Neil MacDonald

Organizations need to integrate security best practices, security testing tools and security-focused processes into their software development life cycle. Proper execution improves application security, reduces overall costs, increases customer satisfaction and yields a more-efficient SDLC.

### WHAT YOU NEED TO KNOW

Integrating security best practices and tools into the software development process does not mean increased costs and longer development cycles. When executed properly, integration of security best practices will reduce overall costs, increase development efficiency, lead to increased customer satisfaction and improve application security.

### STRATEGIC PLANNING ASSUMPTION(S)

Through 2010, software development organizations that integrate security into their software development life cycles will experience an 80 percent decrease in critical vulnerabilities found in their publicly released software or externally facing Web applications (0.8 probability).

Through 2010, reducing vulnerabilities in commercially acquired products and services by just 50 percent will reduce configuration management and incident response costs by 75 percent each (0.7 probability).

Through 2008, application security will become an important evaluation criterion, weighted as high as system functionality (0.7 probability).

### ANALYSIS

The majority of external attacks exploit vulnerabilities found in software; 90 percent or more of all external attacks take advantage of known vulnerabilities, and misconfigured and misadministered systems. Significant vulnerabilities are inevitable when development organizations do not properly integrate security best practices into their development and testing methodologies. While it is unlikely to develop defect-free or 100 percent secure software, organizations can greatly reduce the number of defects and vulnerabilities that result from poor coding practices by integrating security best practices throughout the software development life cycle (SDLC) (see Figure 1).

A common development myth is that increased security awareness and the use of security testing tools and processes within the SDLC will result in increased development costs and slow time to market. This is valid when the process and tools are not used correctly. However, it has been

# ROI Opportunity of Application Security Testing

## *Cost Savings – of testing early in the development process (ALM)*

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

**Testing for vulnerabilities earlier in the development process can help avoid that unnecessary expense**

- ***Cost of finding & fixing problems:***
  - *code stage is $25, QA/Testing is $450, Production $16,000 **
  - *Ex: 50 applications annually & 25 issues per application, testing at code stage* saves $780,000 *(present day dollars – assumes 3% inflation) over testing at QA stage.*

## *Cost Savings – of automated vs manual testing*

**Automated testing provides tremendous productivity savings over manual testing**

**Automated source code testing with periodic penetration testing allows for cost effective security analysis of applications**

- *Outsourced audits can cost $10,000 to $50,000 per application*
- *At $20,000 an app, 50 audits will cost $1M.*
- *With 1 hire + 4 quarterly outsourced audits (ex: $120,000+$80,000),* ***$800,000/yr can be saved*** *(less the cost of testing software)*

## *Cost Avoidance – of a security breach*

**Costs as a result of a security breach can include (but are not limited to) audit fees, legal fees, regulatory fines, lost customer revenue and brand damage**

- *The cost to companies is* ***$202*** *per compromised record***
- *The average cost per data breach is* ***$6.6 Million*****

**** Source: Capers Jones, Applied Software Measurement, 1996***
***** Source: Ponemon Institute, Privacy Rights Clearinghouse, 2008***

# A Cycle to Secure Software

## Design Phase

- ***Consideration is given to security requirements of the application***
- ***Issues such as required controls and best practices are documented on par with functional requirements***

## Development Phase

- ***Software is checked during coding for:***
  - ***Implementation error vulnerabilities***
  - ***Compliance with security requirements***

## Build & Test Phase

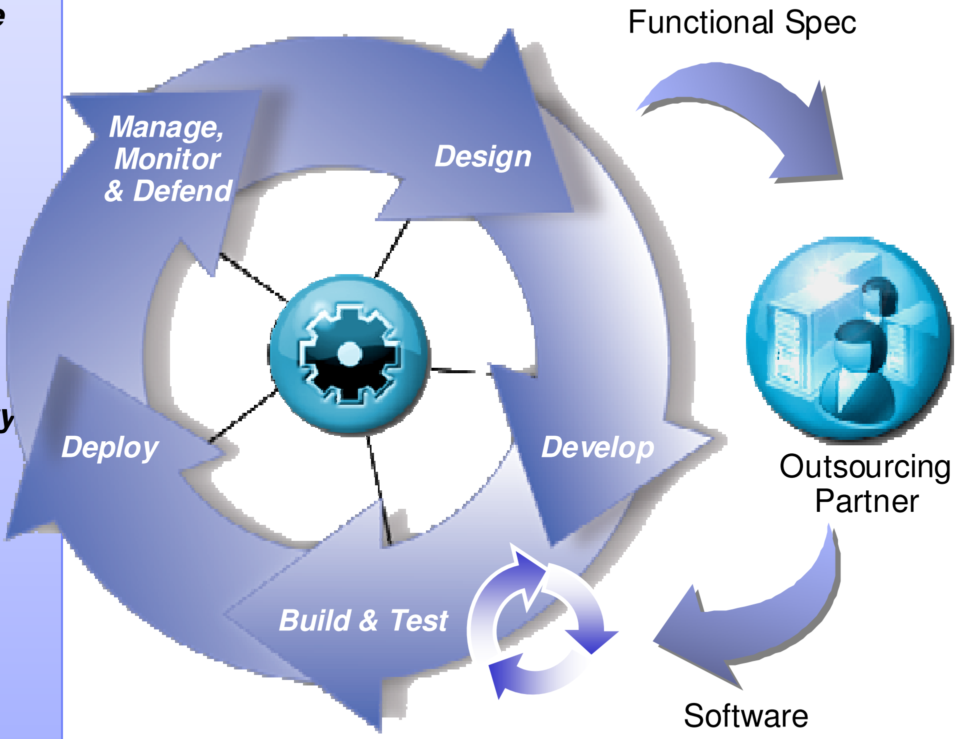
- ***Testing begins for errors and compliance with security requirements across the entire application***
- ***Applications are also tested for exploitability in deployment scenario***

## Deployment Phase

- ***Configure infrastructure for application policies***
- ***Deploy applications into production***

## Operational Phase

- ***Continuously monitor applications for appropriate application usage, vulnerabilities and defend against attacks***

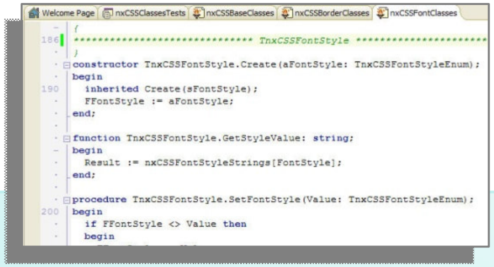


# Security Testing Technologies...

## Combination Delivers a Comprehensive Solution

### Static Code Analysis = Whitebox

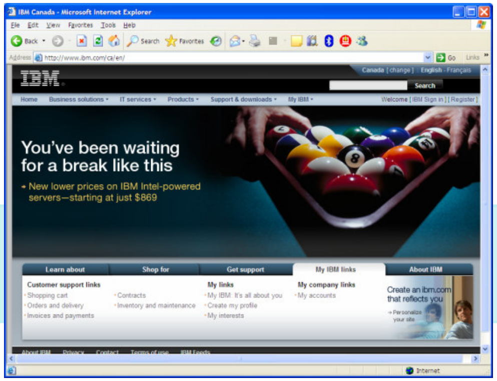
- *Scanning source code for security issues*



```
{
****************************** TnxCSSFontStyle ************************
}
constructor TnxCSSFontStyle.Create(aFontStyle: TnxCSSFontStyleEnum);
begin
  inherited Create(sFontStyle);
  FFontStyle := aFontStyle;
end;

function TnxCSSFontStyle.GetStyleValue: string;
begin
  Result := nxCSSFontStyleStrings[FontStyle];
end;

procedure TnxCSSFontStyle.SetFontStyle(Value: TnxCSSFontStyleEnum);
begin
  if FFontStyle <> Value then
  begin
```

### Dynamic Analysis = Blackbox

- *Performing security analysis of a compiled application*


IBM Canada - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.ibm.com/ca/en/
Go Links
IBM
Canada [ change ] English - Français
Search
Home Business solutions IT services Products Support & downloads My IBM
Welcome [ IBM Sign in ] [ Register ]
Learn about
Shop for
Get support
My IBM links
About IBM
About IBM Privacy Contact Terms of use IBM Feeds
Internet

You've been waiting for a break like this

→ New lower prices on IBM Intel-powered servers—starting at just $869

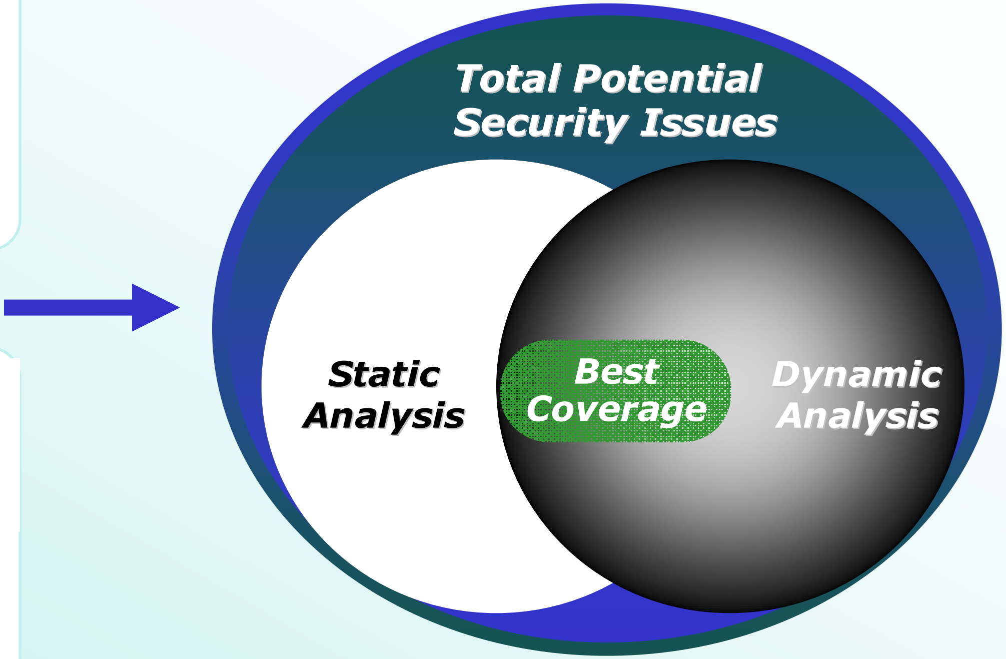
Customer support links
- Shopping cart
- Orders and delivery
- Invoices and payments
- Contracts
- Inventory and maintenance

My links
- My IBM: It's all about you
- Create my profile
- My interests

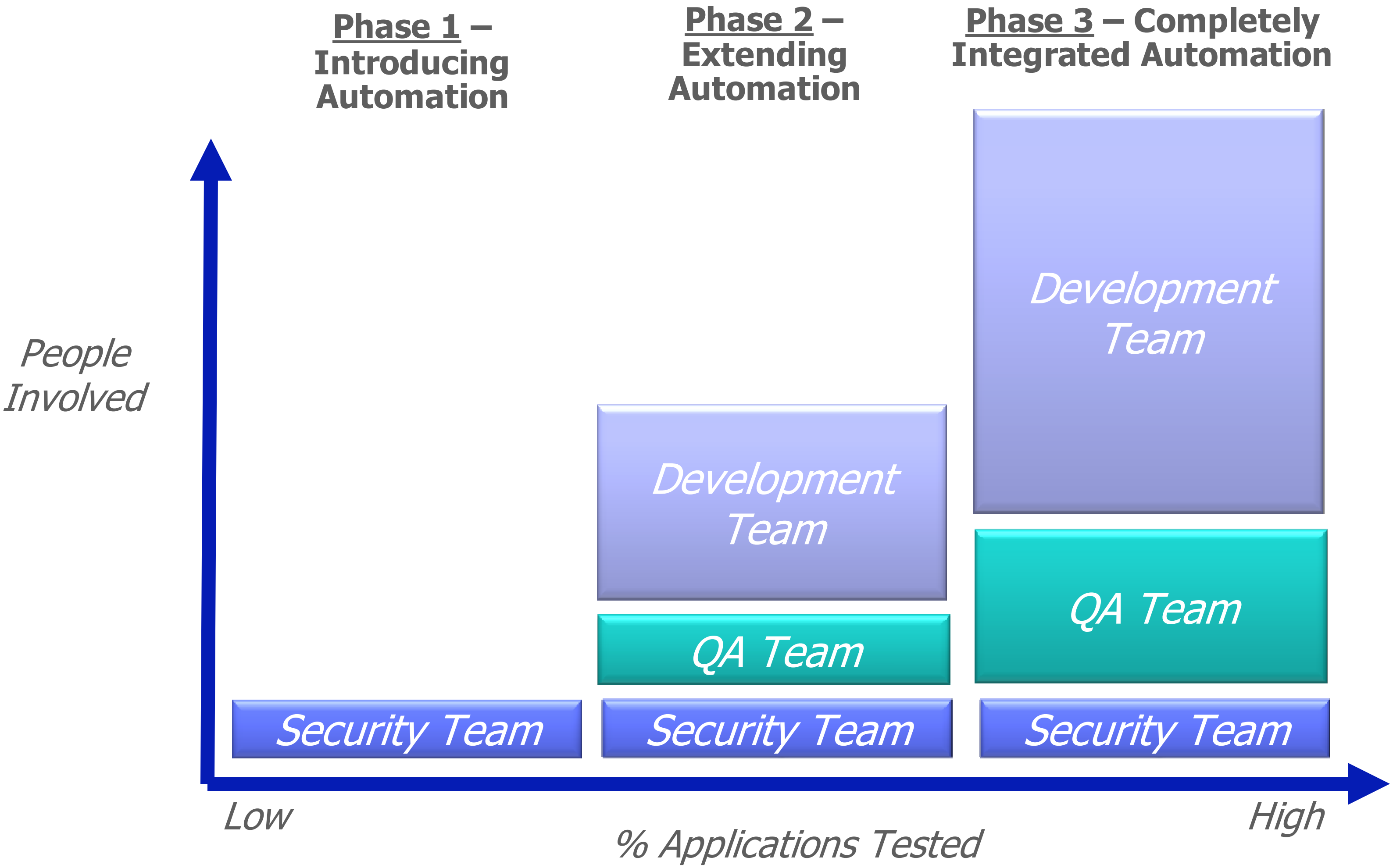
My company links
- My accounts

Create an ibm.com that reflects you

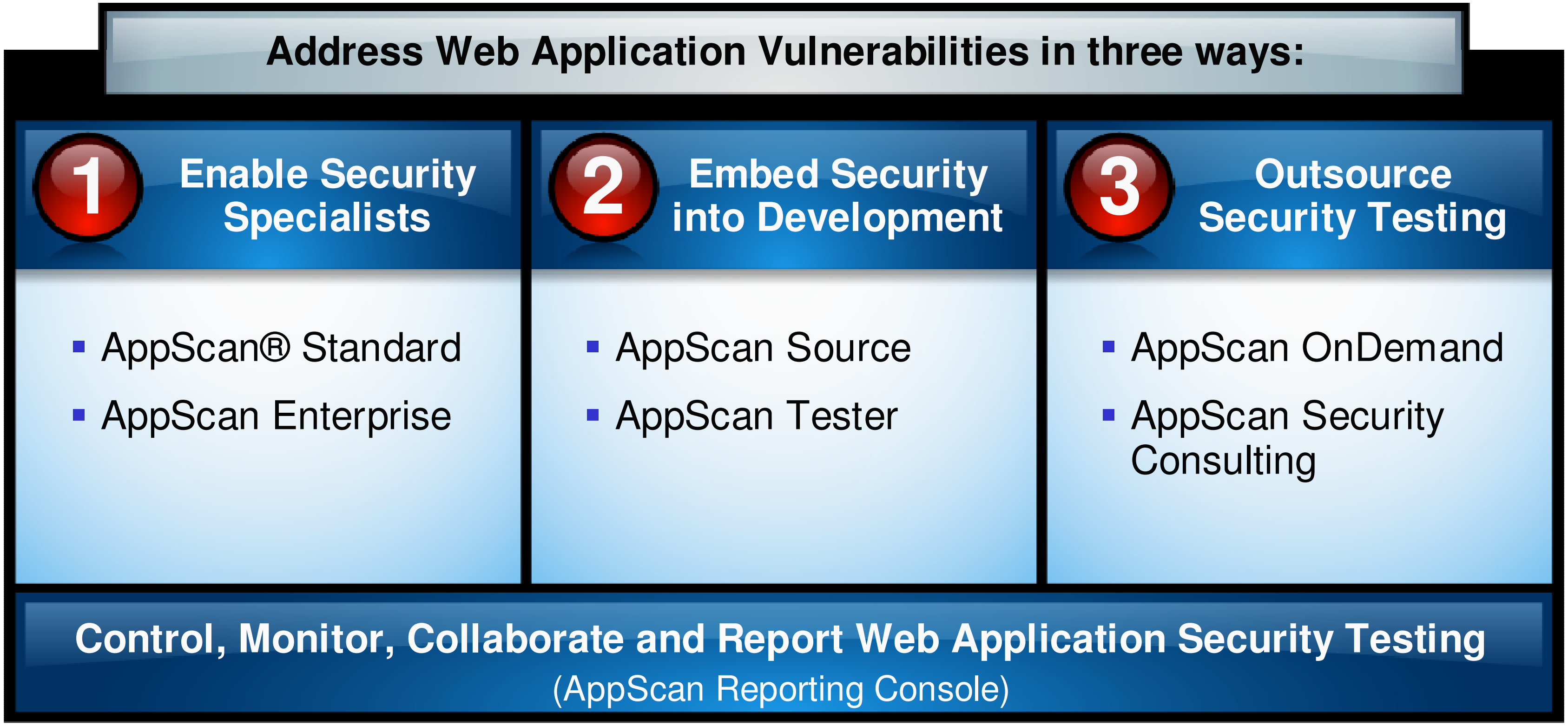
→ Personalize your site



# The Need to Scale Security Testing



# Enabling the operationalization of security testing



**Address Web Application Vulnerabilities in three ways:**

**1 Enable Security Specialists**

- AppScan® Standard
- AppScan Enterprise

**2 Embed Security into Development**

- AppScan Source
- AppScan Tester

**3 Outsource Security Testing**

- AppScan OnDemand
- AppScan Security Consulting

**Control, Monitor, Collaborate and Report Web Application Security Testing**

(AppScan Reporting Console)

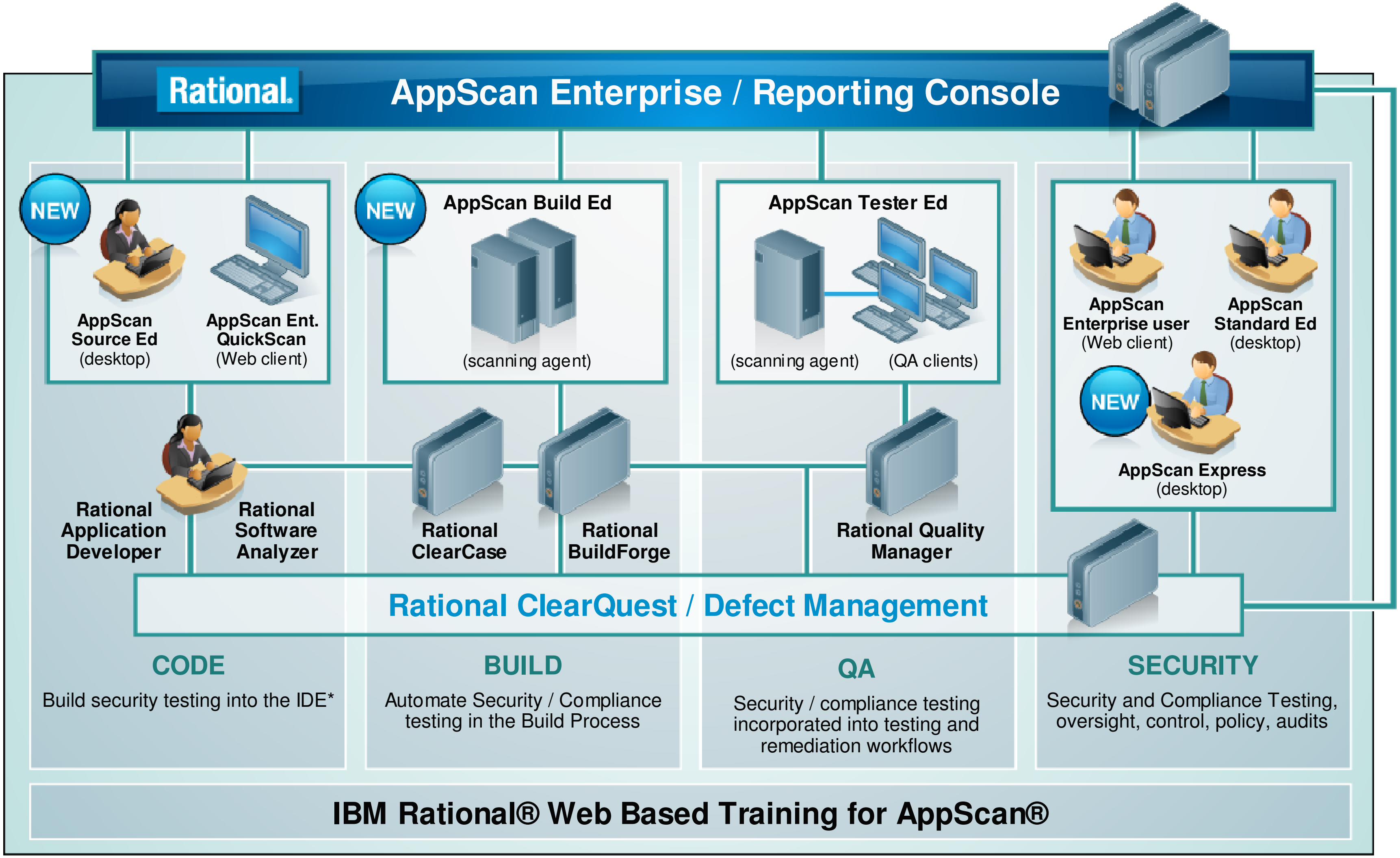
Secure code development and vulnerability management

Protect Web applications from potential attacks

Deliver security and performance in Web services and SOA

Manage secure Web applications

# Enabling security testing through the SDLC



Rational. AppScan Enterprise / Reporting Console

NEW AppScan Source Ed (desktop)

AppScan Ent. QuickScan (Web client)

NEW AppScan Build Ed (scanning agent)

AppScan Tester Ed (scanning agent) (QA clients)

AppScan Enterprise user (Web client)

AppScan Standard Ed (desktop)

NEW AppScan Express (desktop)

Rational Application Developer

Rational Software Analyzer

Rational ClearCase

Rational BuildForge

Rational Quality Manager

Rational ClearQuest / Defect Management

CODE
Build security testing into the IDE*

BUILD
Automate Security / Compliance testing in the Build Process

QA
Security / compliance testing incorporated into testing and remediation workflows

SECURITY
Security and Compliance Testing, oversight, control, policy, audits

IBM Rational® Web Based Training for AppScan®

Secure code development and vulnerability management

Protect Web applications from potential attacks

Deliver security and performance in Web services and SOA

Manage secure Web applications

# Application Security COE at System Integrator

## 1. Embed Security into Development

- Implement Top-down driven model for Application Security with flexible user options ensuring least cost of expansion and SLA adherence for security requirements.

- Incorporate Security as a Standard norm using centralized command centre and deploying the policies across all the Client Application Development /Maintenance Projects.

- Integrate the security tools seamlessly into the ALM lifecycle using Rational SDLC tools thereby causing minimum hindrance/change management issues.

- Develop the culture for Security within entire software development organization thereby reducing cost/increasing marketability of software to a great extent and reducing the bottle necks at the testing/security practice level.

# AppScan Source Edition

- A static code analysis security testing solution with centralized control of security policies
- Allows organizations to create, distribute and enforce consistent security policies
- Provides automated security testing by seamlessly integrating security source code analysis into the build process

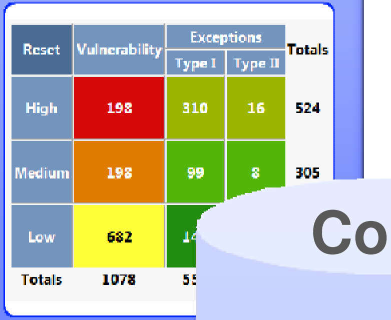
## Benefits:

- Enables security teams strengthen application security, protect confidential data and improve compliance
- Enables the cost effective remediation of vulnerabilities early in the development process to support on-time delivery of projects

# IBM Rational AppScan Source Edition Solution

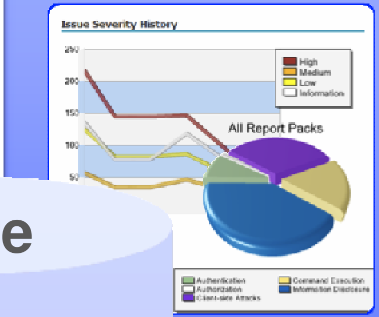
## Security

- Configure Software
- Scan
- Triage Results
- Manage Security Policies



| Reset | Vulnerability | Exceptions | | Totals |
|---|---|---|---|---|
| | | Type I | Type II | |
| High | 198 | 310 | 16 | 524 |
| Medium | 198 | 99 | 8 | 305 |
| Low | 682 | 14 | [illegible] | [illegible] |
| Totals | 1078 | 55 | [illegible] | [illegible] |

## Reporting Console



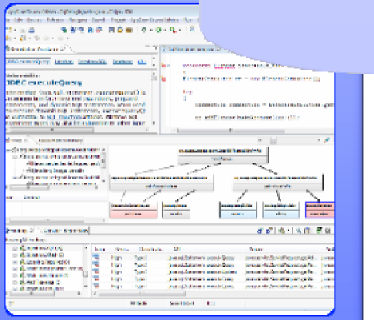
- Track Progress
- Compare Applications
- Customize Dashboards
- Manage Portfolio Risk
- Combine BB/WB results

## Core

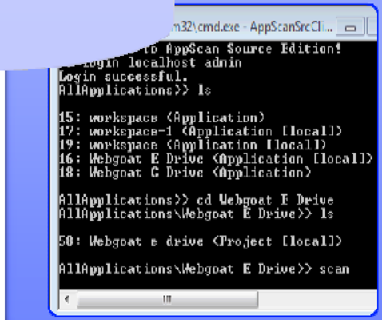
- Knowledgebase
- Assessment Database
- Custom Rules

## IDE Plug-Ins

- Investigate Flaws
- Remediate with Guidance
- Scan
- Confirm Fix



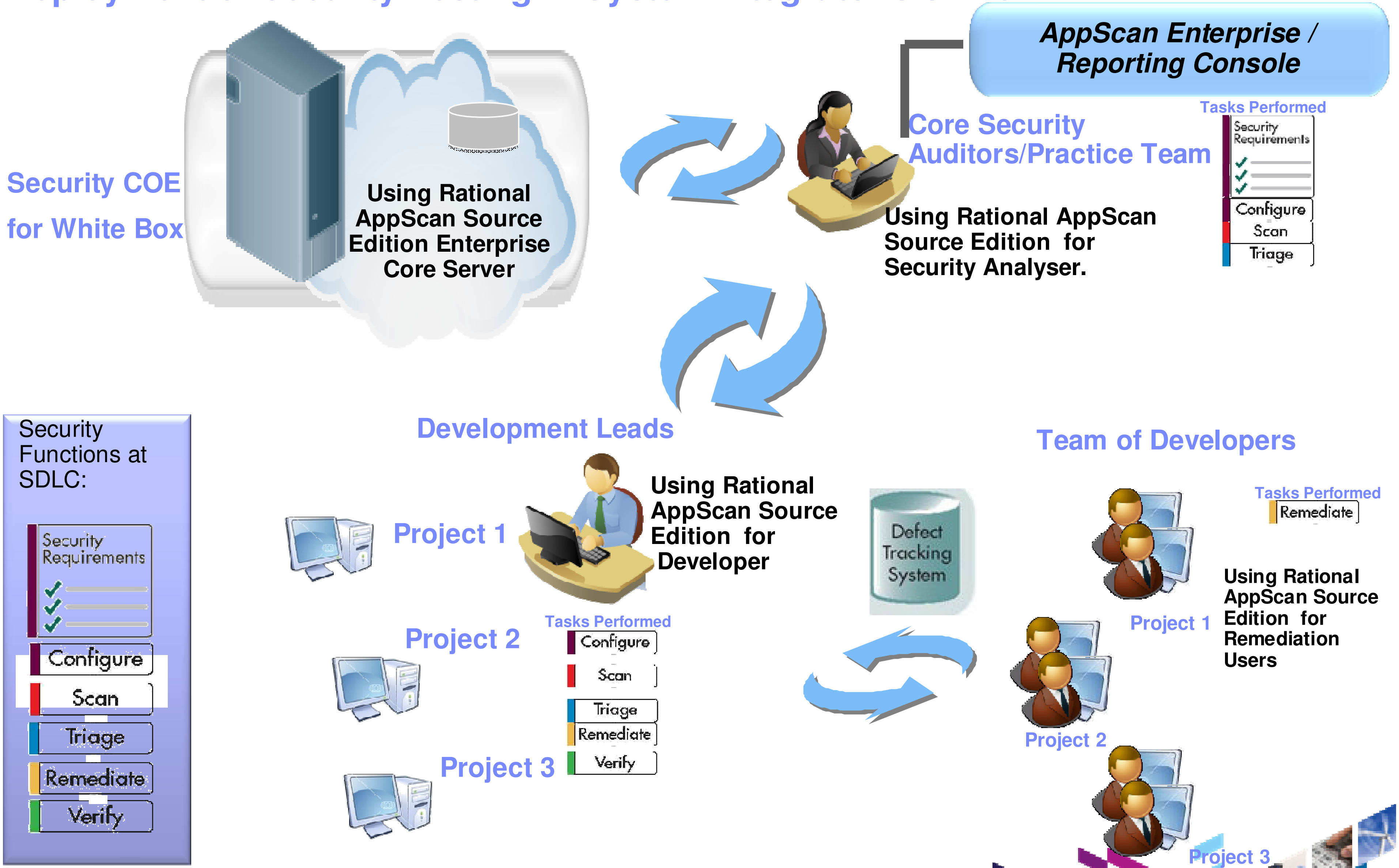
## Automation



```
                to AppScan Source Edition!
   login localhost admin
Login successful.
AllApplications>> ls

15: workspace (Application)
17: workspace-1 (Application [local])
19: workspace (Application [local])
16: Webgoat E Drive (Application [local])
18: Webgoat C Drive (Application)

AllApplications>> cd Webgoat E Drive
AllApplications\Webgoat E Drive>> ls

50: Webgoat e drive (Project [local])

AllApplications\Webgoat E Drive>> scan
```

- Build integration
- Automate Scans
- ANT, Make, Maven integration
- Data Access API

# Deployment of Security Testing in System Integrator's SDLC



Security COE for White Box

Using Rational AppScan Source Edition Enterprise Core Server

*AppScan Enterprise / Reporting Console*

Core Security Auditors/Practice Team

Using Rational AppScan Source Edition for Security Analyser.

Tasks Performed

- Security Requirements
- Configure
- Scan
- Triage

Development Leads

Using Rational AppScan Source Edition for Developer

Project 1

Project 2

Project 3

Tasks Performed

- Configure
- Scan
- Triage
- Remediate
- Verify

Defect Tracking System

Team of Developers

Tasks Performed

- Remediate

Using Rational AppScan Source Edition for Remediation Users

Project 1

Project 2

Project 3

Security Functions at SDLC:

- Security Requirements
- Configure
- Scan
- Triage
- Remediate
- Verify

# Basic Operational Responsibilities

Security Requirements
✓
✓
✓

**Set security requirements:** A manager or security expert defines vulnerabilities and how to judge criticality

Configure

**Configure:** Use the Project Configuration Wizard to get set up to scan your applications

Scan

**Scan:** Scan large code bases and return results. Ounce's unique security compiler technology handles code complexity and size with maximum efficiency

Triage

**Triage:** Separate real vulnerabilities from potential ones, allowing triage on critical issues to begin immediately.

Remediate

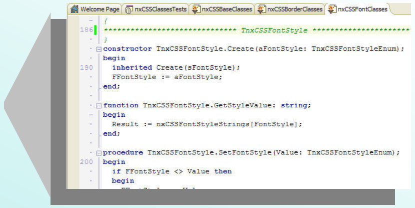
**Resolve:** Eliminate vulnerabilities by rewriting code, removing flaws, or adding security functions

Verify

**Verify fixes:** Rescan the code to assure that vulnerabilities are eliminated

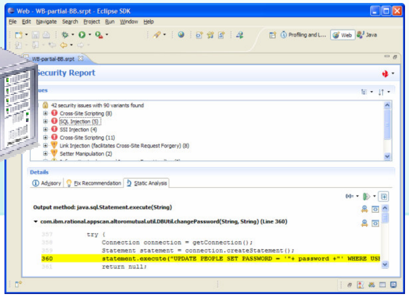
# AppScan Source Edition - Proactive Use Case

## 1. Developer Writes Code



```
{
****************************** TnxCSSFontStyle **********************
}
constructor TnxCSSFontStyle.Create(aFontStyle: TnxCSSFontStyleEnum);
begin
  inherited Create(sFontStyle);
  FFontStyle := aFontStyle;
end;

function TnxCSSFontStyle.GetStyleValue: string;
begin
  Result := nxCSSFontStyleStrings[FontStyle];
end;

procedure TnxCSSFontStyle.SetFontStyle(Value: TnxCSSFontStyleEnum);
begin
  if FFontStyle <> Value then
  begin
```

## 2. Developer Tests Changes Using AppScan Source



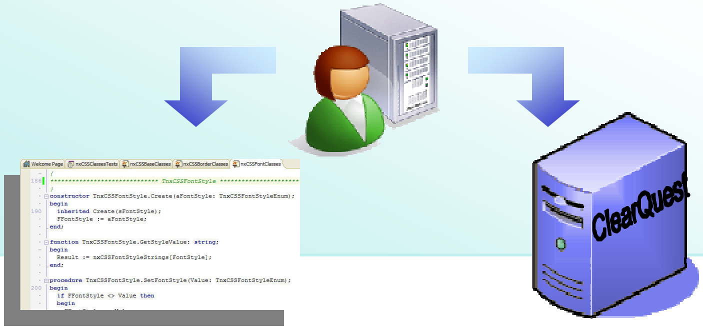
42 security issues with 90 variants found
- Cross-Site Scripting (8)
- SQL Injection (5)
- SSI Injection (4)
- Cross-Site Scripting (11)
- Link Injection (facilitates Cross-Site Request Forgery) (8)
- Setter Manipulation (2)

**Output method: java.sql.Statement.execute(String)**

**com.ibm.rational.appscan.altoromutual.util.DBUtil.changePassword(String, String) (Line 360)**

```
357         try {
358             Connection connection = getConnection();
359             Statement statement = connection.createStatement();
360             statement.execute("UPDATE PEOPLE SET PASSWORD = '"+ password +"' WHERE USI
361             return null;
```

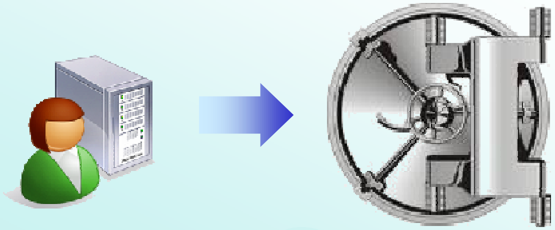
## 3. Developer Fixes or Logs Issues



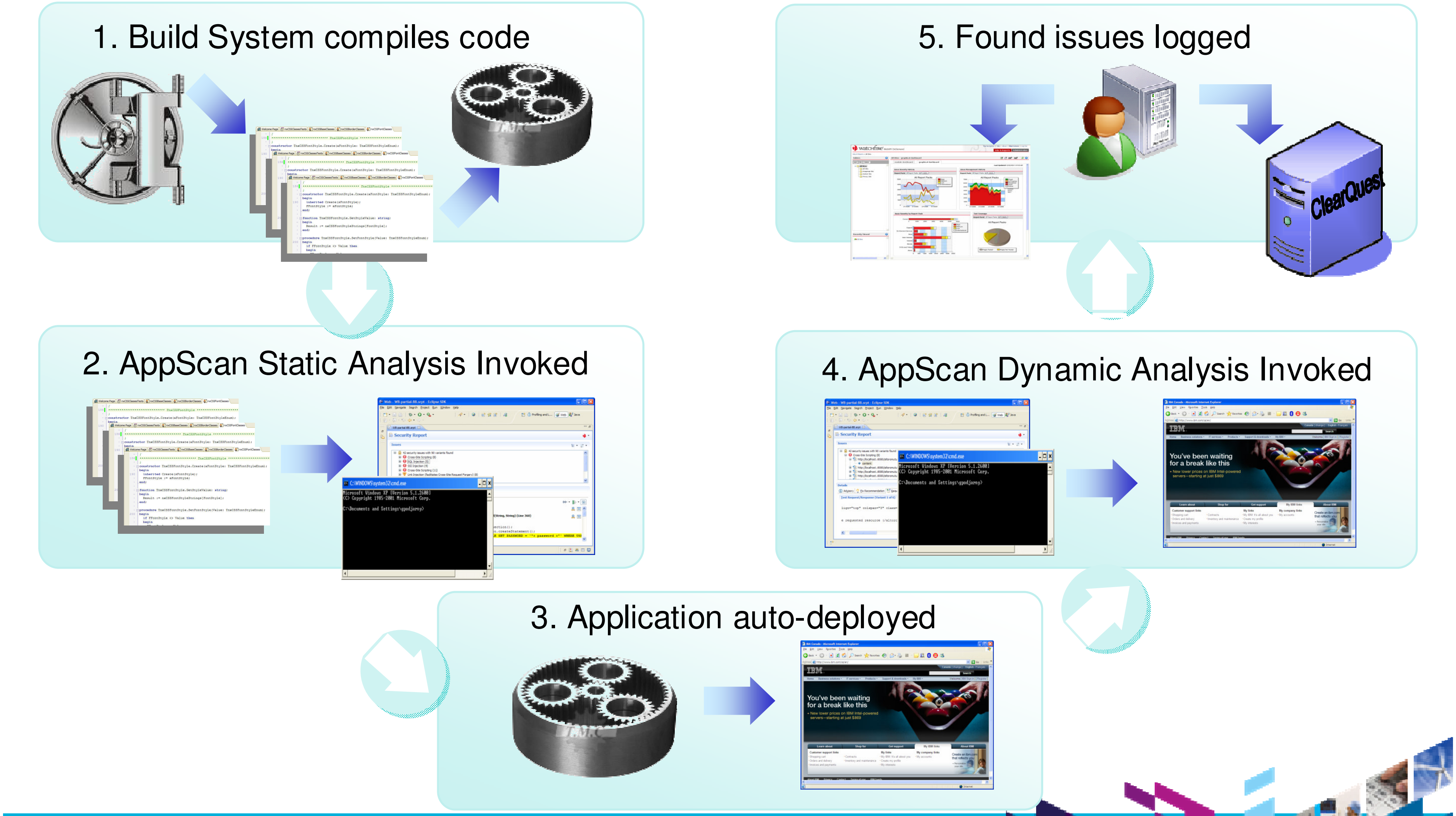
Welcome Page nxCSSClassesTests nxCSSBaseClasses nxCSSBorderClasses nxCSSFontClasses

```
{
****************************** TnxCSSFontStyle **********************
}
constructor TnxCSSFontStyle.Create(aFontStyle: TnxCSSFontStyleEnum);
begin
  inherited Create(sFontStyle);
  FFontStyle := aFontStyle;
end;

function TnxCSSFontStyle.GetStyleValue: string;
begin
  Result := nxCSSFontStyleStrings[FontStyle];
end;

procedure TnxCSSFontStyle.SetFontStyle(Value: TnxCSSFontStyleEnum);
begin
  if FFontStyle <> Value then
  begin
```

## 4. Developer Checks in Code



# AppScan Source Automation Use Case



1. Build System compiles code

2. AppScan Static Analysis Invoked

3. Application auto-deployed

4. AppScan Dynamic Analysis Invoked

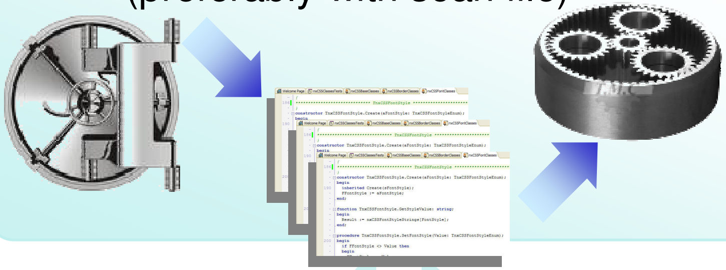
5. Found issues logged

Security Report
C:\WINDOWS\system32\cmd.exe
You've been waiting for a break like this
ClearQuest

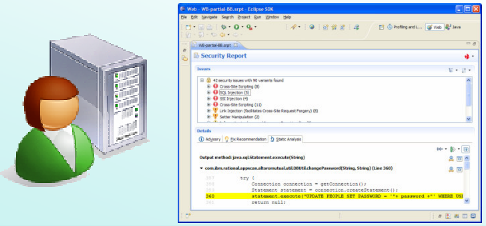
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\gpodjarny>
```

# AppScan Source Edition - Reactive Use-Case

1. Developer receives Defect *
(preferably with scan file)



2. Developer loads scan or
reproduces issue using AppScan Source



Web - WB-partial-BB.srpt - Eclipse SDK
File Edit Navigate Search Project Run Window Help
Profiling and L... Web Java
WB-partial-BB.srpt
Security Report
Issues
Details
Advisory Fix Recommendation Static Analysis

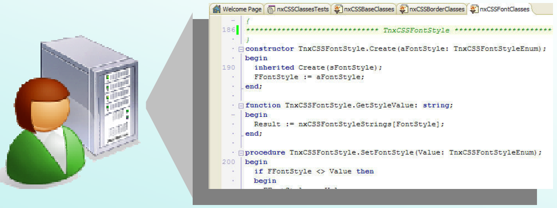
42 security issues with 90 variants found
- Cross-Site Scripting (8)
- SQL Injection (5)
- SSI Injection (4)
- Cross-Site Scripting (11)
- Link Injection (facilitates Cross-Site Request Forgery) (8)
- Setter Manipulation (2)

Output method: java.sql.Statement.execute(String)

com.ibm.rational.appscan.altoromutual.util.DBUtil.changePassword(String, String) (Line 360)

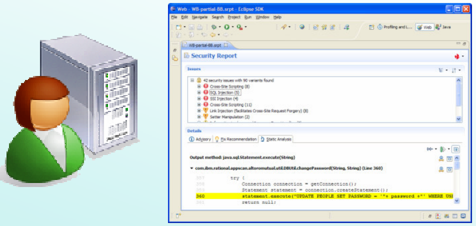
```
            try {
                Connection connection = getConnection();
                Statement statement = connection.createStatement();
360             statement.execute("UPDATE PEOPLE SET PASSWORD = '"+ password +"' WHERE USI
                return null;
```

3. Developer Fixes Issue In Code



```
{
***************************** TnxCSSFontStyle ***********************
}
constructor TnxCSSFontStyle.Create(aFontStyle: TnxCSSFontStyleEnum);
begin
  inherited Create(sFontStyle);
  FFontStyle := aFontStyle;
end;

function TnxCSSFontStyle.GetStyleValue: string;
begin
  Result := nxCSSFontStyleStrings[FontStyle];
end;

procedure TnxCSSFontStyle.SetFontStyle(Value: TnxCSSFontStyleEnum);
begin
  if FFontStyle <> Value then
  begin
```

4. Developer Re-Tests using AppScan Source



Web - WB-partial-BB.srpt - Eclipse SDK
File Edit Navigate Search Project Run Window Help
Profiling and L... Web Java
WB-partial-BB.srpt
Security Report
Issues
Details
Advisory Fix Recommendation Static Analysis

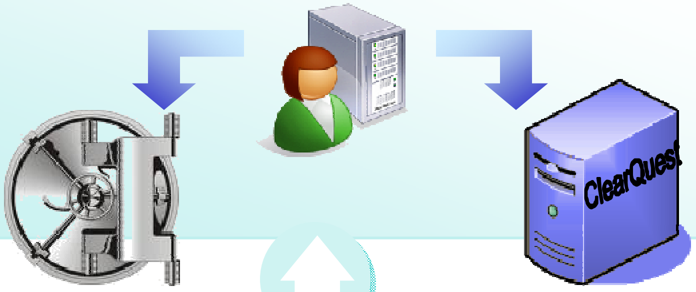
42 security issues with 90 variants found
- Cross-Site Scripting (8)
- SQL Injection (5)
- SSI Injection (4)
- Cross-Site Scripting (11)
- Link Injection (facilitates Cross-Site Request Forgery) (8)
- Setter Manipulation (2)

Output method: java.sql.Statement.execute(String)

com.ibm.rational.appscan.altoromutual.util.DBUtil.changePassword(String, String) (Line 360)

```
            try {
                Connection connection = getConnection();
                Statement statement = connection.createStatement();
360             statement.execute("UPDATE PEOPLE SET PASSWORD = '"+ password +"' WHERE USE
                return null;
```

5. Developer checks in fix and updates defect



*** Defect originating from
other developer, QA or
Build System***

# Addressing organizational security testing requirements

*Enable more testers in the process to alleviate the security bottleneck*

**Rational AppScan Source Edition can be embedded into the development process**

*Collaborative life cycle*

Development & Security Analysts collaborate to achieve greater testing coverage earlier in the development process.

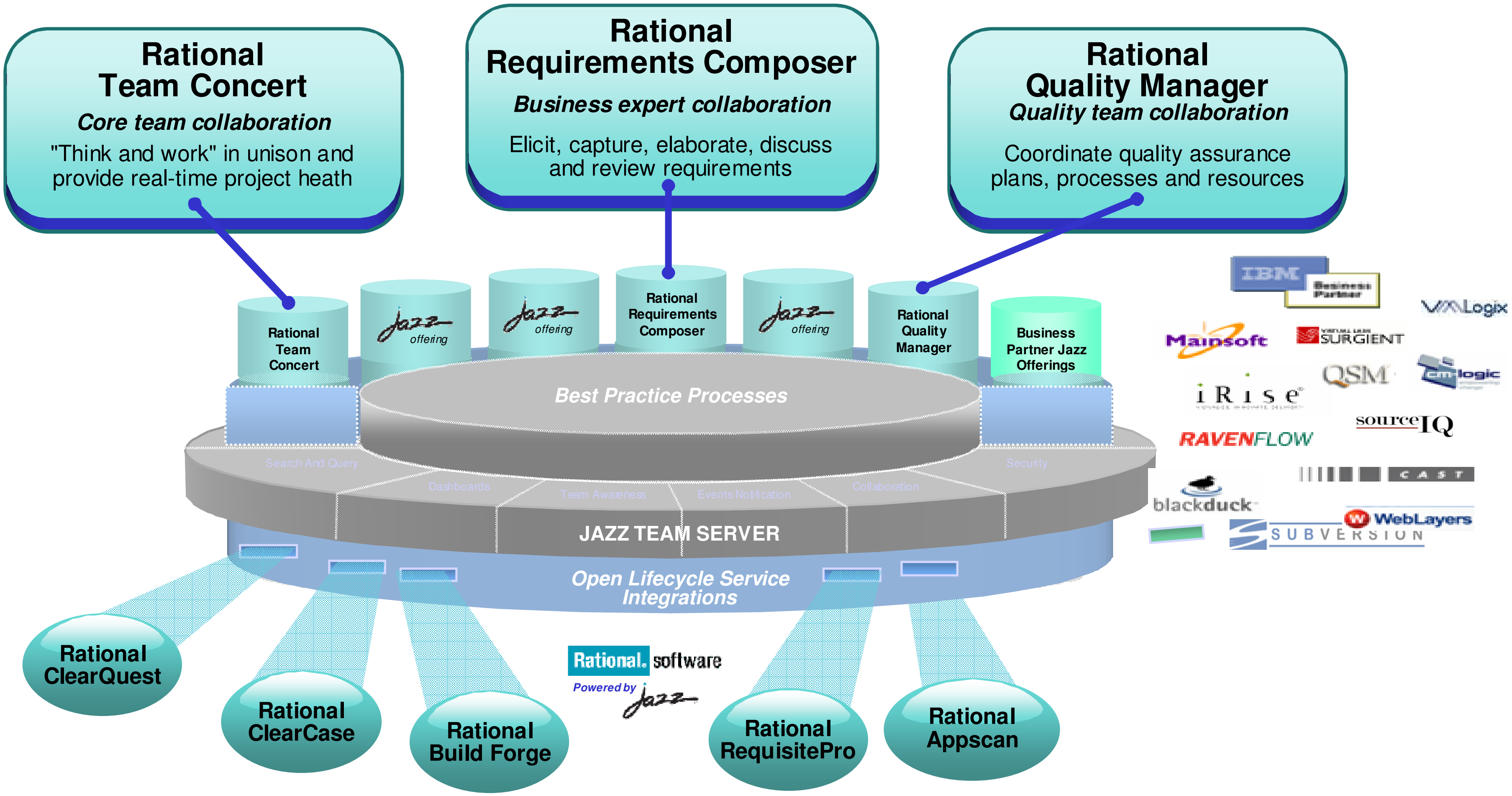
*Powered by automation*

Automate security testing as part of the normal code-build process within existing development environments, eliminating the need for non-security personnel to learn new or advanced security tools

*Govern software delivery*

Govern the process of issue remediation by providing the ability to log security issues directly into defect tracking tools

# SDLC Tight Integration facilitates ease of adoption, usage and traceability:



**Rational Team Concert**

*Core team collaboration*

"Think and work" in unison and provide real-time project heath

**Rational Requirements Composer**

*Business expert collaboration*

Elicit, capture, elaborate, discuss and review requirements

**Rational Quality Manager**

*Quality team collaboration*

Coordinate quality assurance plans, processes and resources

Rational Team Concert

Jazz offering

Jazz offering

Rational Requirements Composer

Jazz offering

Rational Quality Manager

Business Partner Jazz Offerings

*Best Practice Processes*

Search And Query

Dashboards

Team Awareness

Events Notification

Collaboration

Security

JAZZ TEAM SERVER

*Open Lifecycle Service Integrations*

Rational ClearQuest

Rational ClearCase

Rational Build Forge

Rational RequisitePro

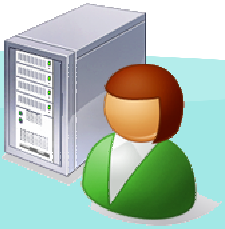
Rational Appscan

# Application Security COE at System Integrator

## 2. Enable Generic Testing Teams to perform Security Test at QA

- *Ensure a strong Security QA check for all the Application Development /Maintenance projects.*
- *Keep the control and visibility of security policies/exposure and improvements in the centralized manner.*
- *Eliminate training requirements for non-security experts by using highly intelligent tools and web based training on security while performing the tests.*
- *Ensure a highly scalable model of adding on QA teams thru client/server technology*
- *Enterprise wide access based/customizable Application Security dashboard, ensuring control on the confidential vulnerability reports and prevent any misuse.*
- *Reduction in the Application Security Audit cost by using perpetual automation tools and also increasing the frequency/coverage of Application to be scanned/rescanned for security Threats*
- *A central client - server model giving feature benefits like* Scalability, Centralizing Reporting, Permission Model, Issue Management , Historical Trending, Centralized Monitoring, Multiple Dashboards, Thin-client, Redundancy & Fail-over etc

# AppScan Enterprise  Edition (Black Box) allows Testing of ready Applications at QA



## Overview

**Rational Enterprise is the Market Leading tool which Automatically Scans all your Web Applications and :**

pinpoint vulnerabilities in web applications

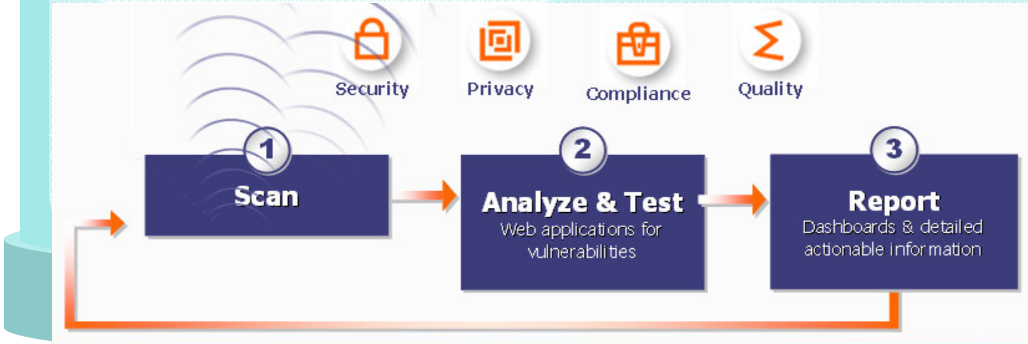
provide guidance for fixing security defects

help ensure compliance with over 40 regulatory requirements

Gives an online enterprise wide dashboard with customized/access controlled view.

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

## How does it do it?



Security

Privacy

Compliance

Quality

1 Scan

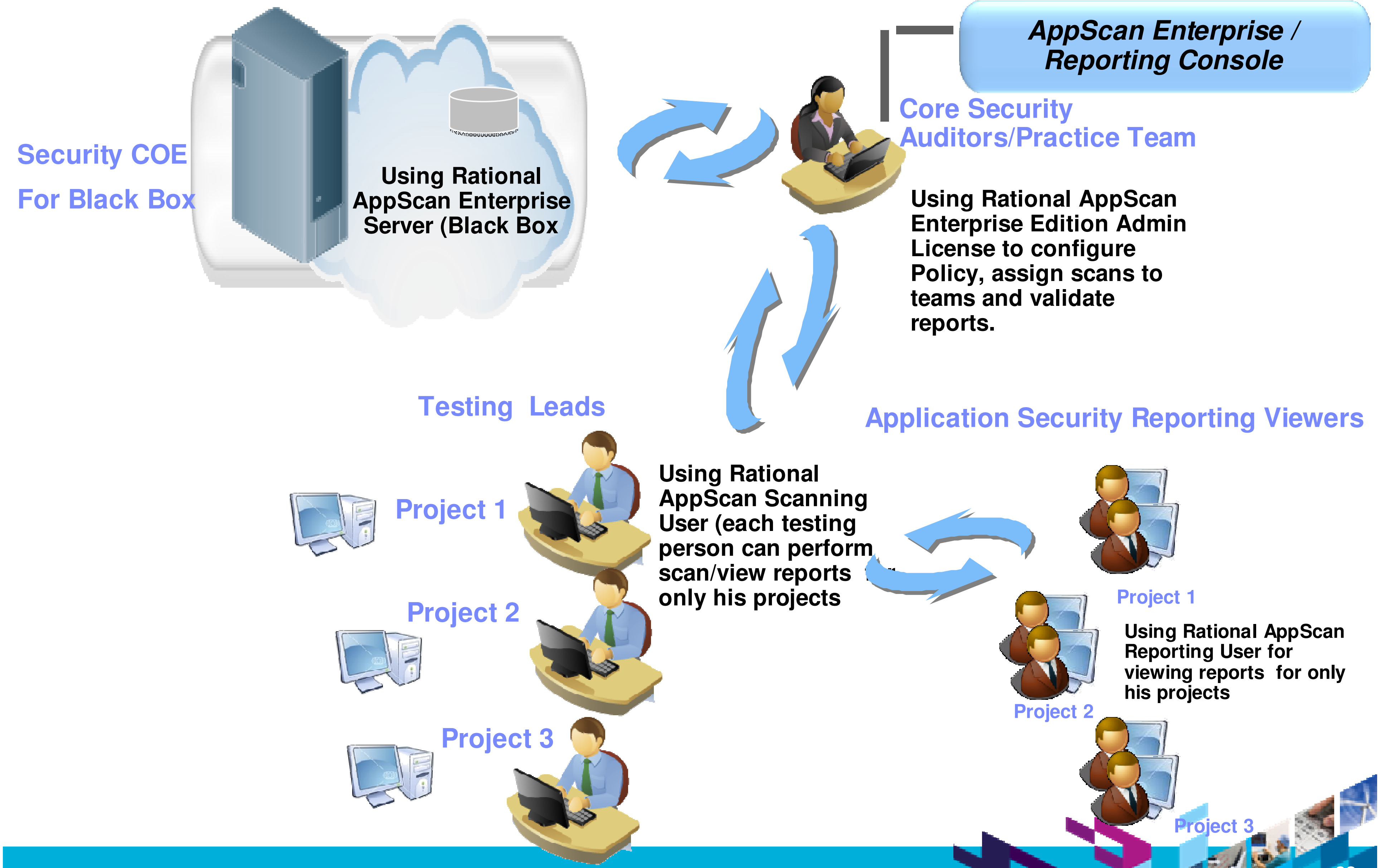
2 Analyze & Test
Web applications for vulnerabilities

3 Report
Dashboards & detailed actionable information

## Checks for vulnerabilities like

- Cross Site Scripting
- SQL Injection
- Buffer Overflow
- Application Malwares
- Denial of Services Attack
- Privilege Escalations
- Flash Vulnerabilities
- And many more….

# Deployment of Security Testing in System Integrator’s QA



Security COE

For Black Box

Using Rational AppScan Enterprise Server (Black Box

AppScan Enterprise / Reporting Console

Core Security Auditors/Practice Team

Using Rational AppScan Enterprise Edition Admin License to configure Policy, assign scans to teams and validate reports.

Testing Leads

Application Security Reporting Viewers

Project 1

Project 2

Project 3

Using Rational AppScan Scanning User (each testing person can perform scan/view reports only his projects

Project 1

Project 2

Project 3

Using Rational AppScan Reporting User for viewing reports for only his projects

# Application Security COE at System Integrator

## 3. Handling Security Test Consulting Projects

- Executing the  Application Security Consulting projects using flexible customer based licensing.

- Provide pdf/attachment free managed services to end client using Securty Dashboards and SaaS offerings.

- 3 different Deployment models to cater to different kind of Consulting Projects. (Models mentioned in later slides)

# Net New Revenue Opportunities for Global SI's in this Space

- Assessment Services
- Expansion of Current Application Testing Services
- Solutions Management
- Remediation Services
- Tools and Technology

# Deployment Model –1 (Traditional Consulting with no option to offer SaaS)

## Traditional Black Box Scanning

- **Modality ---** It is a Desktop technology, so System Integrator Consultant can take the laptop with tool to the client site or any specific network and perform Black Box scan as long as the target URL is reachable

- **Scanning License ---** Annual Appscan Standard Consulting License.

- **Scanning Rights ---** Multiple Applications, Multiple customers, Global.

- **Reporting Mode ---** PDF/HTML based reporting, the reports can be shared as attachments with the client.

- **Concurrency ---** Concurrent desktop based.

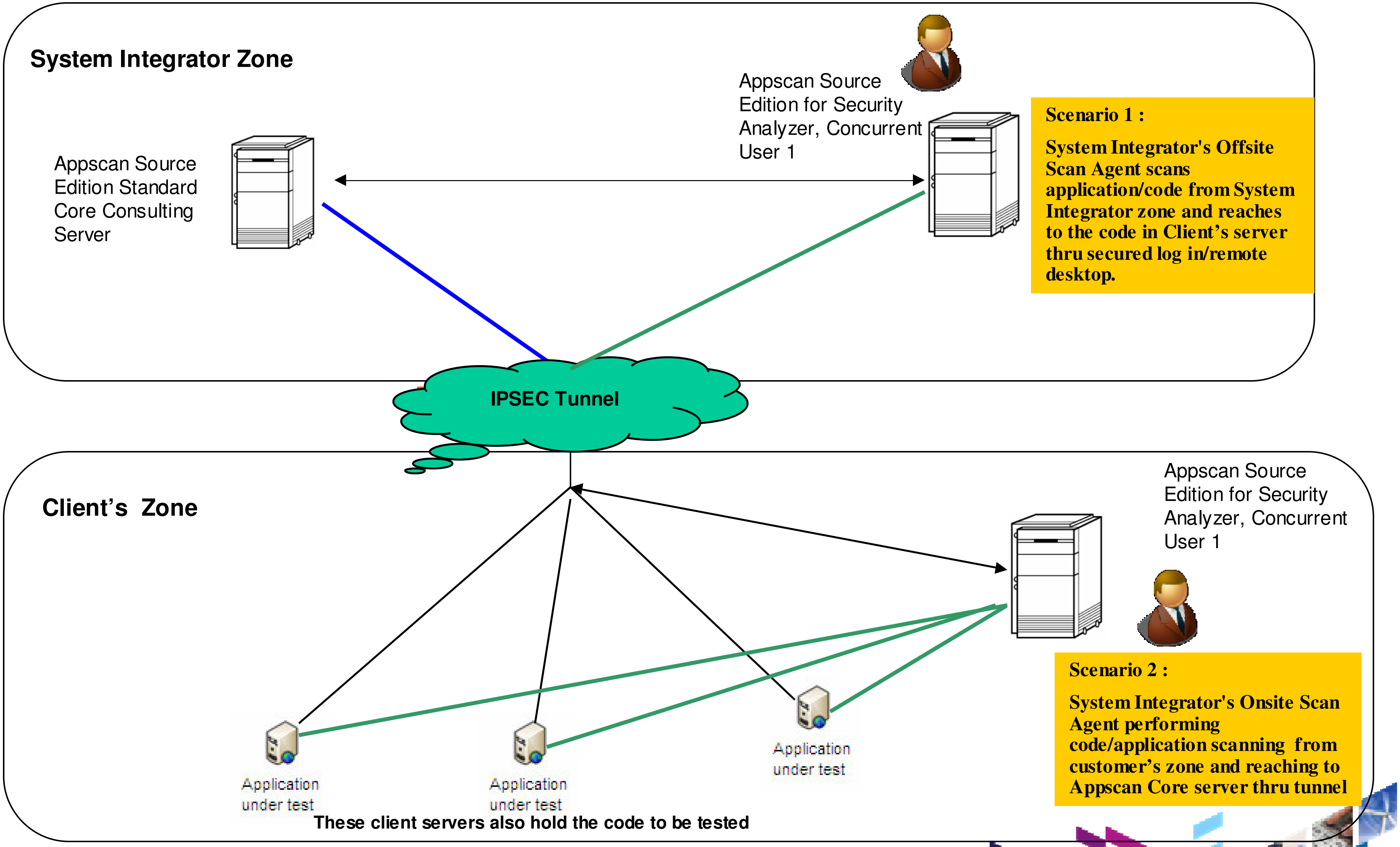
- **Cost ---**

# Deployment Model –1 (Traditional Consulting with no option to offer SaaS)

## Traditional White Box Scanning

- **Modality ---** Scanning can be done by the consultant remotely as per the options mentioned in next slide
- **Scanning License ---** Annual Appscan Source Edition Consulting Bundle which includes 1 Appscan Source Edition Core server +1 Appscan Source Edition for Security Analyzer i.e a scanning agent.
- **Scanning Rights ---** Multiple Applications, Multiple customers, Global.
- **Reporting Mode ---** PDF/HTML based reporting, the reports can be shared as attachments with the client.
- **Concurrency ---** Server is Node Locked but Security Analyzer licenses are concurrent.
- **Cost ---**
- **Subsequent Additional License ----** Additional concurrent Security Analyzer License and additional concurrent Developer License can be purchased without investing in the server again.

# Model 1 - Using the Source Code Scanning tool remotely - Two Possible Scenarios


System Integrator Zone
Appscan Source Edition Standard Core Consulting Server
Appscan Source Edition for Security Analyzer, Concurrent User 1
IPSEC Tunnel
Client's Zone
Appscan Source Edition for Security Analyzer, Concurrent User 1
Application under test
Application under test
Application under test

**Scenario 1 :**

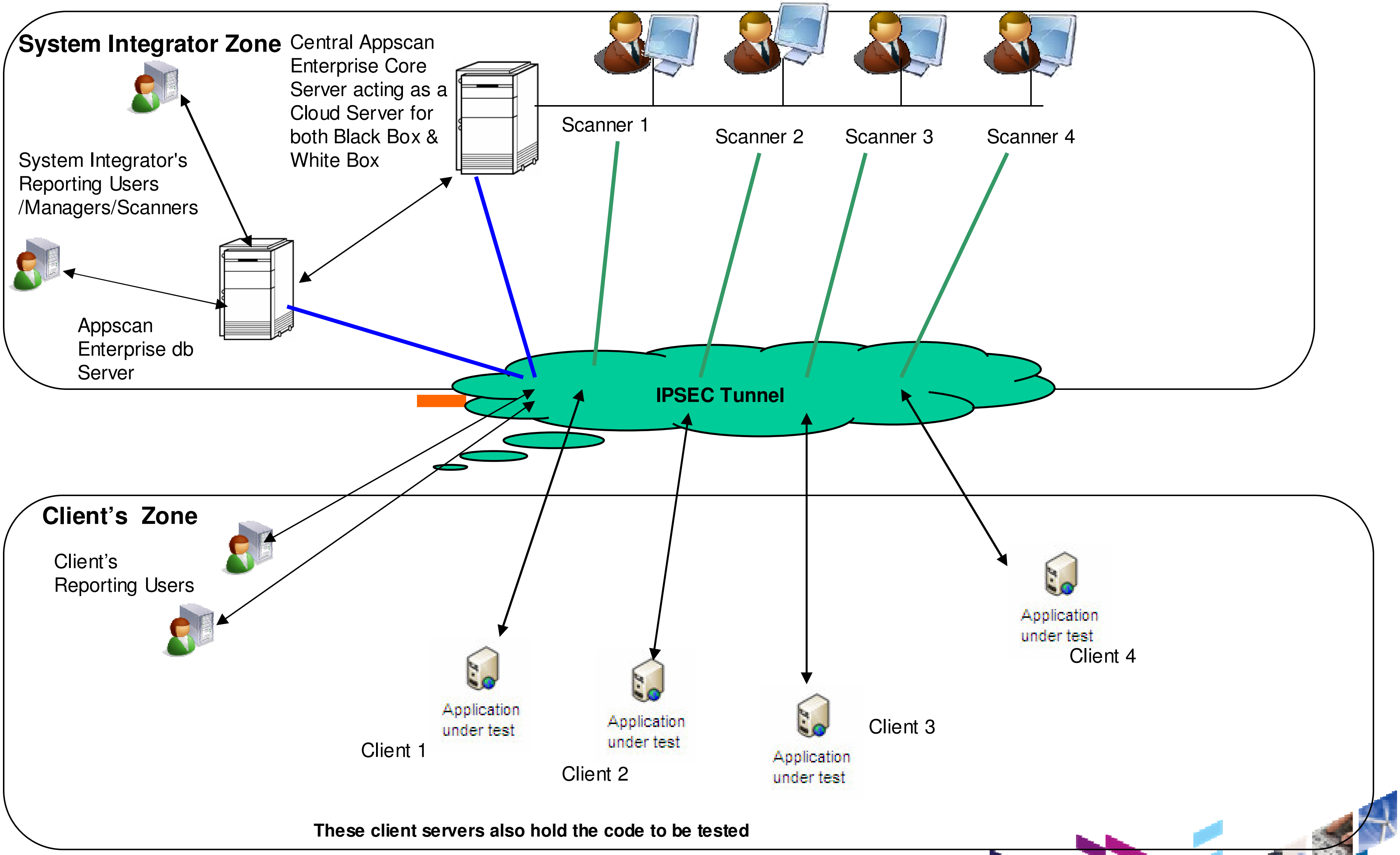
**System Integrator's Offsite Scan Agent scans application/code from System Integrator zone and reaches to the code in Client's server thru secured log in/remote desktop.**

**Scenario 2 :**

**System Integrator's Onsite Scan Agent performing code/application scanning from customer's zone and reaching to Appscan Core server thru tunnel**

These client servers also hold the code to be tested

# Using the Scanning tool remotely - Two Possible Scenarios (Visually)



These client servers also hold the code to be tested

# Deployment Model – 2 (On System Integrator' Private Cloud)

## Central Appscan Enterprise Core set up to Provide both Black Box and White Box Scanning

- **Modality ---** System Integrator provides both the Infrastructure as well as the appsec services / consulting to its' end clients using their own private cloud.

- **Scanning Licenses ---** Monthly licenses for the all the Scanning / Reporting tools.

- **Scanning Rights ---** Single Customer, Multiple Applications, Global.

- **Reporting Mode ---** Dashboard reporting , Customizable as per the client or role of the report user within client side.

- **Cost ---** Mentioned in the Bill of Material attached in the next slide.

# Deployment Model – 3 (System Integrator uses IBM Cloud to offer Black Box Consulting)

## On IBM Cloud, Black Box Scanning

- **Modality ---** For every new client System Integrator uses IBM Cloud to perform Scans, Dash boarding and SaaS access of scanning tool to the end client. System Integrator consultants performs scans. consulting and services. There will be a tri partite contract between IBM, System Integrator and Client.
- **Scanning License ---** Annual Appscan On demand Licenses with different limitation of Web-pages scanned.

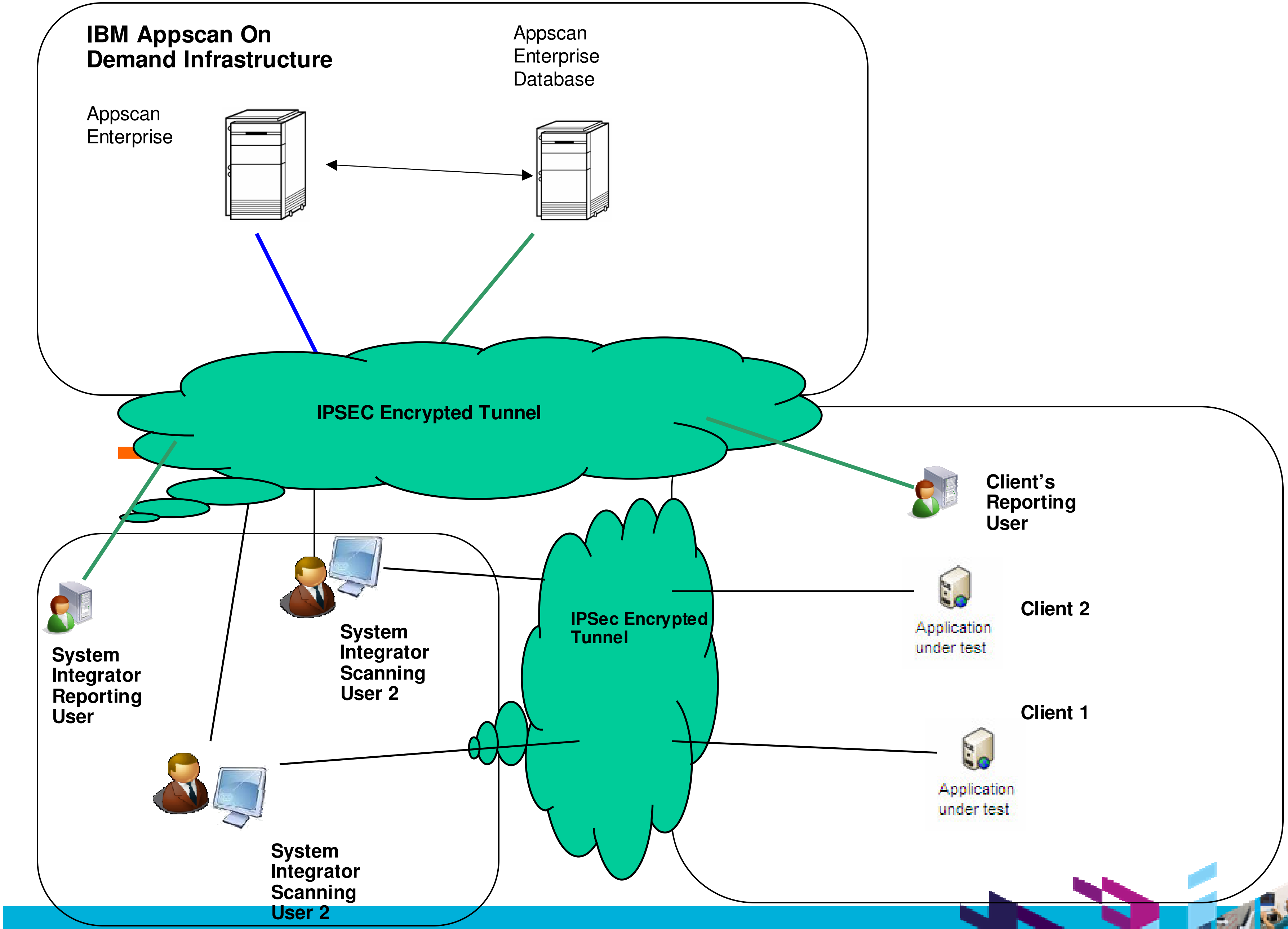
Appscan On Demand for Small Business --- 5 Users --- 1,000 web pages ----

Appscan On Demand for Medium Business – 10 Users – 10,000 web pages ---

Appscan On Demand for Large Business ---- 25 Users – 100,000 web pages ----

- **Scanning Rights ---** One license used for one customer. If required, Remote scanning rights can be assigned to the End Client by System Integrator.
- **Reporting Mode ---** Dashboard reporting , Customizable as per the client or role of the report user within client side.
- **Concurrency ---** User defined licenses.
- **Cost ---** As mentioned above
- **Subsequent Additional License ----** Same as mentioned above.

*******Licensing details of White Box solution on “IBM Cloud” are being frozen as of now, can be shared on specific request.***


IBM Appscan On Demand Infrastructure
Appscan Enterprise Database
Appscan Enterprise
IPSEC Encrypted Tunnel
Client's Reporting User
IPSec Encrypted Tunnel
Application under test
Client 2
Client 1
Application under test
System Integrator Reporting User
System Integrator Scanning User 2
System Integrator Scanning User 2

# IBM Avenues of Investment in System Integrator as a Partner for Application Security

- Lab/COE Branding/Co-Marketing/Marketing
- Joint Press Release
- Sales/Pre-Sales Enablement
- Workshops
- Elite member of IBM Security Customer Council
- RFP Support
- IBM Management Focus with direct connect to AppSec Thought Leaders
- Lab Advocacy
- Certifications
- IBM Strategy & Roadmap discussions
- Success Stories – publish/demonstrate capability at IBM WW Conferences and events attended by top Rational customers

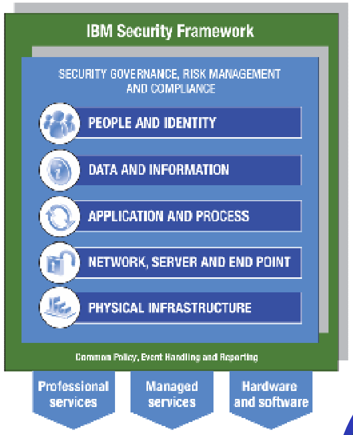
# Why IBM?

- **IBM continues to demonstrate leadership in security**
  - IBM Wins ‘Best Security Company’
  - IBM recognized as International Association of Privacy Professionals “Top Privacy Innovators” in 2009
- **Rational is #1 in Application Security Testing Market Share**
  - According to Gartner and IDC
- **Complete security from IBM Security Solutions**
  - 5 Security Pillars
  - Enterprise-wide coverage of application security from design through development and into production
  - Secure Engineering Framework – security practices employed by IBM and for customers (Rebook)
- **Rational AppScan breadth of technologies and offerings**
  - Solutions for all SDLC stakeholder use cases
  - Leverages best-of-breed static and dynamic analysis
  - Over 60 application vulnerability management innovations patented or publically disclosed
- **Commitment to customer success – R&D Investment**
  - More than 100 resources, 6 labs, plus extend R&D teams

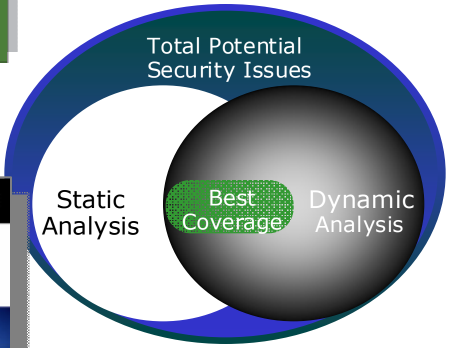
SC MAGAZINE AWARDS 2010 WINNER

**Excellence Award:**
**2010 Best Security Company**

2007 Best Security Company – Watchfire
2006 Best Security Company - ISS



2010 iapp Celebrating Ten Years



IBM

Security in Development: The IBM Secure Engineering Framework

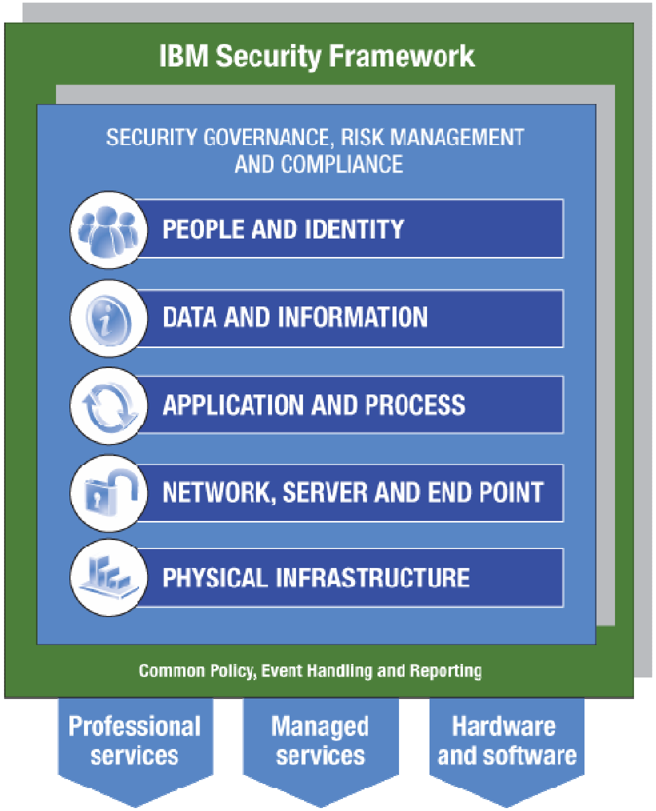
Redguides for Business Leaders

Danny Allan
Tim Hahn
Andras Szakal
Jim Whitmore
Axel Buecker

- Investigating common development processes and the IBM Integrated Product Development process
- Emphasizing security awareness and requirements in the software development process
- Discussing test and vulnerability assessments

Redbooks

# IBM Security Framework



IBM Security Framework

SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

PEOPLE AND IDENTITY

DATA AND INFORMATION

APPLICATION AND PROCESS

NETWORK, SERVER AND END POINT

PHYSICAL INFRASTRUCTURE

Common Policy, Event Handling and Reporting

Professional services

Managed services

Hardware and software

**IBM Security: Improving service, managing risk and reducing cost of Security without compromise**

Market data source: IBM Security Landscape, Jan 2009

- **IBM is the *only security vendor* in the market today with *end-to-end coverage of critical controls***
- IBM Proof Points:
  - 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 7B security events per day for clients
  - IBM Security Framework, Security Blueprint

# Why IBM - Recent accolades

"IDC believes IBM has recognized this trend and has created comprehensive security packages that leverage various products to provide for multiple layers of security to customers."

***— Charles Kolodgy, IDC, March 2010***

IBM and a few others can help any sized customer with security, regardless of whether they need help securing their business, implementing an enterprise security initiative, or fixing a big security problem."

***— Jon Oltsik, Enterprise Strategy Group, March 2010***

In light of IBM's growing presence in security and compliance, and the weight of its impact on the larger issues of business risk control, these factors should make IBM a primary partner to consider in shaping strategy and evaluating technologies and services that make a difference. Few others have the range of capabilities of today's IBM for addressing the challenge—fewer still have the resources of an IBM for understanding the nature of business risks and emerging threats, and how best to address them going forward."

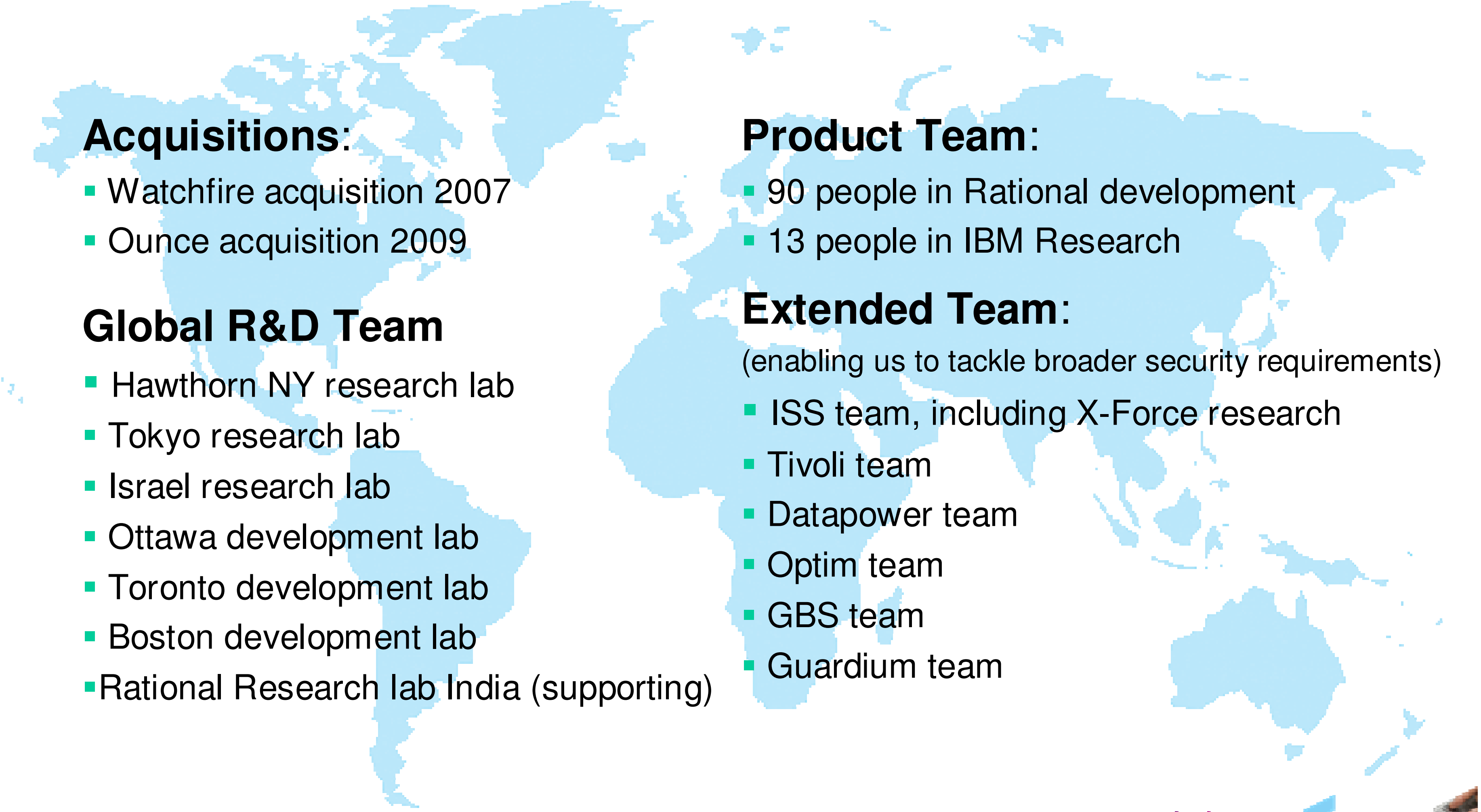
***High Performers and Foundational Controls: Building a Strategy for Security and Risk Management - Enterprise Management Associates® (EMA™), Dec 2009***

SC MAGAZINE AWARDS 2010 WINNER Honored in the U.S.

IBM was named the **"Best Security Company"*** by SC Magazine

Source: SC Magazine award, March 2, 2010

# IBM Investment & Commitment to Customer Success



## Acquisitions:

- Watchfire acquisition 2007
- Ounce acquisition 2009

## Global R&D Team

- Hawthorn NY research lab
- Tokyo research lab
- Israel research lab
- Ottawa development lab
- Toronto development lab
- Boston development lab
- Rational Research lab India (supporting)

## Product Team:

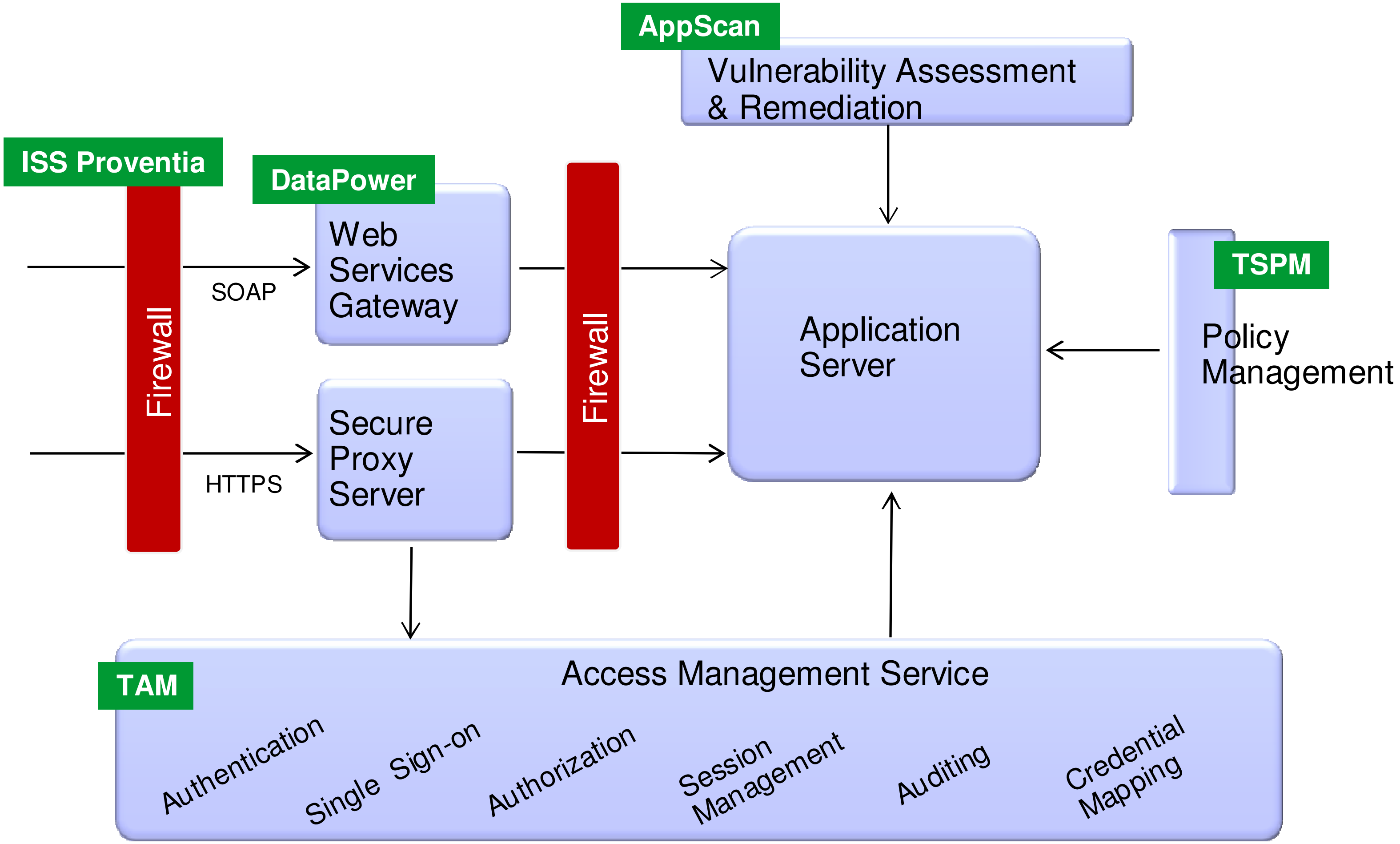
- 90 people in Rational development
- 13 people in IBM Research

## Extended Team:

(enabling us to tackle broader security requirements)

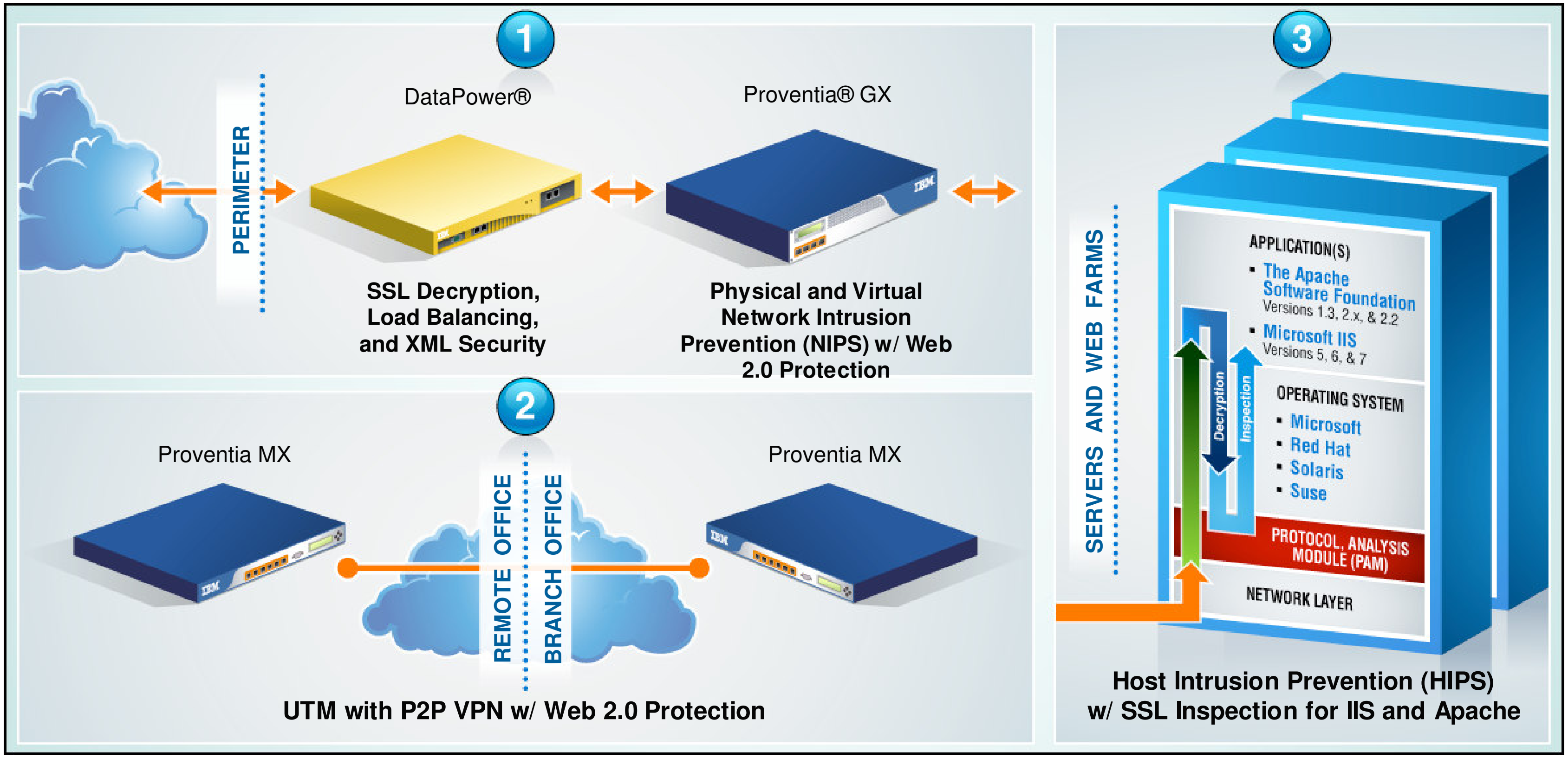
- ISS team, including X-Force research
- Tivoli team
- Datapower team
- Optim team
- GBS team
- Guardium team

# IBM Security Solutions End-to-End Application Coverage



TAM = Tivoli Access Manager
TSPM = Tivoli Security Policy Manager
DataPower = Secure XML Gateway

# Integrate Web application security from Network to Host


1
PERIMETER
DataPower®
Proventia® GX
SSL Decryption, Load Balancing, and XML Security
Physical and Virtual Network Intrusion Prevention (NIPS) w/ Web 2.0 Protection
2
Proventia MX
Proventia MX
REMOTE OFFICE
BRANCH OFFICE
UTM with P2P VPN w/ Web 2.0 Protection
3
SERVERS AND WEB FARMS
APPLICATION(S)
The Apache Software Foundation
Versions 1.3, 2.x, & 2.2
Microsoft IIS
Versions 5, 6, & 7
Decryption
Inspection
OPERATING SYSTEM
Microsoft
Red Hat
Solaris
Suse
PROTOCOL ANALYSIS MODULE (PAM)
NETWORK LAYER
Host Intrusion Prevention (HIPS) w/ SSL Inspection for IIS and Apache

# Integrate Web application security from Network to Host

## Intrusion prevention and protection for:

- **Web 2.0:** JSON (java script object notation) hijacking
- **Database:** SQL, LDAP and XPath injection
- **Web application protection:** shell command, server side include, XSS and directory traversal

## X-Force® protection across all Proventia® products:

- **Network Protection**: IBM Proventia Network Intrusion Prevention System (IPS)
- **Remote / Branch Office**: IBM Proventia Network Multi-Function Security (MFS)
- **Host Protection**: IBM Proventia Server IPS

## Benefits:

- Consolidated security products designed to reduce the cost and complexity of deploying and maintaining multiple point products
- Achieve PCI compliance for DSS 6.6 (June 30, 2008)
- Ease of use with wizard GUI for applying IPS policies to OWASP top vulnerabilities

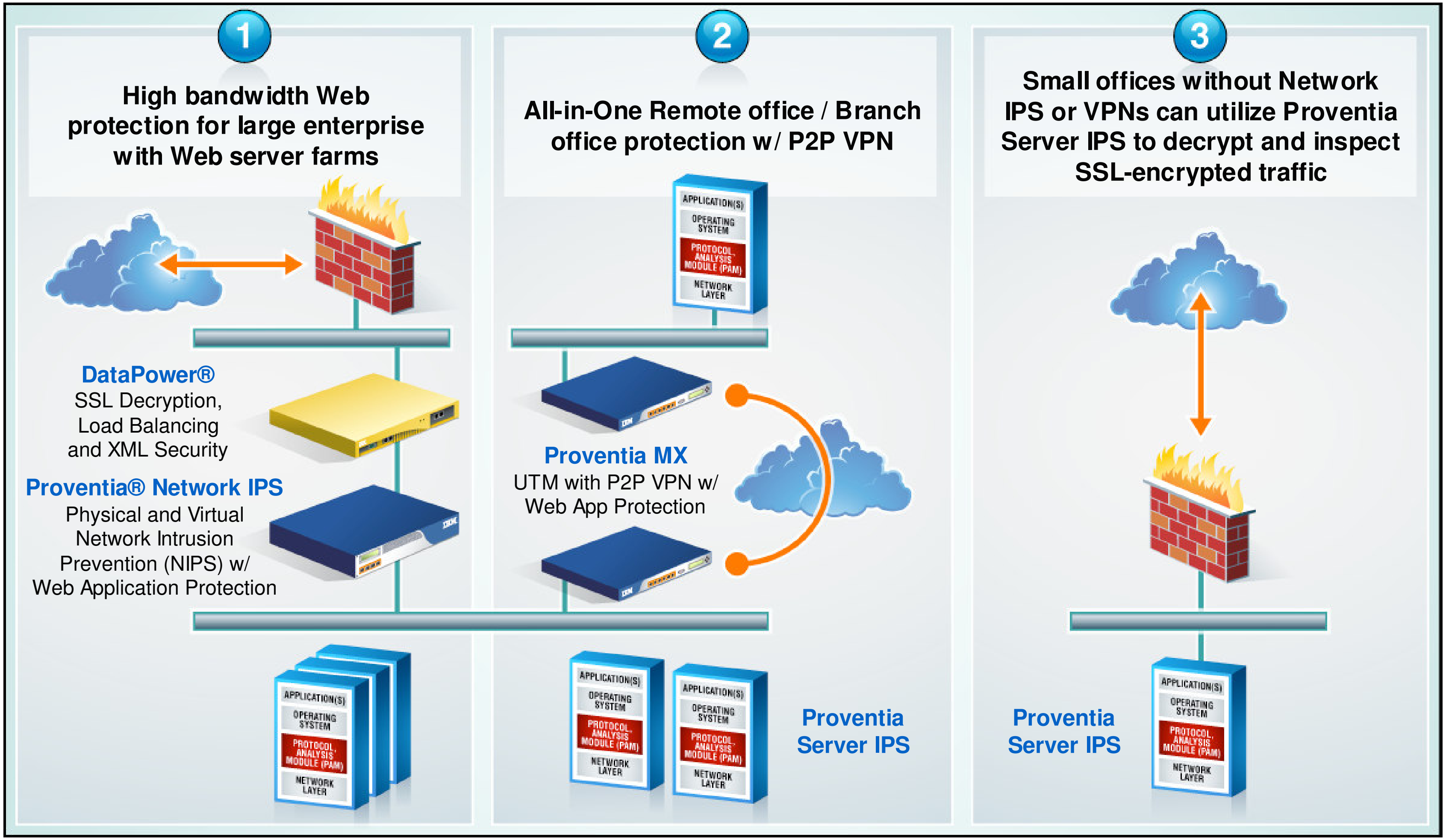
Secure code development and vulnerability management

Protect Web applications from potential attacks

Deliver security and performance in Web services and SOA

Manage secure Web applications

# IBM Proventia Web security


1
High bandwidth Web protection for large enterprise with Web server farms
DataPower®
SSL Decryption, Load Balancing and XML Security
Proventia® Network IPS
Physical and Virtual Network Intrusion Prevention (NIPS) w/ Web Application Protection
APPLICATION(S)
OPERATING SYSTEM
PROTOCOL ANALYSIS MODULE (PAM)
NETWORK LAYER
2
All-in-One Remote office / Branch office protection w/ P2P VPN
Proventia MX
UTM with P2P VPN w/ Web App Protection
Proventia Server IPS
3
Small offices without Network IPS or VPNs can utilize Proventia Server IPS to decrypt and inspect SSL-encrypted traffic
Proventia Server IPS

Secure code development and vulnerability management

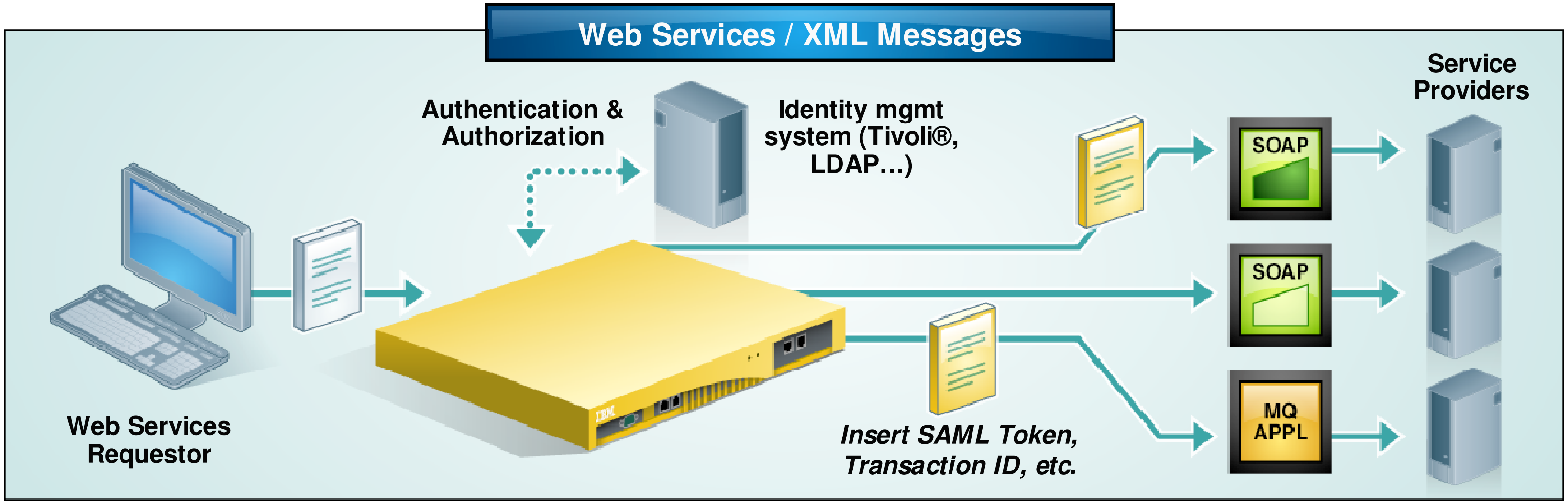
Protect Web applications from potential attacks

Deliver security and performance in Web services and SOA

Manage secure Web applications

# Comprehensive Web services and XML security

## WebSphere DataPower appliances


Web Services / XML Messages
Authentication & Authorization
Identity mgmt system (Tivoli®, LDAP…)
Service Providers
SOAP
SOAP
MQ APPL
Web Services Requestor
Insert SAML Token, Transaction ID, etc.

- **Encryption of transport layer –** HTTP, HTTPS, SSL
- **XML/SOAP Firewall –** Filter on any content, metadata or network variables
- **Data Validation –** Enforce incoming/outgoing XML schema, well-formedness
- **Field Level Security –** WS-Security, encrypt and sign individual fields, non-repudiation

- **Access Control (AAA) –** Authentication, Authorization, Accountability enforces access policy stored in an Identity Management Solution
- **Message Enrichment –** Insert header info, SAML token, Kerberos token and transaction ID
- **Anti Virus Protection –** Integrates with corporate virus checking through ICAP protocol
- **Security standards –** WS-Security, WS-Policy, SAML, XACML, WS-Trust and WS-Addressing

Secure code development and vulnerability management
Protect Web applications from potential attacks
Deliver security and performance in Web services and SOA
Manage secure Web applications

# Together Proventia® Web application security and WebSphere® DataPower® provide full Web Application Firewall (WAF) functionality

- **Proventia Web Application Security Features**
  - Buffer overflow exploits
  - CGI-BIN parameter manipulation
  - Form/hidden field manipulation
  - Forceful browsing
  - Cross-site scripting (XSS)
  - Command injection
  - SQL injection
  - Web site defacement
  - Well-known platform vulnerabilities
  - Zero-day exploits

- **DataPower Features**
  - Cookie watermarking (sign and/or encrypt)
  - Customizable error handling
  - SSL Acceleration and Termination (Link)
  - Dynamic routing and load balancing
  - Session handling policies
  - Rate limiting and traffic throttling/shaping
  - General name-value criteria boundary profiles for:
    - Query string and form parameters
    - HTTP headers
    - Cookies

**Eliminate the need to purchase a stand-alone WAF**

Secure code development and vulnerability management

Protect Web applications from potential attacks

**Deliver security and performance in Web services and SOA**

Manage secure Web applications

Questions

**www.ibm/software/rational**