watchfire
an IBM company

IBM

IBM Software Group

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

Rational. software

Go to IBM

Martin Borrett
Lead Security Architect
Technical Staff Member
NE Europe
IBM SWG

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

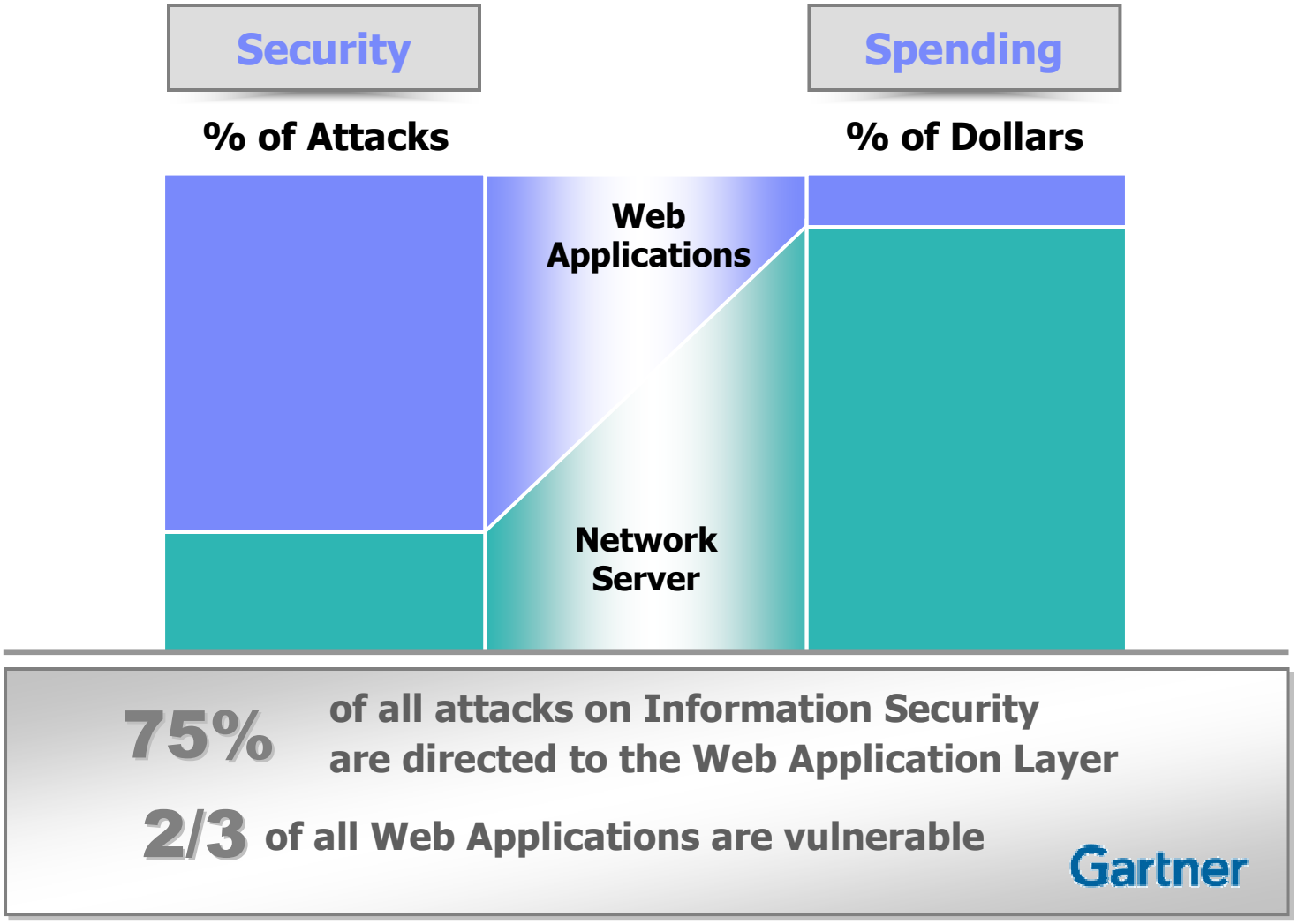
"Personal information stolen from 2.2 million active-duty members of the military, the government said…"

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

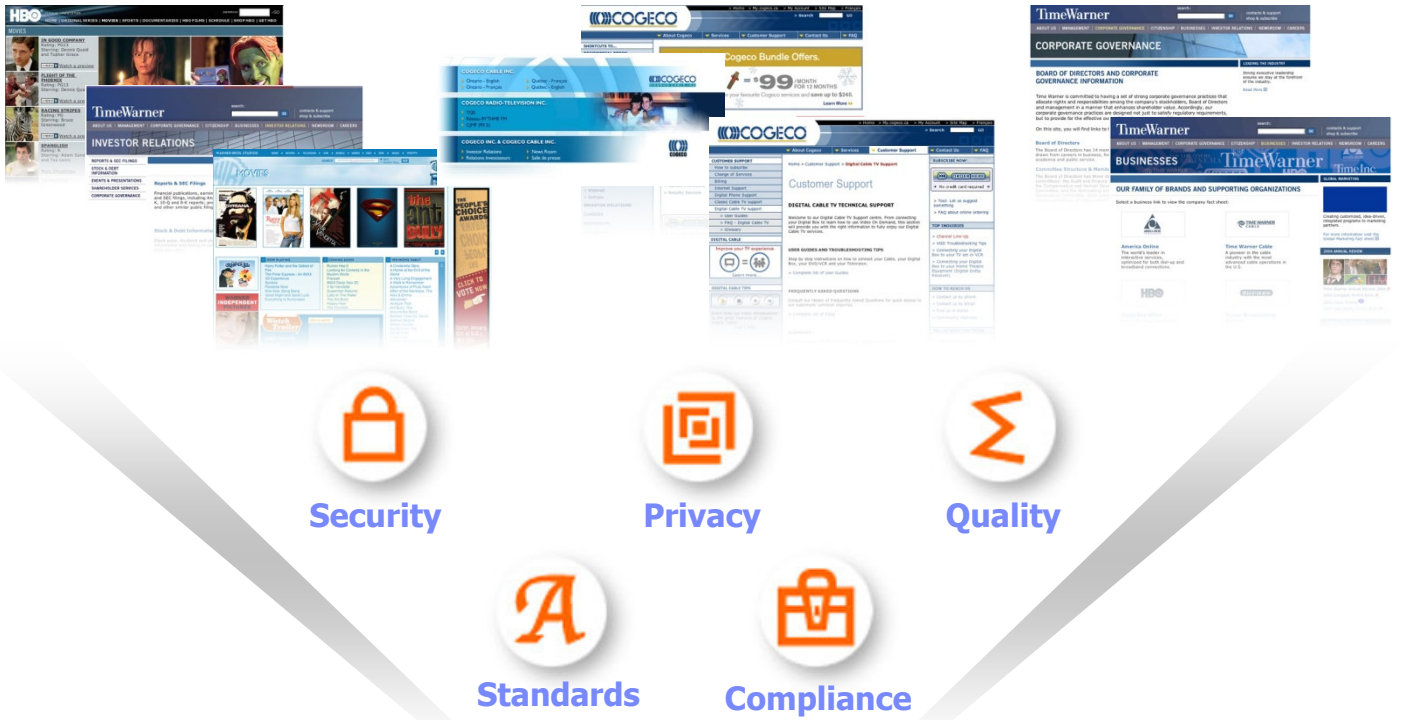


Sources: Gartner, Watchfire

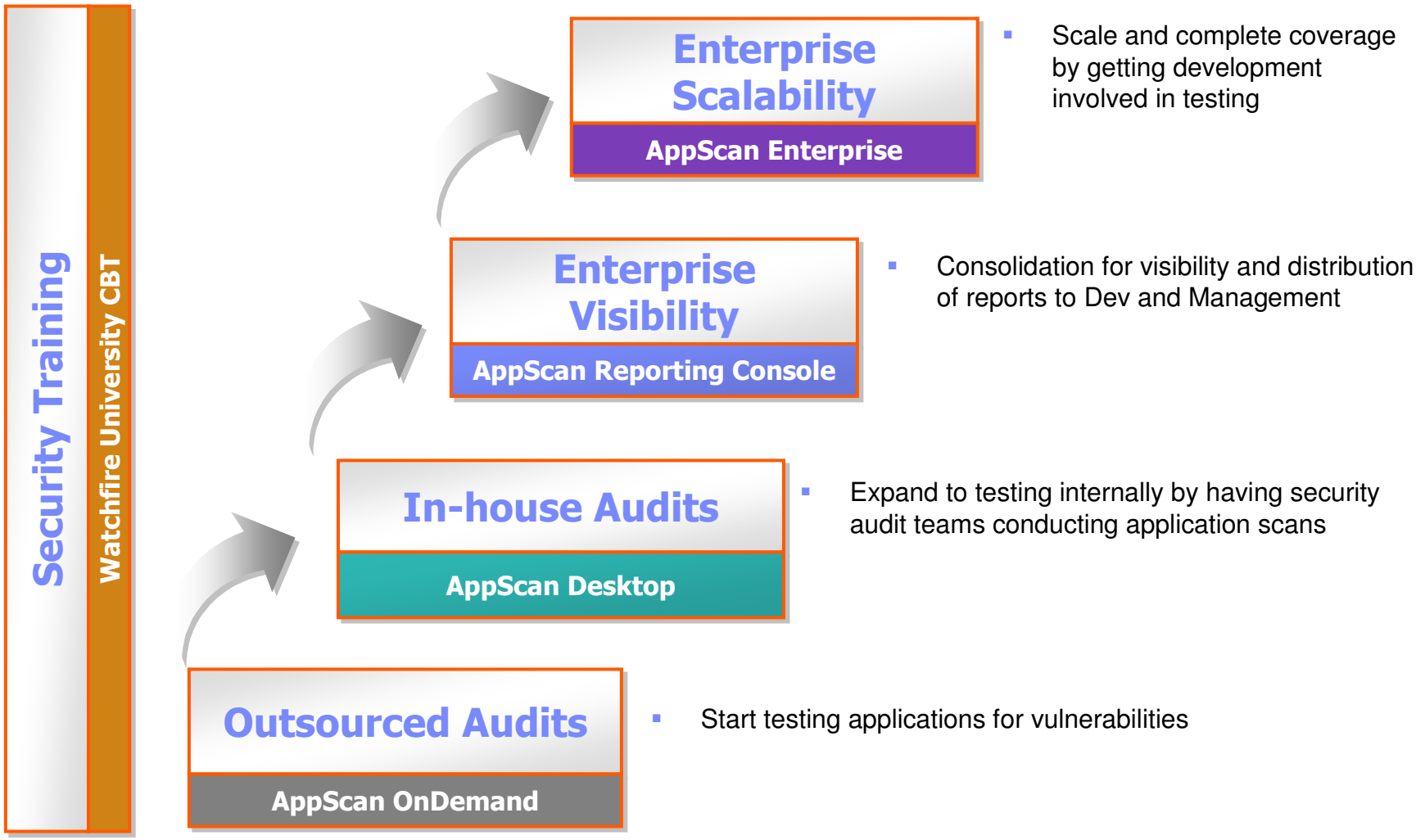
Why Application Security Problems Exist

- **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**

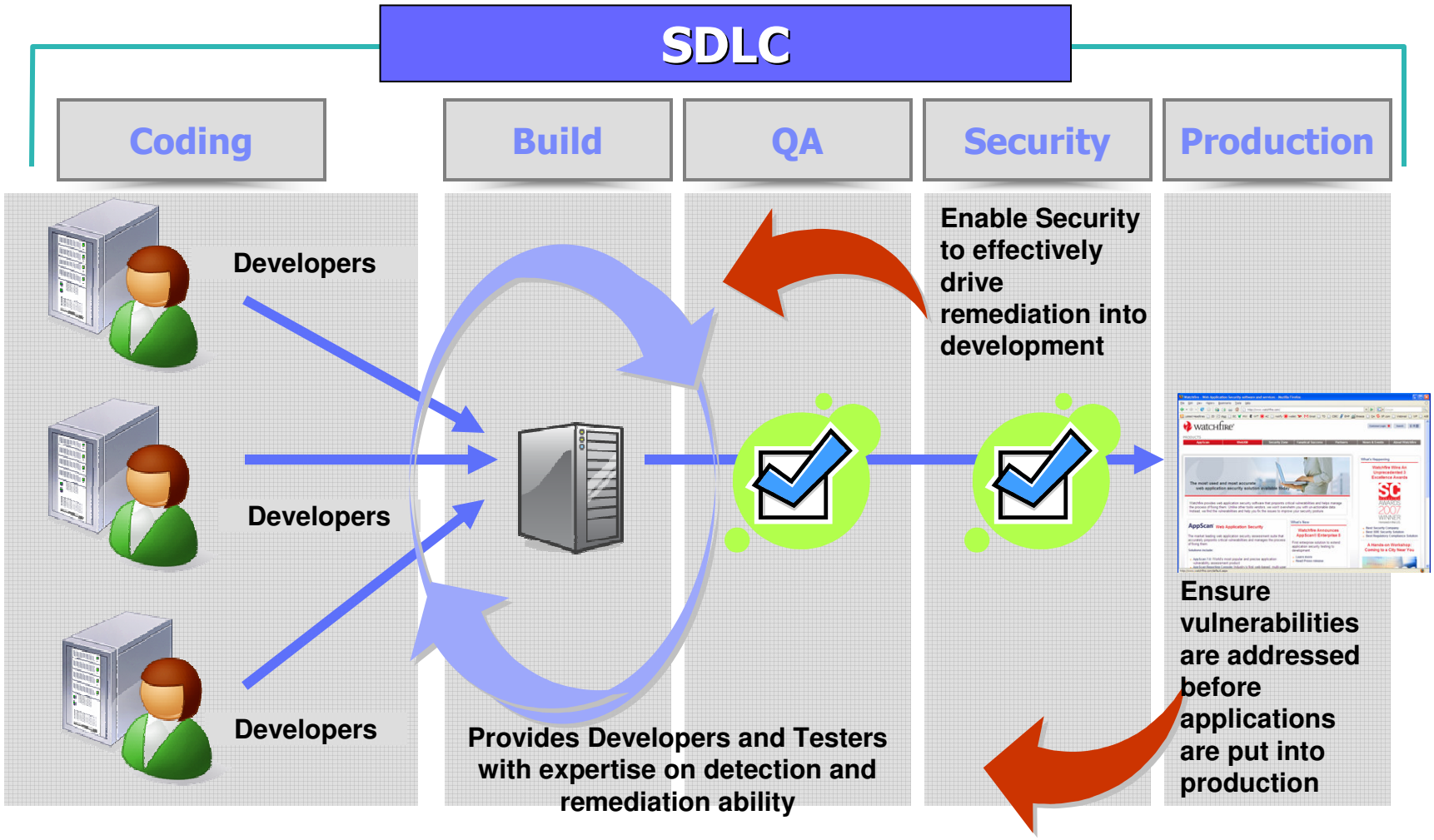
How Watchfire's technology works



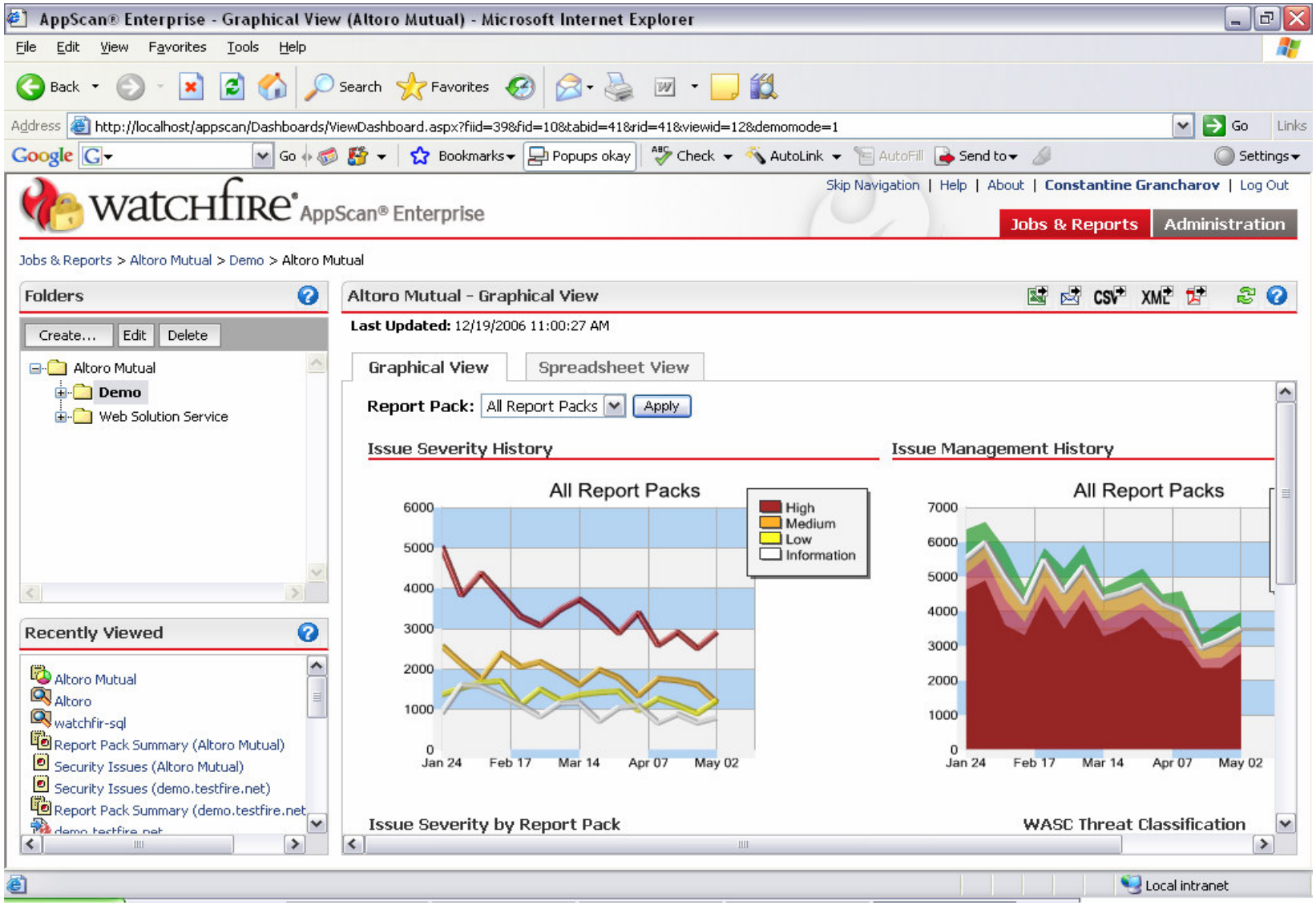
Web application testing maturity model



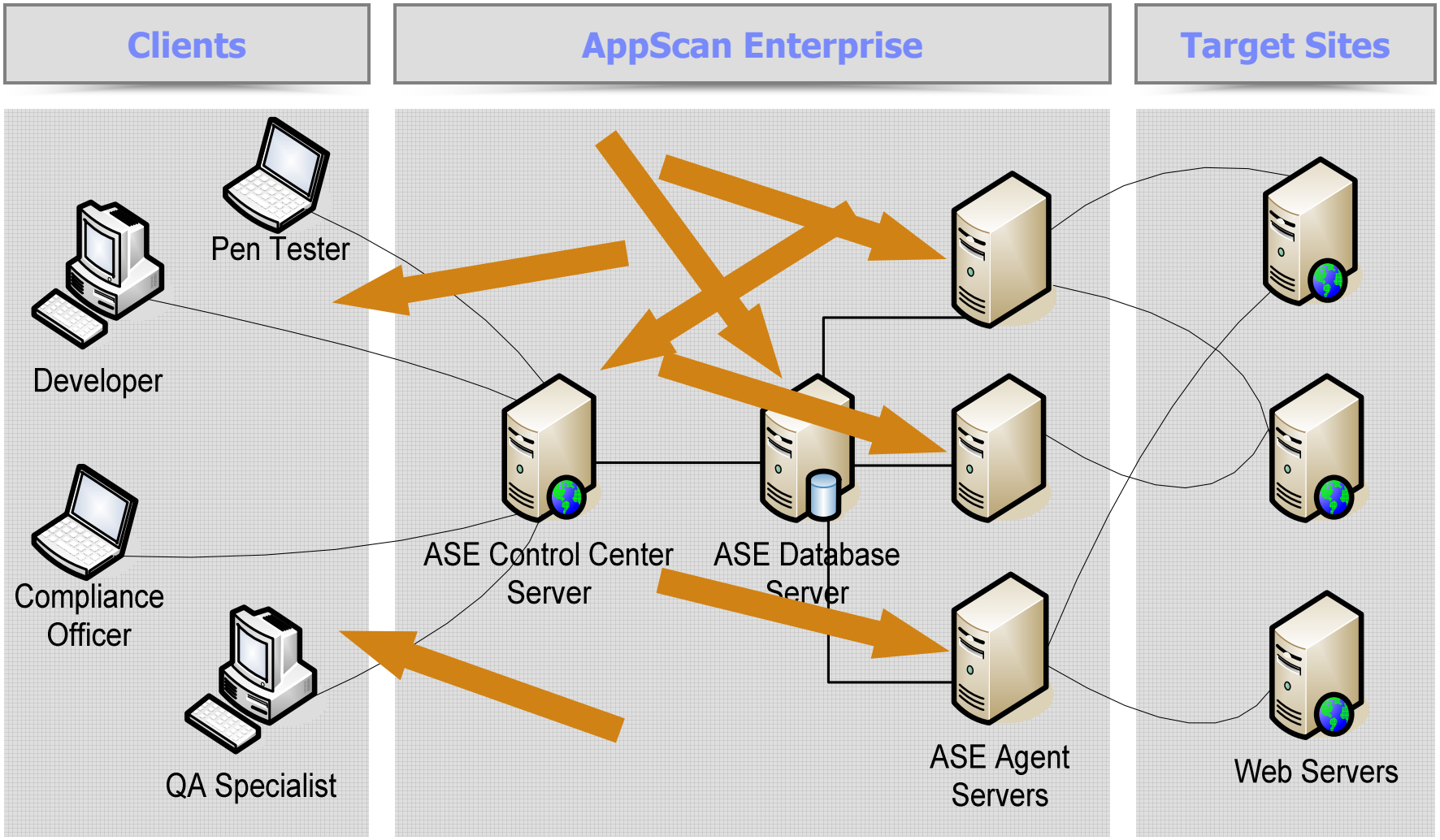
Building security & compliance into the SDLC



Web-based User Interface

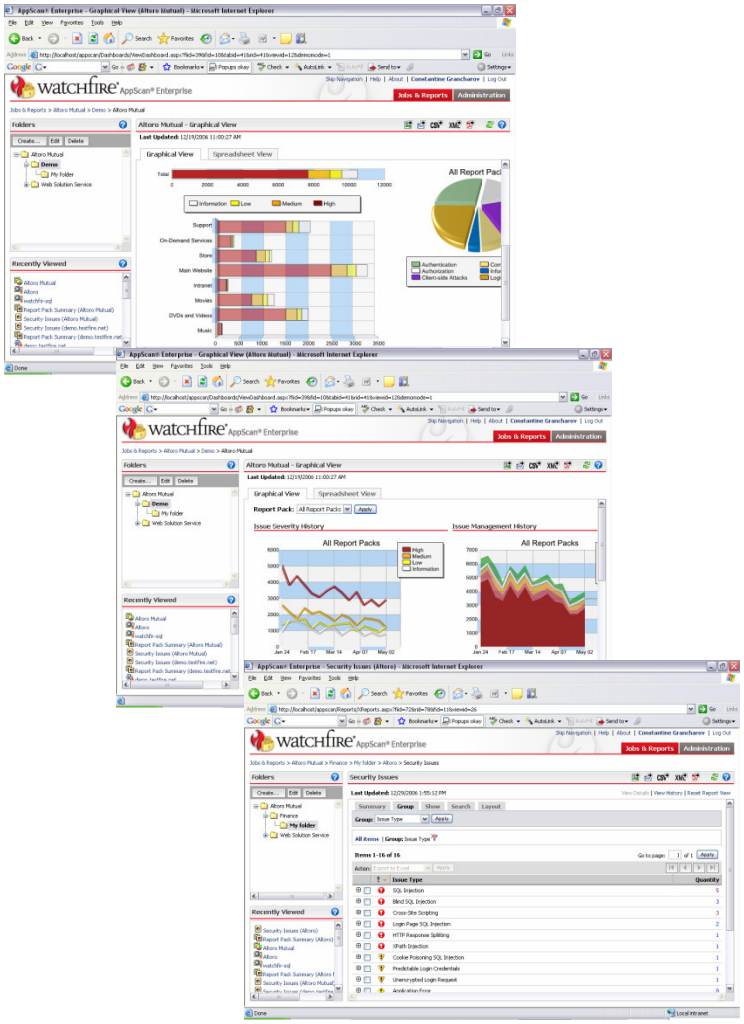


Scalable Enterprise Architecture



Multi-Level Reporting

- Dashboard Summaries & Trending
- Compliance Reports
- Detailed Vulnerability Reports
- Advisories
- Fix Recommendations



Rational Software Quality Solutions