Rational Appscan
– Web Application Security QA
- Your Last Line of Defense

Rational software

Martin Borrett

Lead Security Architect

Technical Staff Member

NE Europe

IBM SWG

Go to **IBM**

Why application security, compliance and policies are high priority

- **Web applications are the #1 focus of hackers:**
  - ▸ 75% of attacks at Application layer (Gartner)
  - ▸ XSS and SQL Injection are #1 and #2 reported vulnerabilities (Mitre)

- **Most sites are vulnerable:**
  - ▸ 90% of sites are vulnerable to application attacks (Watchfire)
  - ▸ 78% percent of easily exploitable vulnerabilities affected Web applications (Symantec)
  - ▸ 80% of organizations will experience an application security incident by 2010 (Gartner)

- **Web applications are high value targets for hackers:**
  - ▸ Customer data, credit cards, ID theft, fraud, site defacement, etc

- **Compliance requirements and standards provide overall assurance of quality and business governance:**
  - ▸ Payment Card Industry (PCI) Standards, GLBA, HIPPA, FISMA,
  - ▸ Internal regulatory policies

The Alarming Truth

"**Approximately 100 million Americans have been informed that they have suffered a security breach so this problem has reached epidemic proportions.**"

Jon Oltsik – Enterprise Strategy Group

"**Up to 21,000 loan clients may have had data exposed**"

Marcella Bombardieri, Globe Staff/August 24, 2006

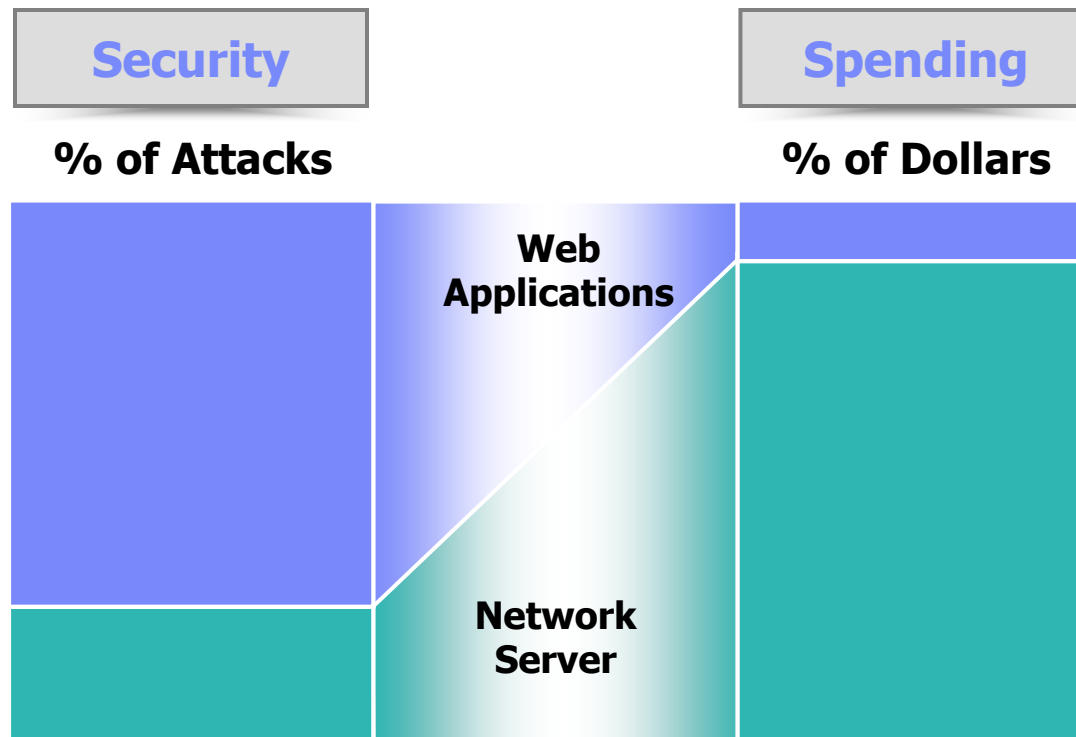"**Personal information stolen from 2.2 million active-duty members of the military, the government said…**"

New York Times/June 7, 2006

"**Hacker may have stolen personal identifiable information for 26,000 employees..**"

ComputerWorld, June 22, 2006

The Reality: security and spending are unbalanced

Security	Spending

% of Attacks   **% of Dollars**

Web
Applications

Network
Server

75% of all attacks on Information Security
are directed to the Web Application Layer

2/3 of all Web Applications are vulnerable

Gartner

Why Application Security Problems Exist

- **Developers have usually little training or experience in writing or testing for secure code**
  - **More likely don't care**
- **IT security professionals are mostly from network and infrastructure side**
  - Have little experience in application development
- **Firewalls, IPS and other network security solutions don't block application attacks.**
  - **Port 80, 8080, 443**
- **Network scanners won't find application vulnerabilities.**
  - Nessus, ISS, Qualys, Nmap, etc.
- **Network security (firewall, IDS, etc) do nothing once an organization web enables an application.**
- **Attempts to protect application traffic makes transaction experience cumbersome and inefficient**

How Watchfire's technology works
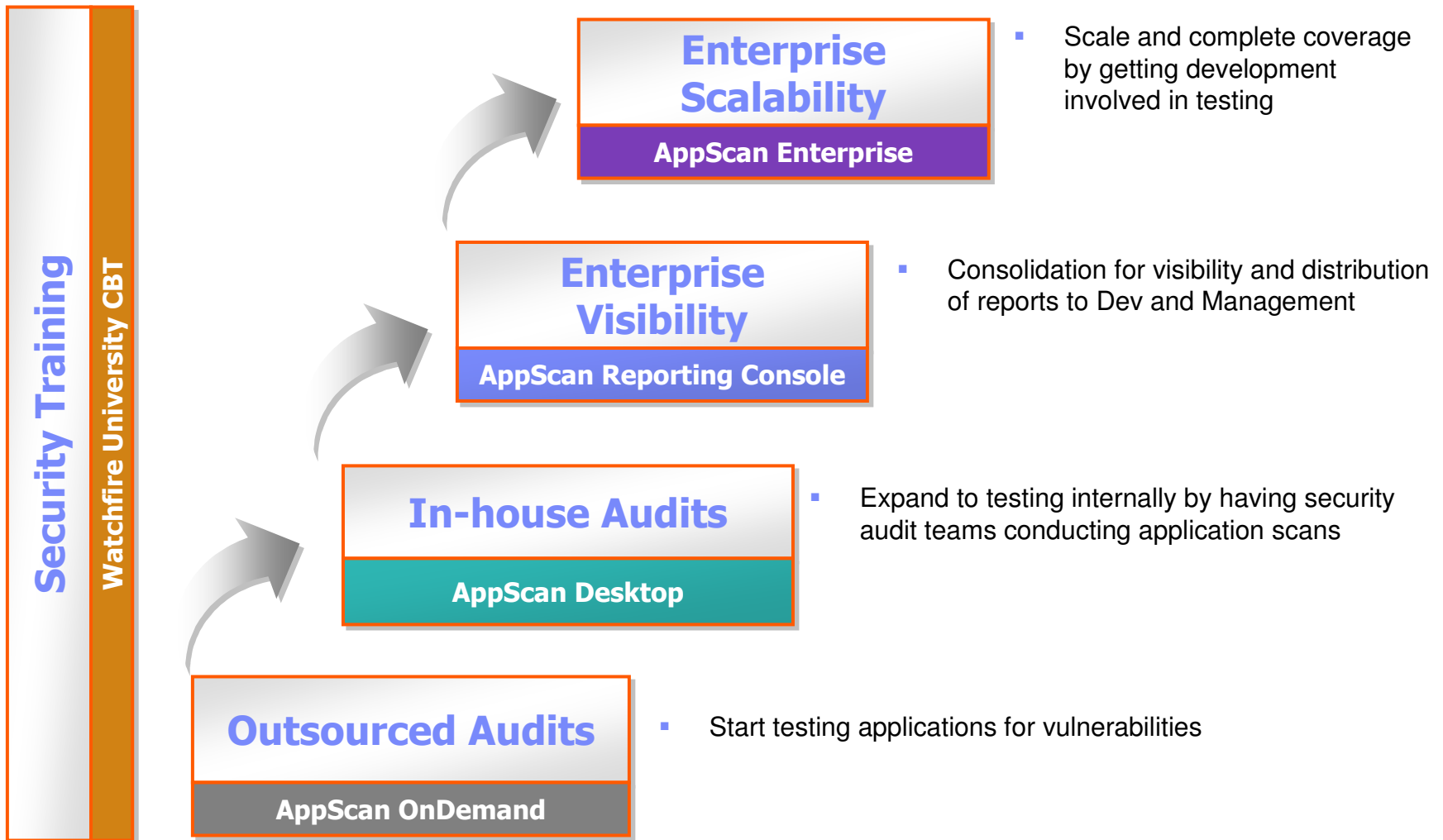

Security **Privacy** **Quality**
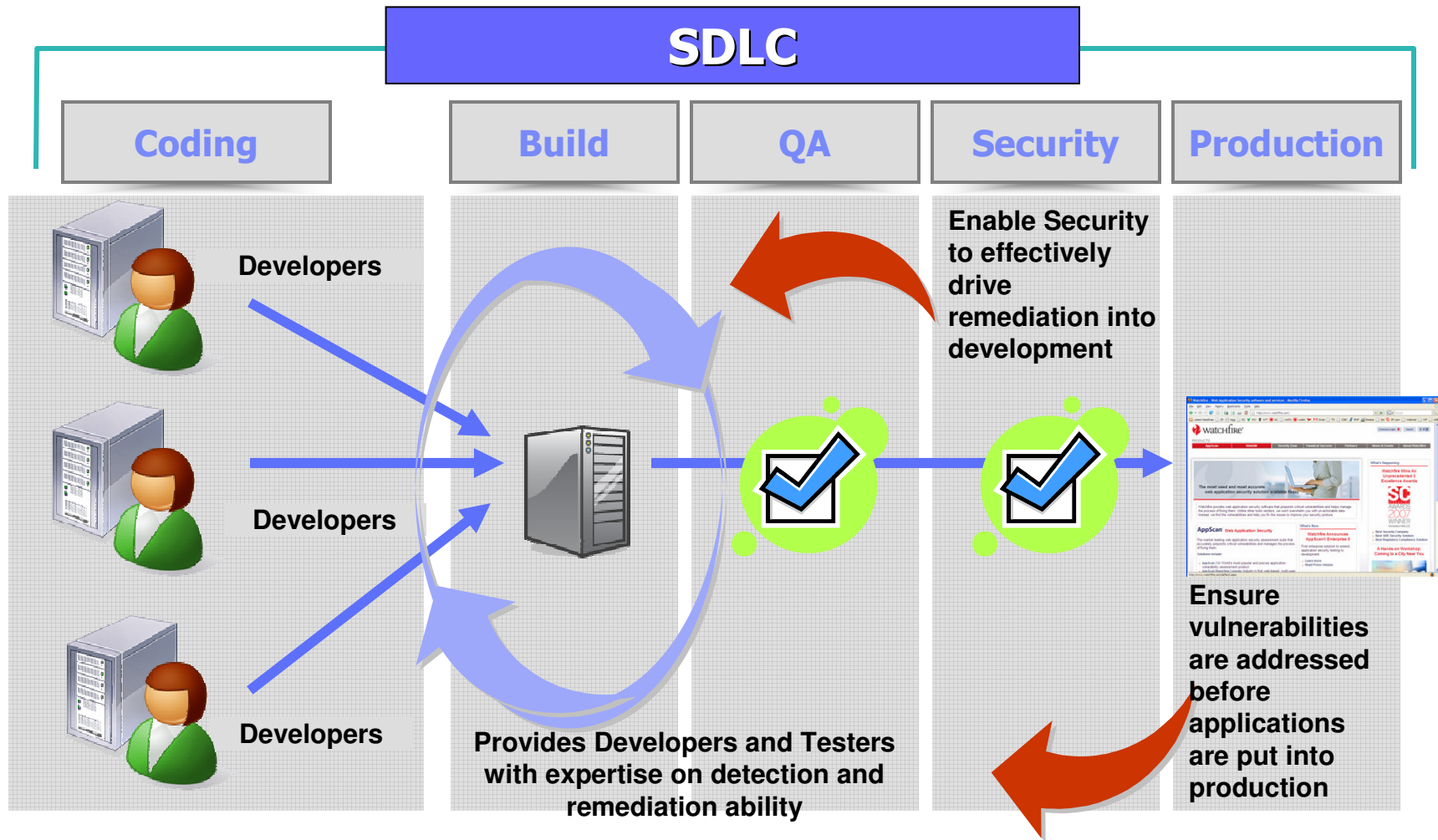
Standards **Compliance**

| ① **Scan** | → | ② **Analyze** | → | ③ **Report** Detailed, Actionable Information |

Web application testing maturity model

Security Training

Watchfire University CBT

Enterprise Scalability

AppScan Enterprise

- Scale and complete coverage by getting development involved in testing

Enterprise Visibility

AppScan Reporting Console

- Consolidation for visibility and distribution of reports to Dev and Management

In-house Audits

AppScan Desktop

- Expand to testing internally by having security audit teams conducting application scans

Outsourced Audits

AppScan OnDemand

- Start testing applications for vulnerabilities

Building security & compliance into the SDLC

SDLC

Coding	Build	QA	Security	Production

Developers

Developers

Developers

Enable Security to effectively drive remediation into development

Provides Developers and Testers with expertise on detection and remediation ability

Ensure vulnerabilities are addressed before applications are put into production

8

Web-based User Interface

Scalable Enterprise Architecture

Clients	AppScan Enterprise	Target Sites

Pen Tester

Developer

Compliance Officer

QA Specialist

ASE Control Center Server

ASE Database Server

ASE Agent Servers

Web Servers
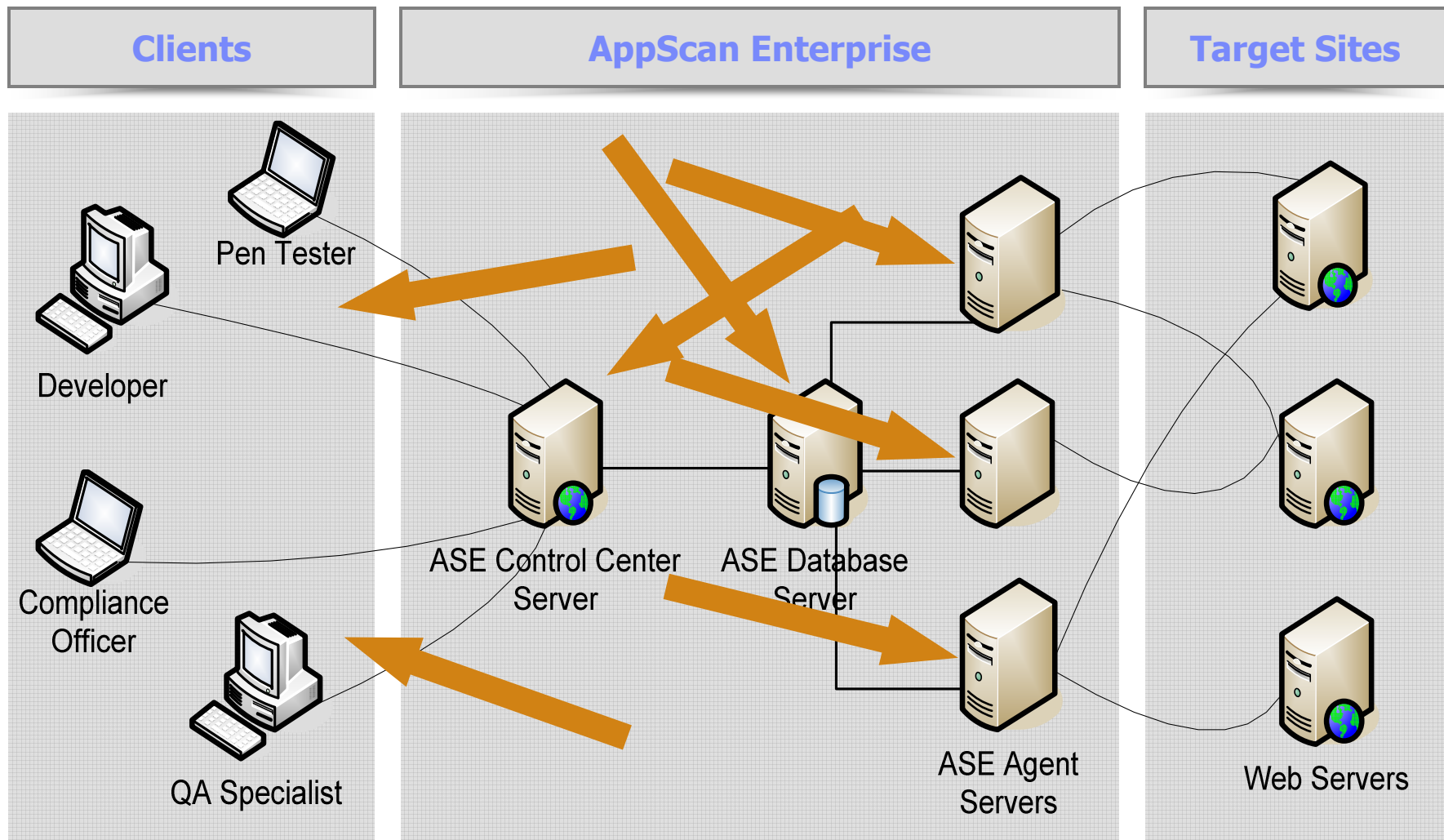
Multi-Level Reporting

- Dashboard Summaries & Trending

- Compliance Reports

- Detailed Vulnerability Reports

- Advisories

- Fix Recommendations
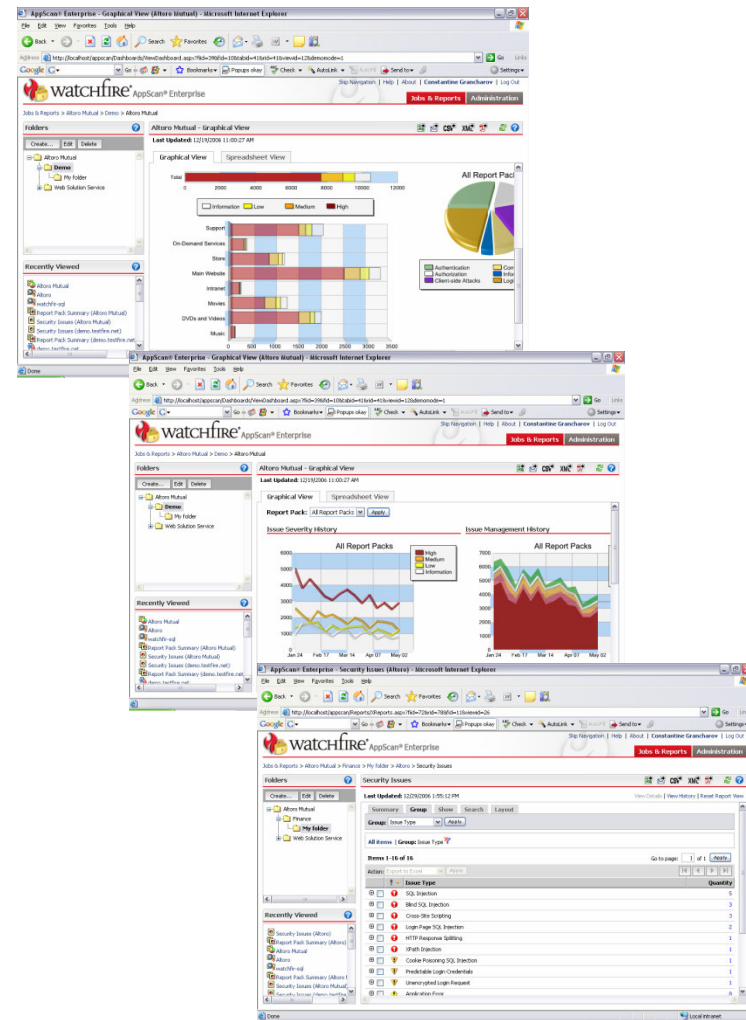
Rational Software Quality Solutions

BUSINESS

SOFTWARE QUALITY SOLUTIONS

Test and Change Management

Requirements	**Test**	**Change**	**Defects**
Rational RequisitePro	**Rational ClearQuest**	**Rational ClearQuest**	**Rational ClearQuest**

Test Automation

Developer Test

Rational PurifyPlus

Rational Test RealTime

Functional Test

Rational Functional Tester Plus

Automated	**Manual**
Rational Functional Tester	Rational Manual Tester

Rational Robot

Security and Compliance Test

AppScan

WebXM

Performance Test

Rational Performance Tester

Quality Metrics

Project Dashboards   **Detailed Test Results**   **Quality Reports**

DEVELOPMENT

OPERATOINS