IBM Security Solutions

Security By Design For The Smarter Planet

Keith Pope
Rational Application Security Leader EMEA

Innovate2010
The Rational Software Conference

Let's build a smarter planet.

The premiere software and product delivery event.
4 de Noviembre, Madrid

Agenda

- Market Trends
- IBM Application Security
- IBM Secure by Design
- Rational Application Security (Appscan)

The Smarter Planet

Our world is getting **Instrumented**

Our world is getting **Interconnected**

Our world is getting **Intelligent**

The Costs from Security Breaches are Staggering

285 MILLION RECORDS COMPROMISED IN 2008

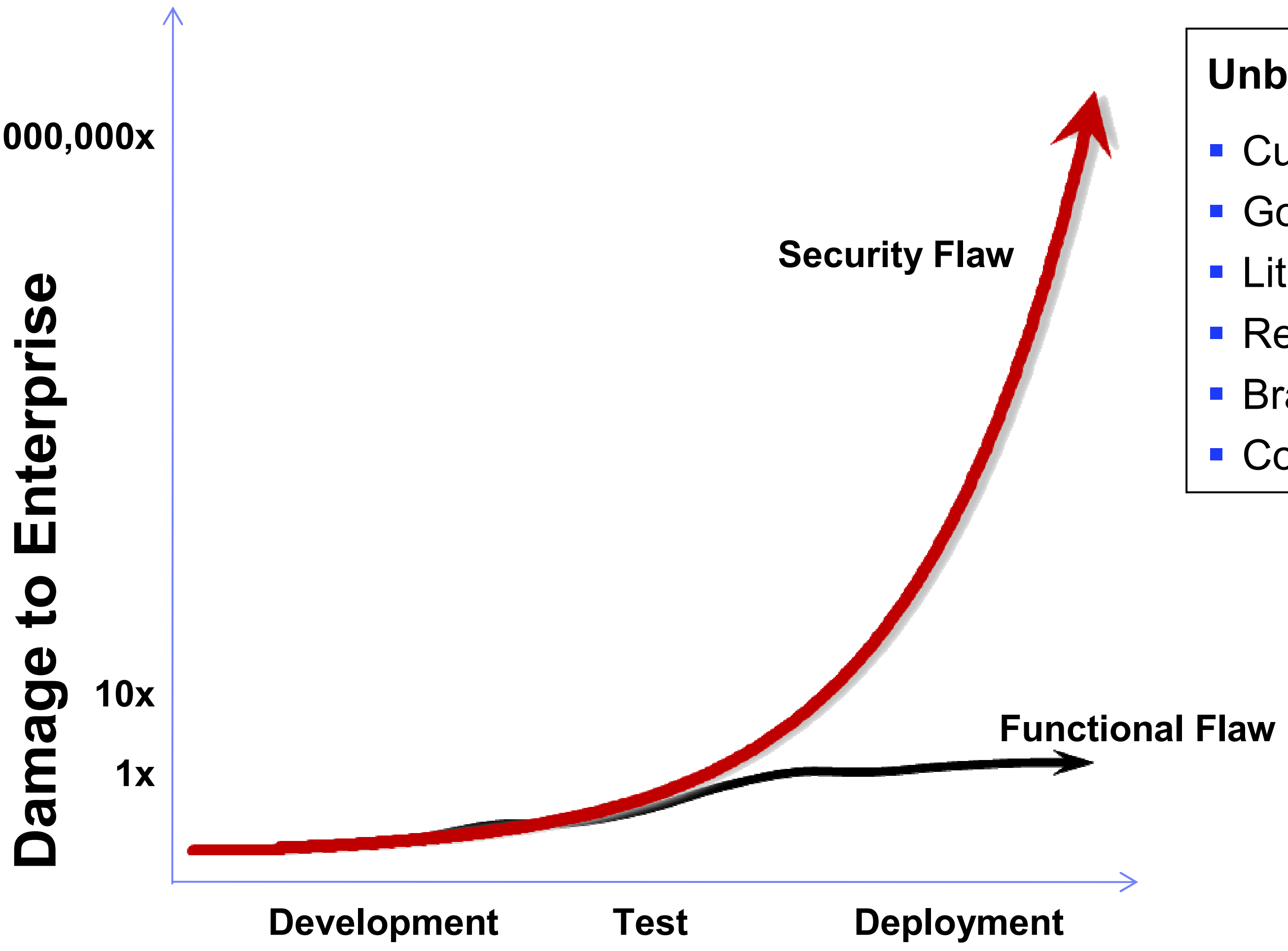
Verizon 2009 data Breach Investigations Report

$204 COST PER COMPROMISED RECORD

Ponemon 2009-2010 Cost of a data Breach Report

TRANSLATES TO $58.1B COST TO CORPORATIONS

Sources of Security Breach Costs



Unbudgeted Costs:

- Customer notification / care
- Government fines
- Litigation
- Reputational damage
- Brand erosion
- Cost to repair

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 **$204** per compromised customer record (**£112** in the UK)

Reducing Costs

Source Code Scanning can deliver around 44k per application in reduced costs with remediation times cut from an average 10 days to a couple of hours

Source http://searchcompliance.techtarget.com/news/article/0,289142,sid195_gci1375707,00.html

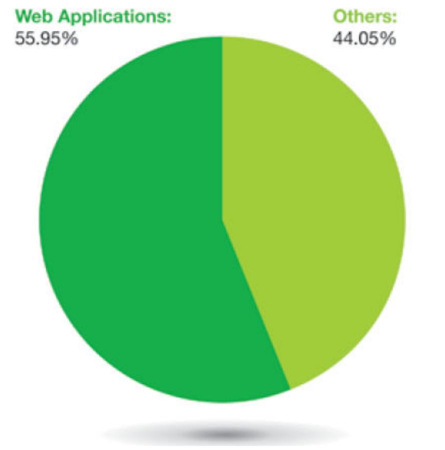
Agenda

- Market Trends
- IBM Application Security
- IBM Secure by Design
- Rational Application Security – AppScan

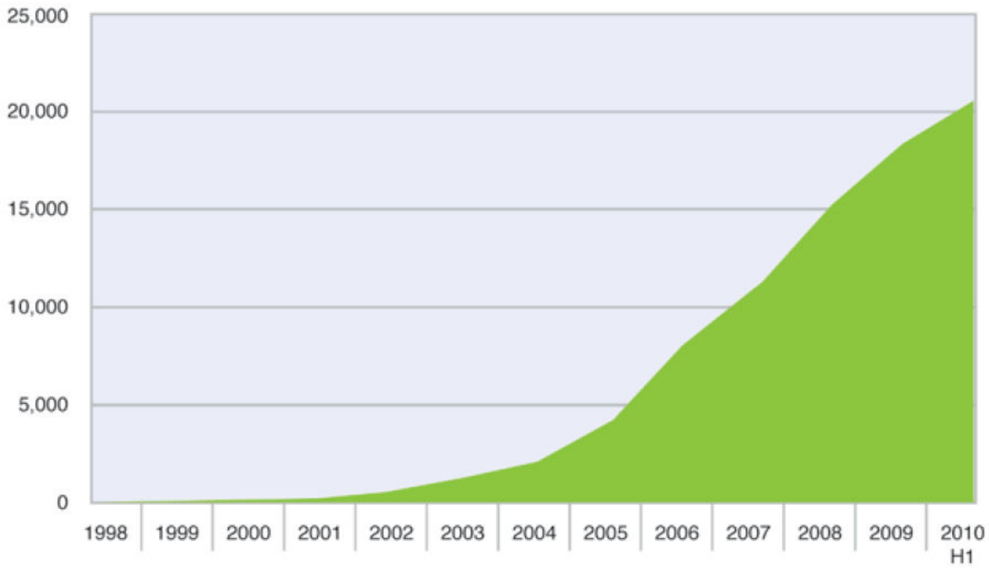
Web Application Vulnerabilities are still the greatest source of risk for organizations

- **55%** of all vulnerabilities are Web application vulnerabilities.
- Cross-Site Scripting & SQL injection vulnerabilities continue to dominate.
- **88%** of web application vulnerabilities affect plug-ins and not the base platform

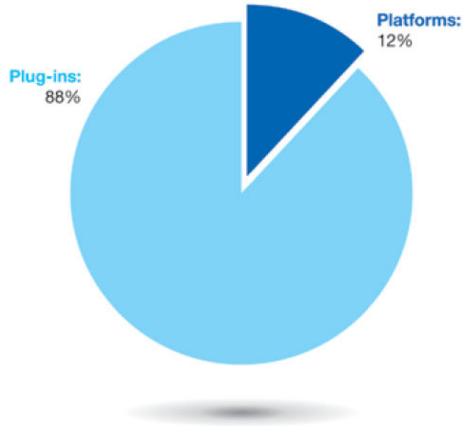
Percentage of Vulnerability Disclosures that Affect Web Applications 2010 H1



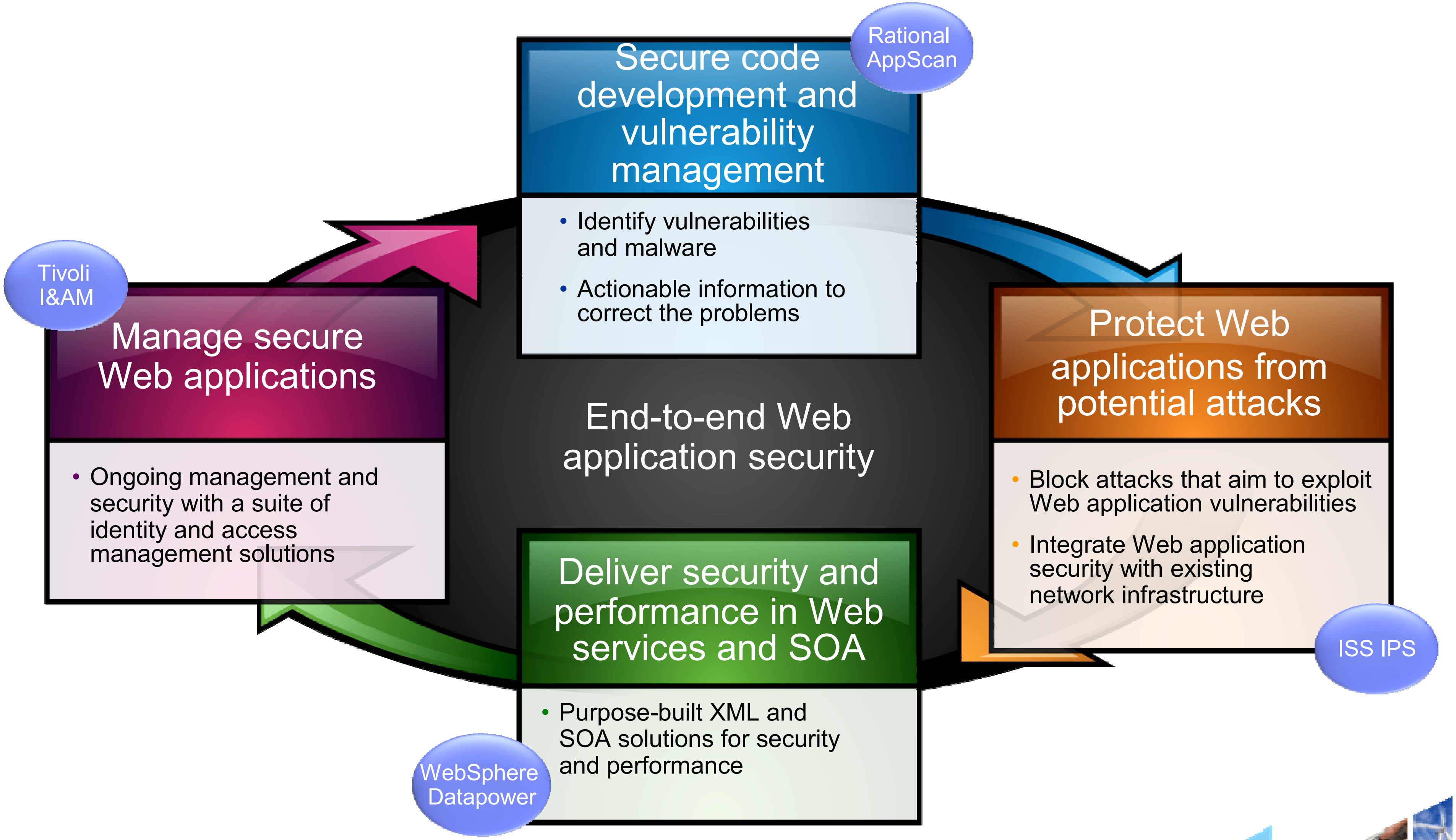
Cumulative Count of Web Application Vulnerability Disclosures 1998-2010 H1



Percentage of All Vulnerability Disclosures that Affect Web Application Platforms and Their Plug-ins 2010 H1



IBM Web application security for a smarter planet



End-to-end Web application security

Rational AppScan

Secure code development and vulnerability management

- Identify vulnerabilities and malware
- Actionable information to correct the problems

ISS IPS

Protect Web applications from potential attacks

- Block attacks that aim to exploit Web application vulnerabilities
- Integrate Web application security with existing network infrastructure

WebSphere Datapower

Deliver security and performance in Web services and SOA

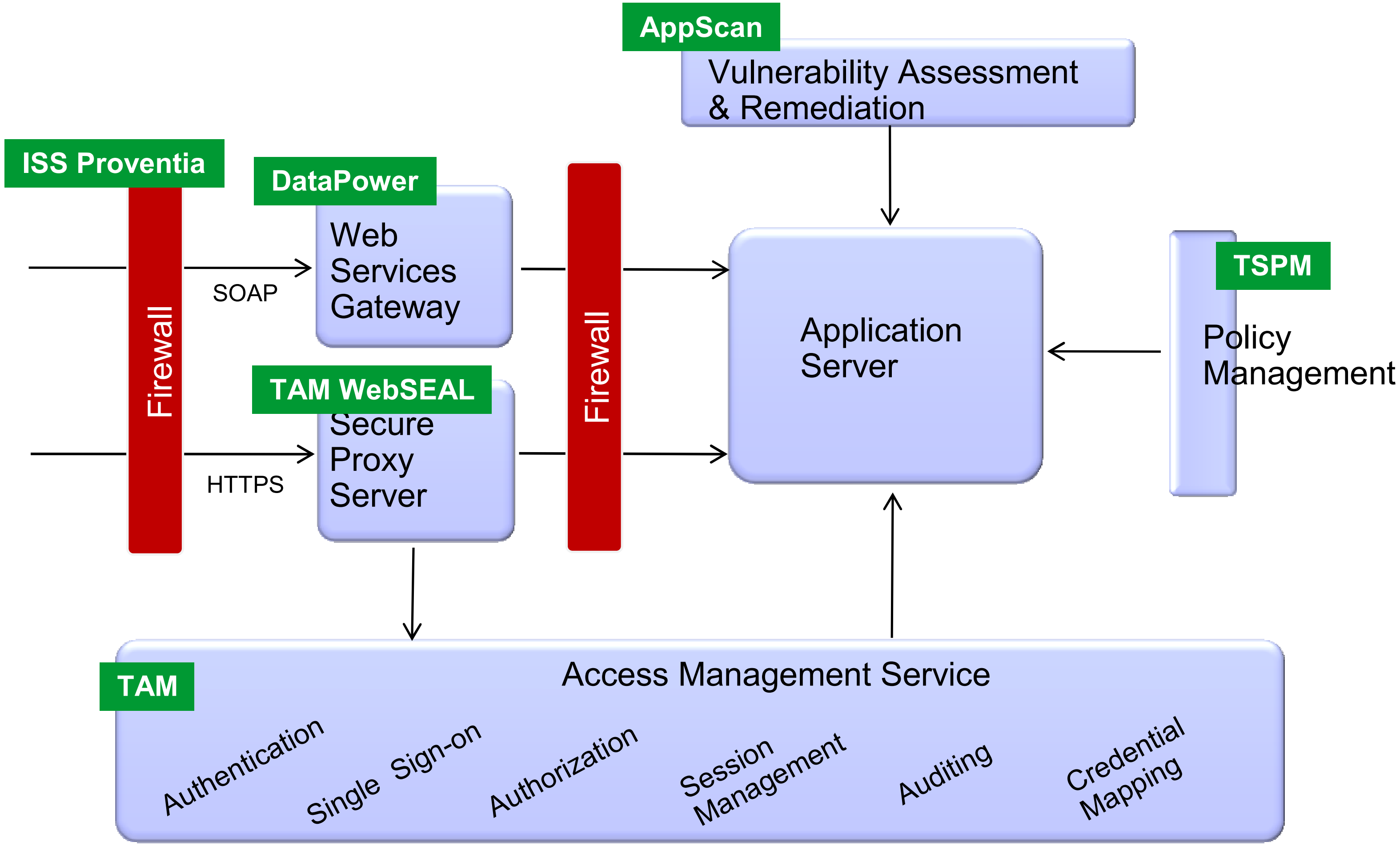
- Purpose-built XML and SOA solutions for security and performance

Tivoli I&AM

Manage secure Web applications

- Ongoing management and security with a suite of identity and access management solutions

IBM Security Solutions End-to-End Application Coverage



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

Why are Web Applications so Vulnerable?

- Developers are mandated to deliver functionality on-time and on-budget - but not to develop secure applications
- Developers are not generally educated in secure code practices
- Product innovation is driving development of increasingly complicated software for a Smarter Planet

Globalization and Globally Available Resources
Access to streams of information in the Realtime
INTERNET
facebook
myspace
iTunes
Google
Billions of mobile devices accessing the Web
New Forms of Collaboration

Volumes of applications continue to be deployed that are riddled with security flaws…

…and are non compliant with industry regulations

Agenda

- IBM Security Framework
- Market Trends
- IBM Application Security
- IBM Secure by Design
- Rational Application Security (Appscan)

It’s time to start thinking differently about security

Build products and services that are ***Secure by Design***

Safely and Securely adopt new forms technology and business models

Let’s make innovation real

Let’s deliver new services faster

Let’s reduce costs

IBM executes on Secure by Design

Secure by Design – Element #1

Develop an understanding of the design point for security

Determine how security, compliance and dependability are assessed

Take those requirements into consideration when designing the application, not after it is already deployed

Secure by Design – Element #2

Be aware of impending threats

Designs must incorporate a balanced view of risk that includes the urgency of security

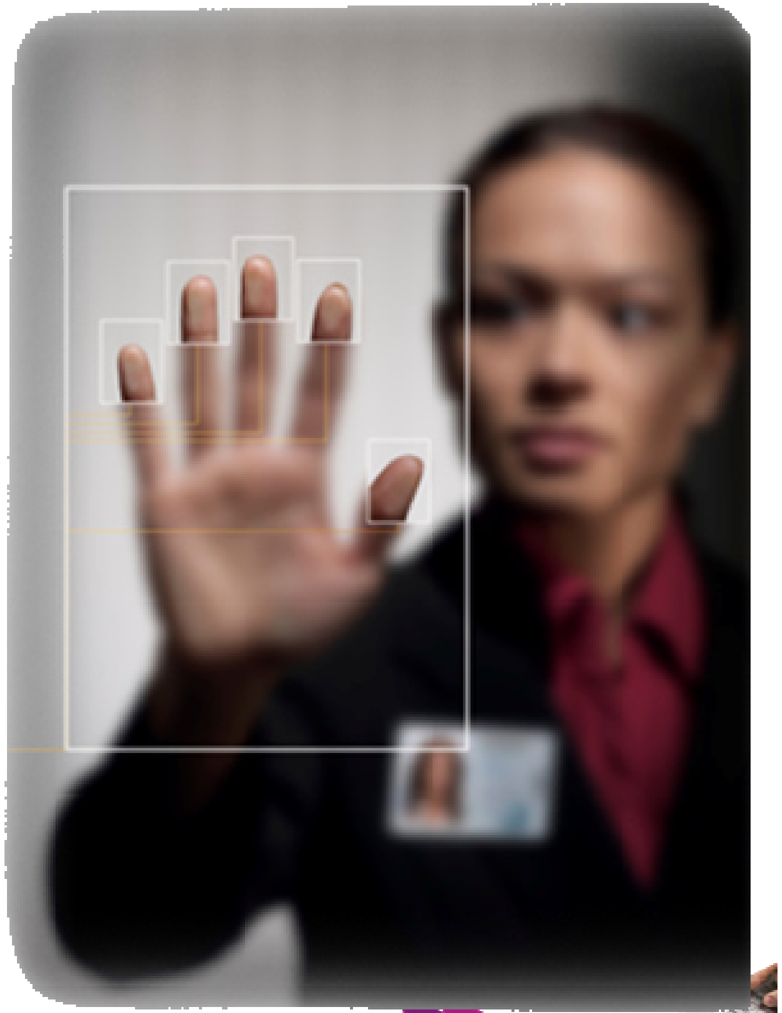
Maintaining an up-to-date view of their possible impact requires a level of commitment and knowledge

Secure by Design – Element #3

Protect Your Infrastructure

Utilize technologies that provide or enforce secure behaviors

Set safety standards early on in the process to ensure the right people have access to the right information



Secure by Design – Element #4

Remain committed to secure by design process

Implementing checkpoints to constantly reinforce design objectives

Simplify and automate security checkpoints as a standard practice throughout the development lifecycle

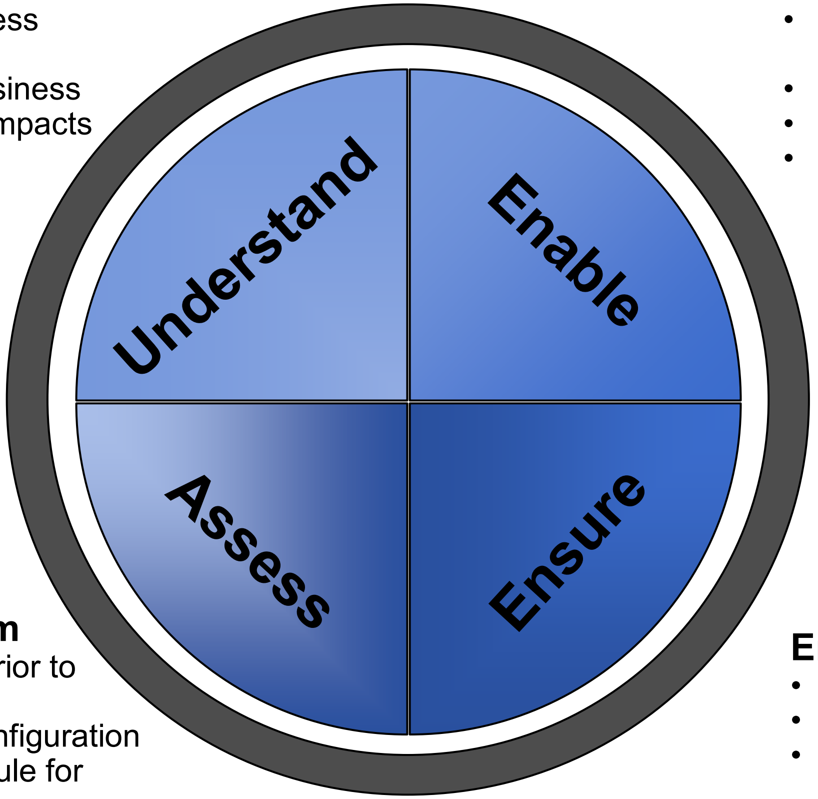
Components of Secure by Design for Development

Understand Security Drivers

- Recognize specific business opportunity and priority
- Assess system risk to business
- Model likely threats and impacts

Enable System Security

- Mandate appropriate security controls within applications
- Implement system monitoring/logging
- Specify secure platform & configuration
- Document update management plan



Assess Production System

- Test composed application prior to deployment
- Verify security of platform configuration
- Establish process and schedule for regular checking

Ensure secure development

- Protect development infrastructure
- Verify safety of third-party software
- Check system for security during coding/build/integration stages

Secure by Design Value

Secure by Design is a **cost-effective** approach to constructing *safe and reliable systems* by applying IBM's experience with security technologies and best practices in all phases of system creation, **from conception through system design, construction and deployment.**

Being **Secure by Design** reduces the **cost**, **risk**, and **unpredictability** of integrating new technologies.

Make Applications Secure, by Design

Cycle of secure application development

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

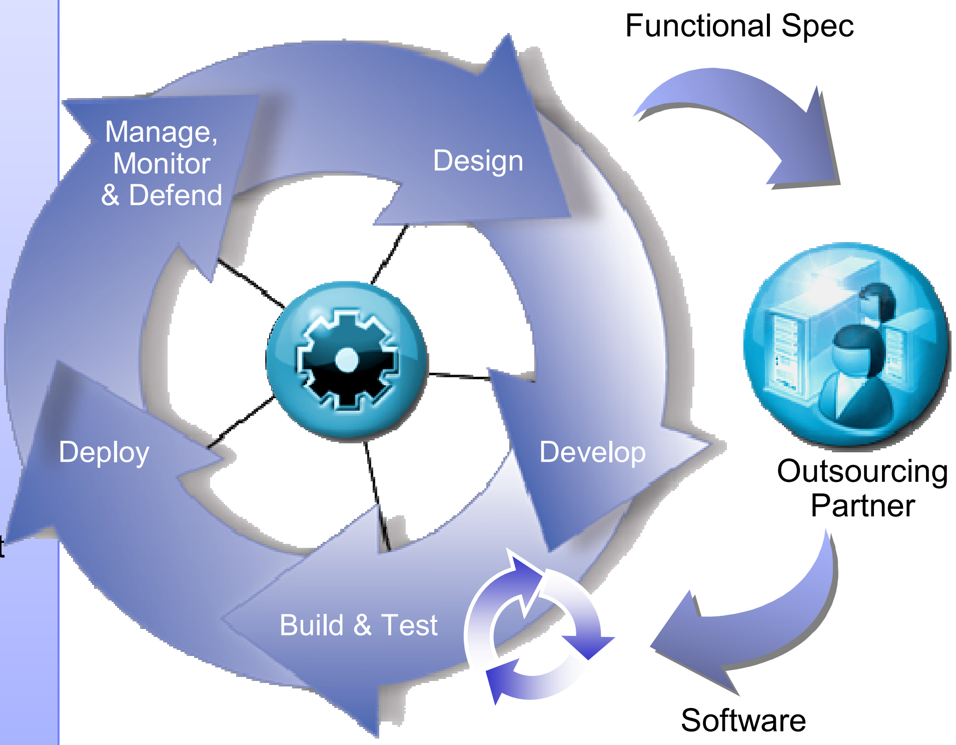
- Testing begins for errors and compliance with security requirements across the entire application
- Applications are also tested for exploitability in deployment scenario

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



Agenda

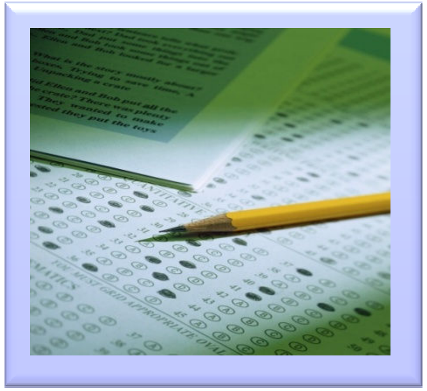
- IBM Security Framework
- Market Trends
- IBM Application Security
- IBM Secure by Design
- Rational Application Security (Appscan)

Cost is a Significant Driver

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

During the **coding** phase $80/defect

During the **build** phase $240/defect



During the **QA/Testing** phase $960/defect

Once **released** as a product $7,600/defect

+

Law suits, loss of customer trust, damage to brand

The increasing costs of fixing a defect….

*National Institute of Standards & Technology

Source: GBS Industry standard study

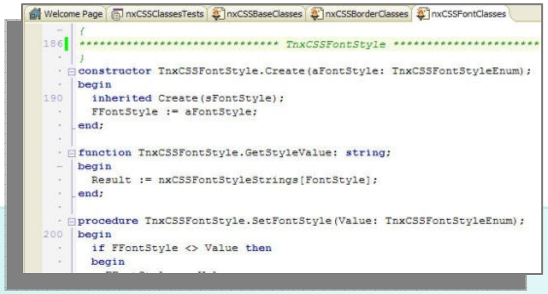
Defect cost derived in assuming it takes 8 hrs to find, fix and repair a defect when found in code and unit test.
Defect FFR cost for other phases calculated by using the multiplier on a blended rate of $80/hr.

Security Testing Technologies...

Combination Drives Greater Solution Accuracy

Static Code Analysis (Whitebox)

- Scanning source code for security issues



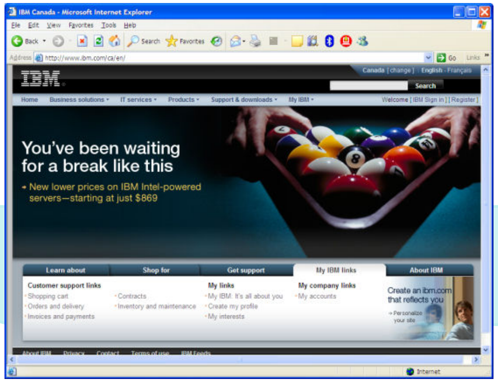
```
{
****************************** TnxCSSFontStyle **********************
}
constructor TnxCSSFontStyle.Create(aFontStyle: TnxCSSFontStyleEnum);
begin
  inherited Create(sFontStyle);
  FFontStyle := aFontStyle;
end;

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



You've been waiting for a break like this

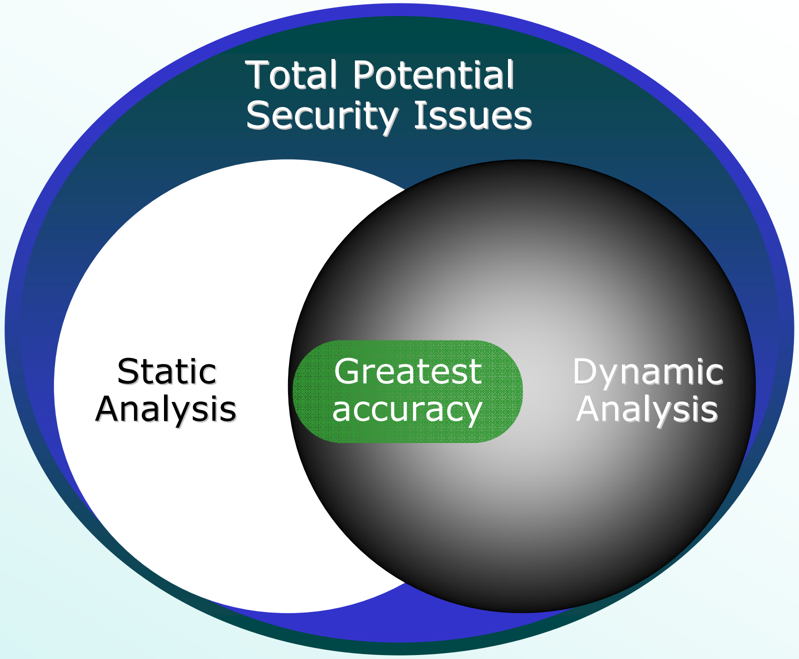
→ New lower prices on IBM Intel-powered servers—starting at just $869

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

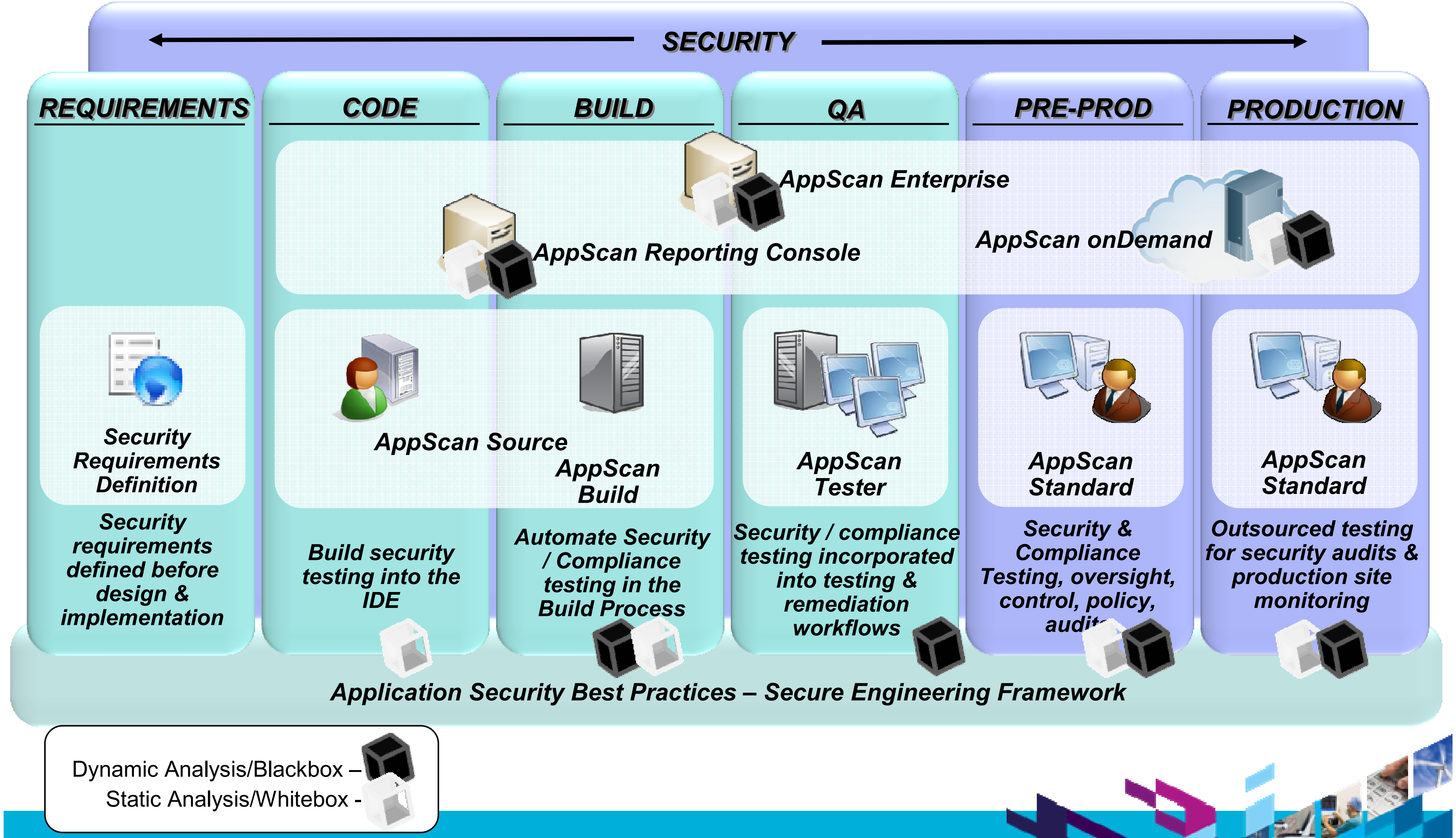
My links
- My IBM: It's all about you
- Create my profile
- My interests

My company links
- My accounts

Create an ibm.com that reflects you
→ Personalize your site



IBM Rational AppScan Suite –
Comprehensive Application Vulnerability Management



SECURITY

REQUIREMENTS

CODE

BUILD

QA

PRE-PROD

PRODUCTION

AppScan Enterprise

AppScan Reporting Console

AppScan onDemand

Security Requirements Definition

AppScan Source

AppScan Build

AppScan Tester

AppScan Standard

AppScan Standard

Security requirements defined before design & implementation

Build security testing into the IDE

Automate Security / Compliance testing in the Build Process

Security / compliance testing incorporated into testing & remediation workflows

Security & Compliance Testing, oversight, control, policy, audit

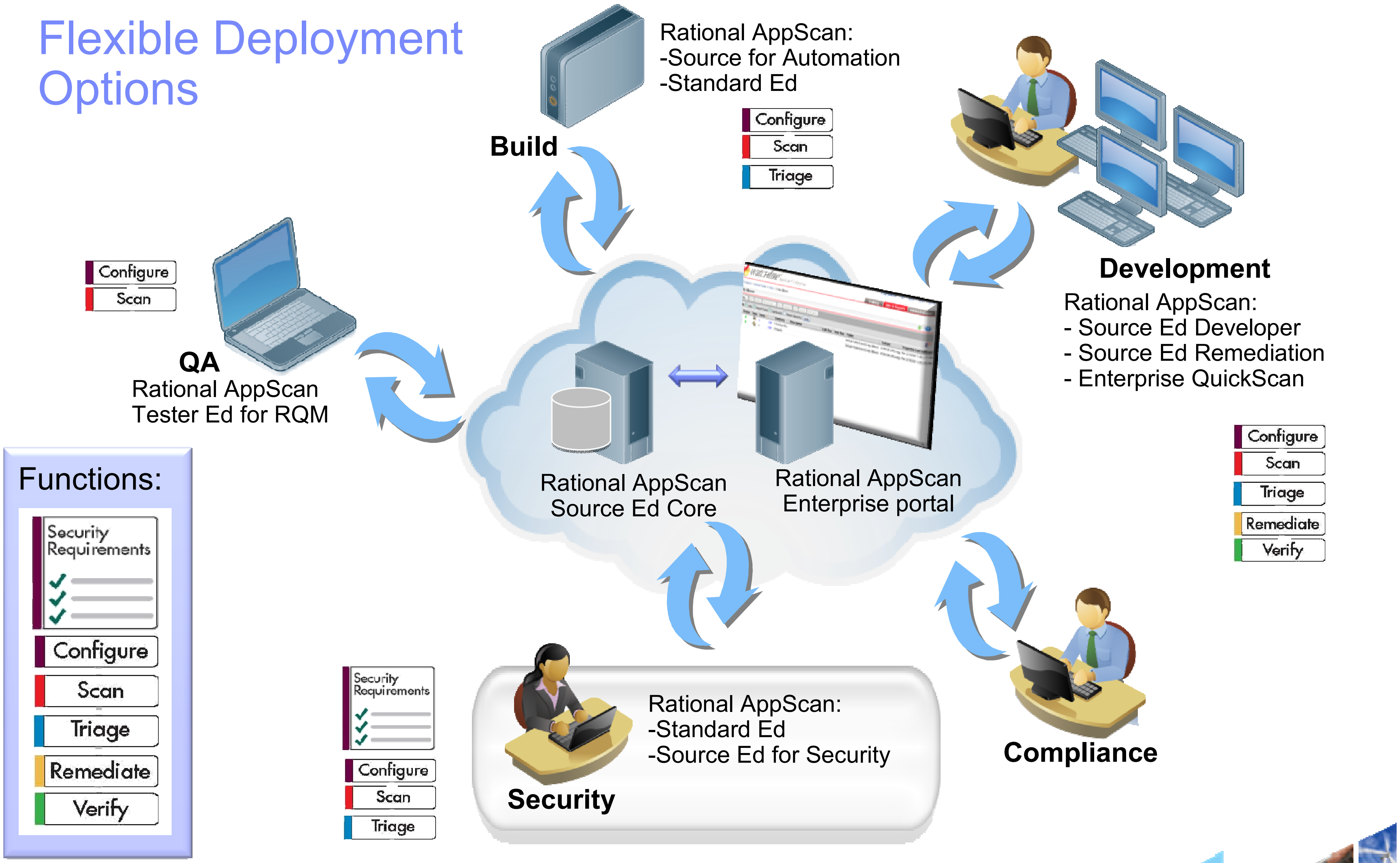
Outsourced testing for security audits & production site monitoring

Application Security Best Practices – Secure Engineering Framework

Dynamic Analysis/Blackbox –

Static Analysis/Whitebox -

Flexible Deployment Options



Build

Rational AppScan:
-Source for Automation
-Standard Ed

Development

Rational AppScan:
- Source Ed Developer
- Source Ed Remediation
- Enterprise QuickScan

QA

Rational AppScan
Tester Ed for RQM

Rational AppScan
Source Ed Core

Rational AppScan
Enterprise portal

Security

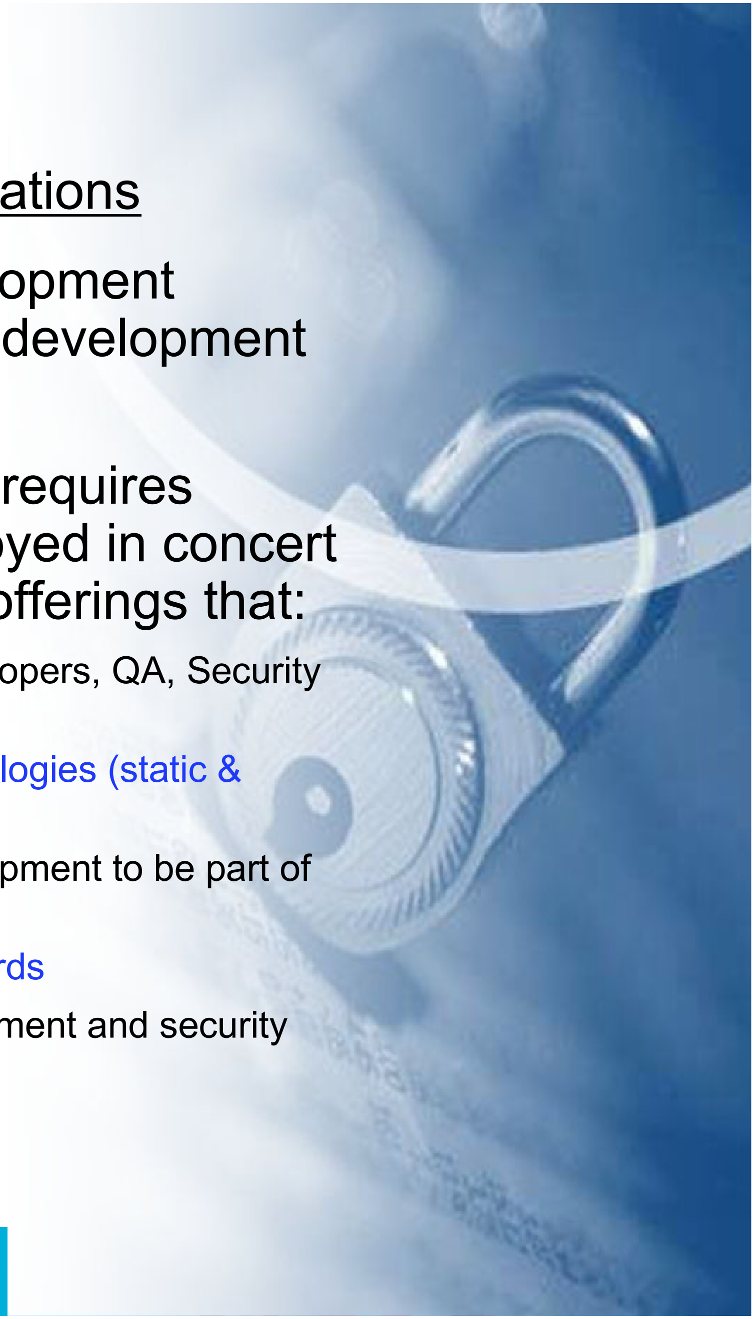
Rational AppScan:
-Standard Ed
-Source Ed for Security

Compliance

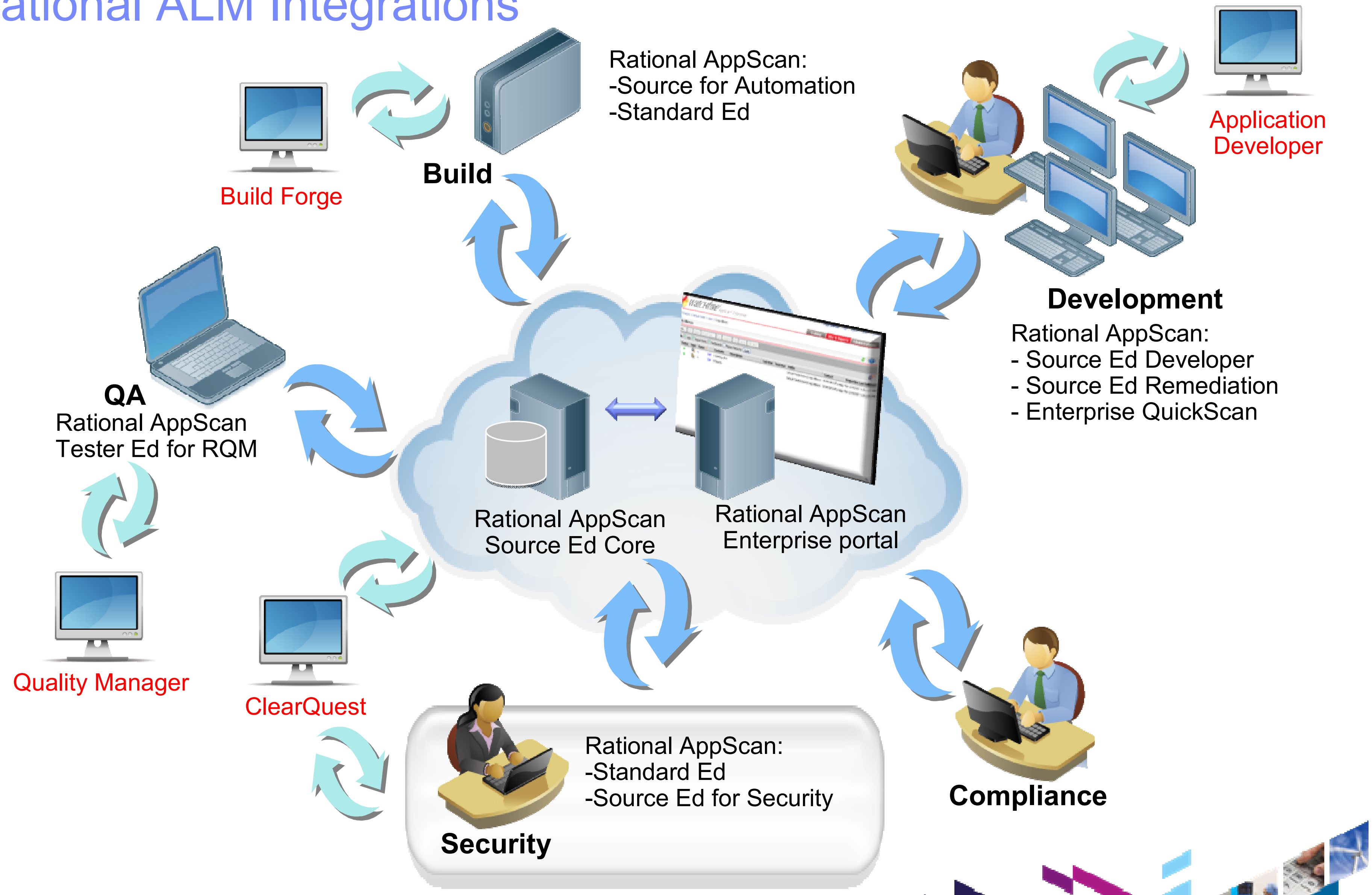
Functions:

Security for Smarter Products

- Smarter Products require <u>secure applications</u>
- Security needs to be built into the development process and addressed throughout the development lifecycle
- Providing security for smarter products requires comprehensive security solutions deployed in concert with application lifecycle management offerings that:
  - Provide integrated testing solutions for developers, QA, Security and Compliance stakeholders
  - Leverage multiple appropriate testing technologies (static & dynamic analysis)
  - Provide effortless security that allows development to be part of the solution
  - Support governance, reporting and dashboards
  - Can facilitate collaboration between development and security teams



Rational ALM Integrations



Rational AppScan:
-Source for Automation
-Standard Ed

Build

Build Forge

Application Developer

Development

Rational AppScan:
- Source Ed Developer
- Source Ed Remediation
- Enterprise QuickScan

QA

Rational AppScan
Tester Ed for RQM

Quality Manager

ClearQuest

Rational AppScan
Source Ed Core

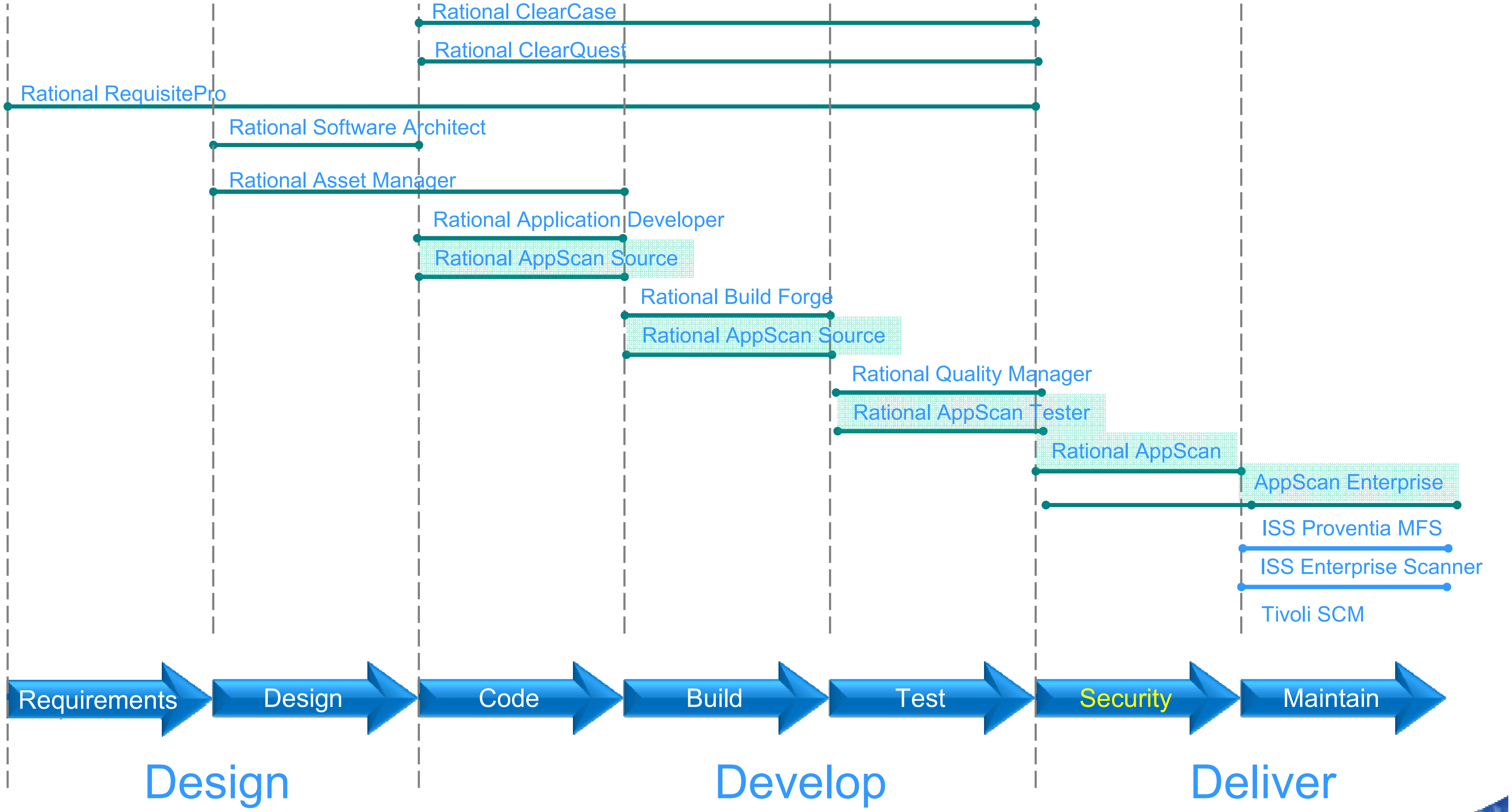
Rational AppScan
Enterprise portal

Rational AppScan:
-Standard Ed
-Source Ed for Security

Security

Compliance

Required Technologies by Lifecycle Phase



Rational ClearCase

Rational ClearQuest

Rational RequisitePro

Rational Software Architect

Rational Asset Manager

Rational Application Developer

Rational AppScan Source

Rational Build Forge

Rational AppScan Source

Rational Quality Manager

Rational AppScan Tester

Rational AppScan

AppScan Enterprise

ISS Proventia MFS

ISS Enterprise Scanner

Tivoli SCM

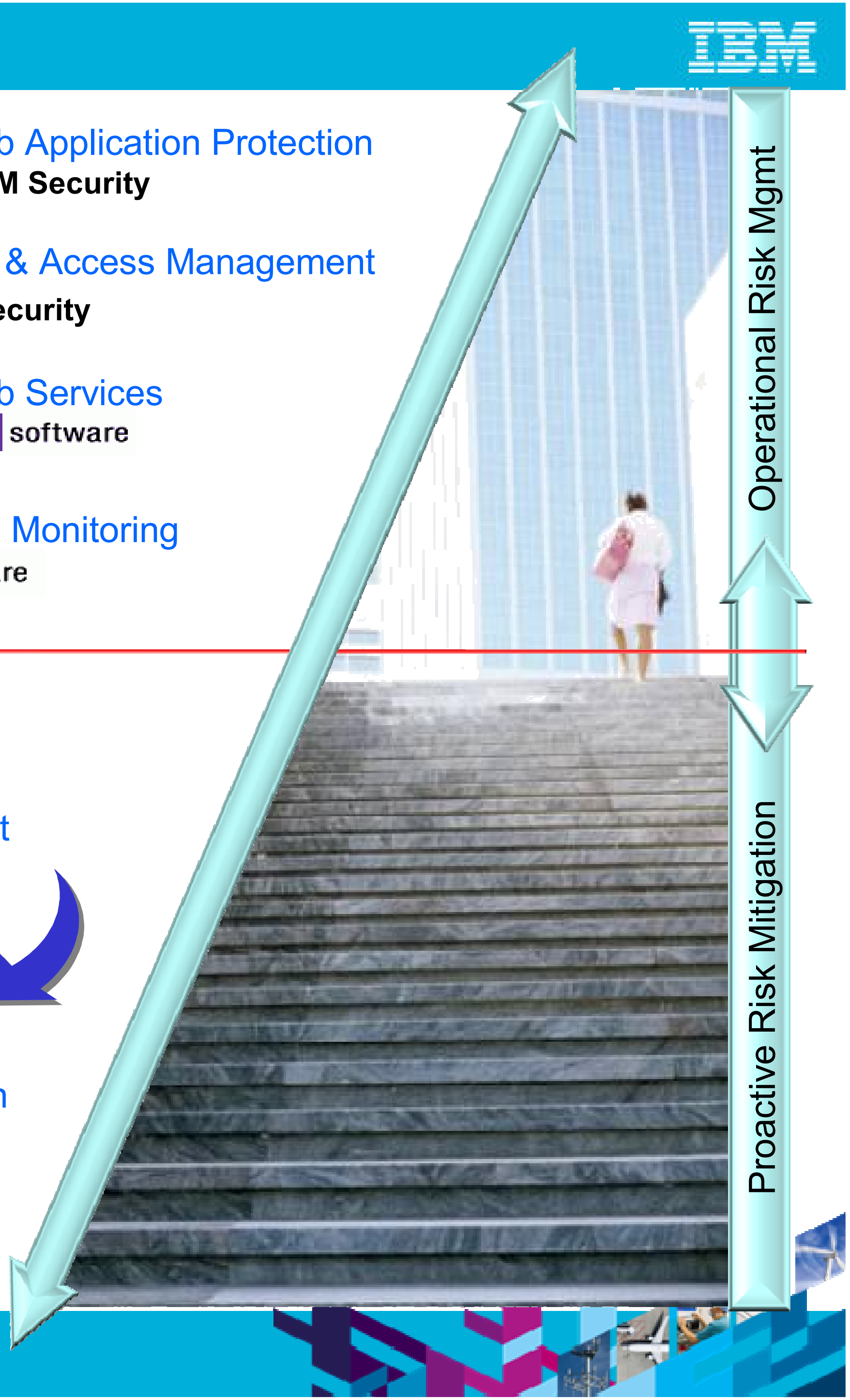
Requirements → Design → Code → Build → Test → Security → Maintain

Design

Develop

Deliver

A Path to Secure Applications



Application & resource protection in operation

Web Application Protection
IBM Security

Identity & Access Management
IBM Security

Secure Web Services
WebSphere. software

Production-Site Monitoring
Rational. software

Deploy Application

Secure application development across design, code, build, test phases

Final Security Audit
Rational. software

Vulnerability Assessment Functioning Application
Rational. software

Vulnerability Assessment of Source Code
Rational. software

Policy & Requirements Definition
Rational. software
IBM Security Services

Risk Assessment
IBM Security Services

Thank You