IBM Rational Vision and Roadmap for Application Security

John Burroughs, CISSP
IBM Product Manager
Web Application Security and Compliance

Rational. software

ASC01

Go to IBM

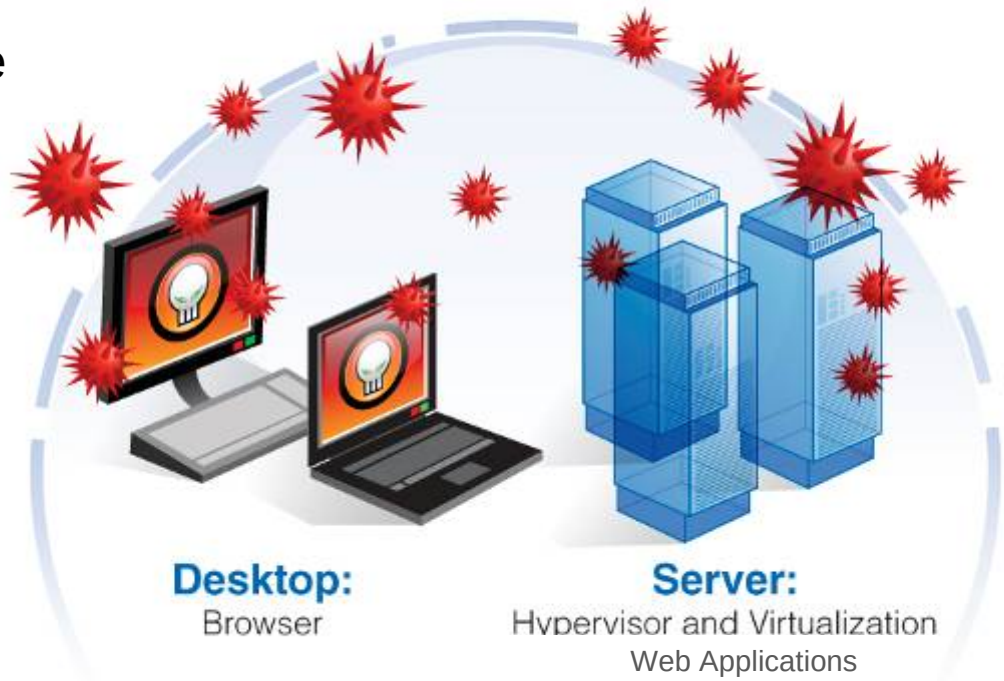
Today's Agenda

- Strategic Trends in Application Security
- Best Practices and Strategies
- Vision and Roadmap for 2009 and Beyond

Changing security landscape creates complex threats

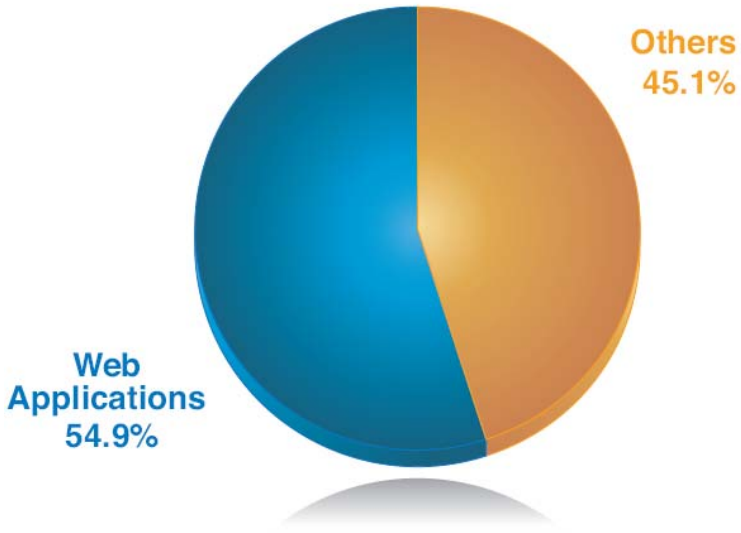
Web-enabled Applications Drive the Need for Security

- 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)



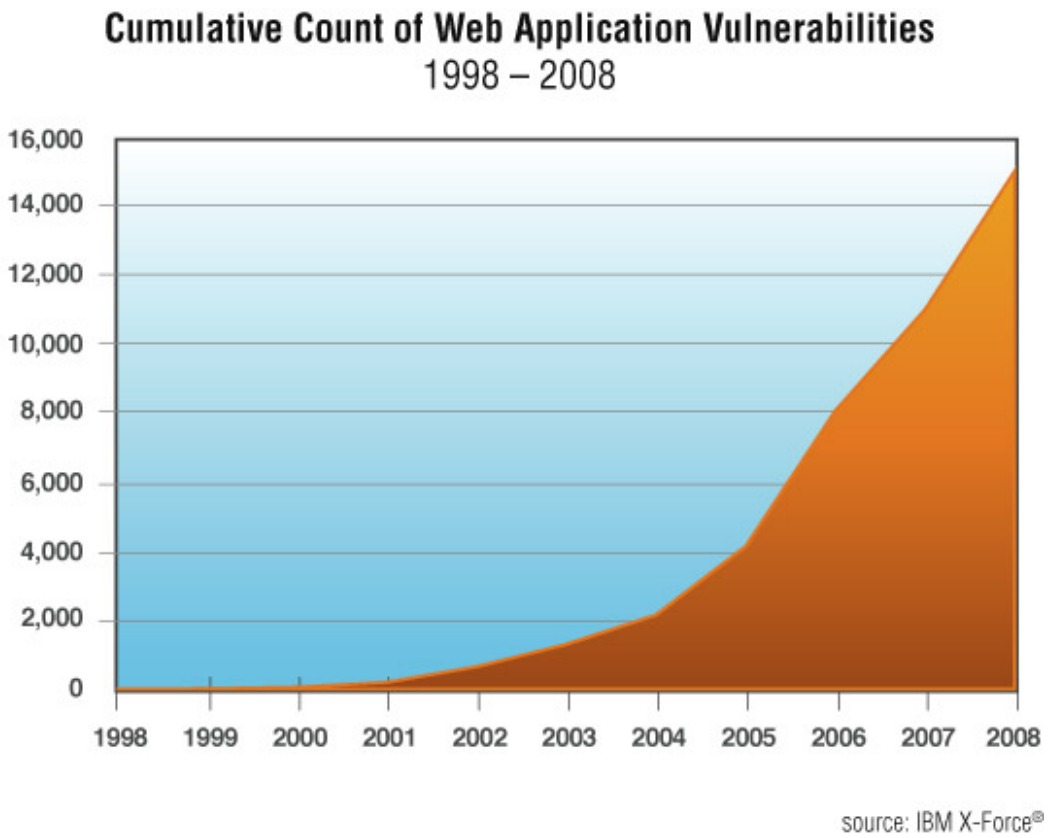
2009 Web Threats Take Center Stage

- Web application vulnerabilities
  - ***Web applications have become the Achilles heel of Corporate IT Security***
  - Represent largest category in vuln disclosures (55% in 2008)
  - *This number does not include custom-developed Web applications!*



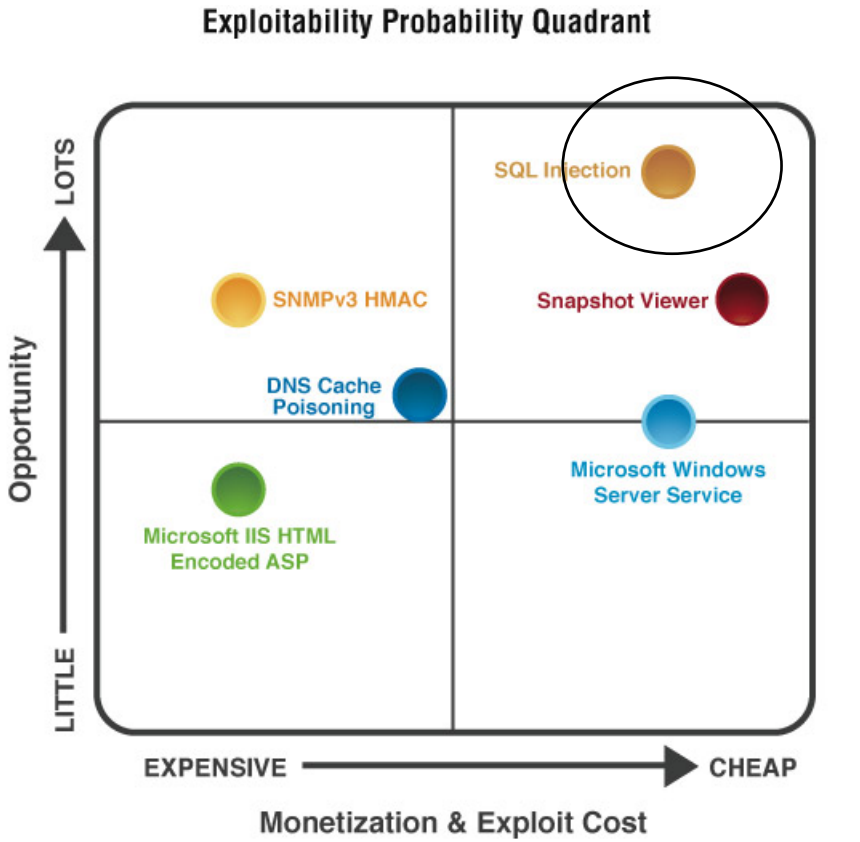
Growth of Web Application Vulnerabilities

- SQL injection vulnerability disclosures more than doubled in comparison to 2007



- The number of active, automated attacks on web servers was unprecedented

Webapp Exploitation is Cheaper and Easier than Alternatives



source: IBM X-Force®

Exploitation of SQL injection skyrocketed in 2008

- Increased by 30x from the midyear to the end of 2008

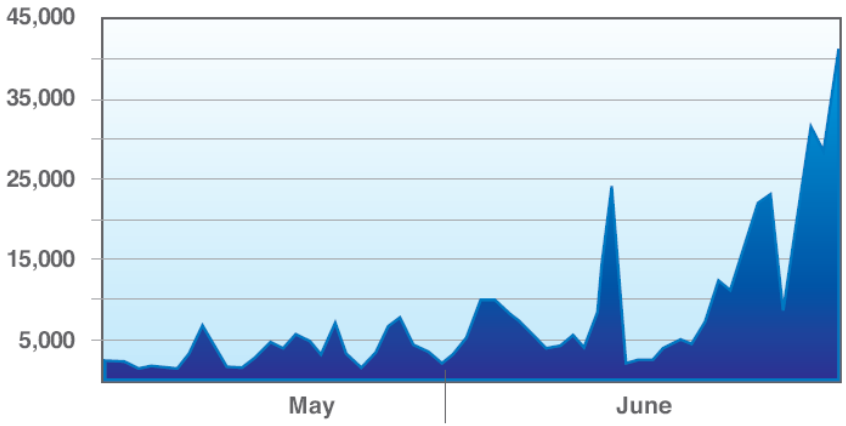


Figure 20: Initial SQL Injection Attacks Monitored by IBM ISS Managed Security Services, May – June 2008

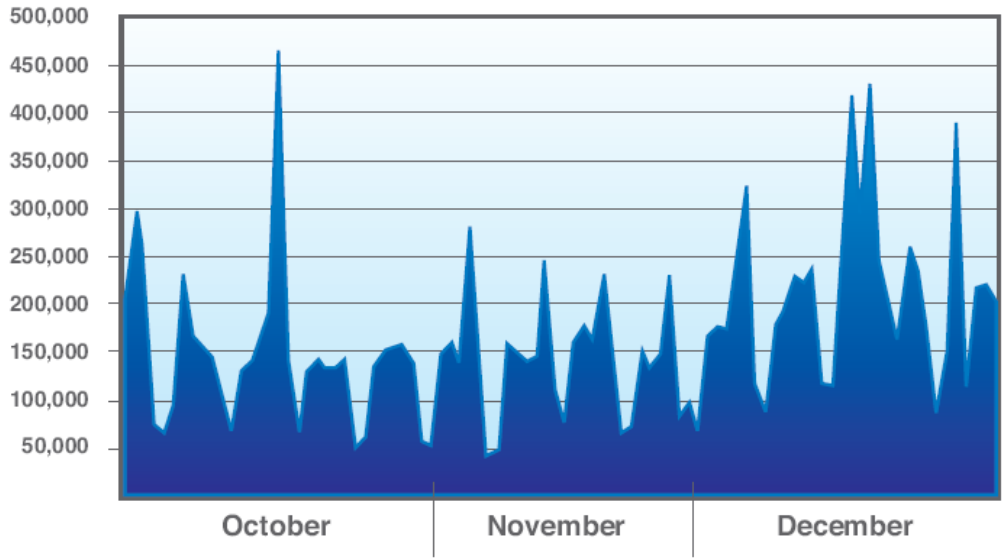


Figure 21: SQL Injection Attacks Monitored by IBM ISS Managed Security Services, Q4 2008

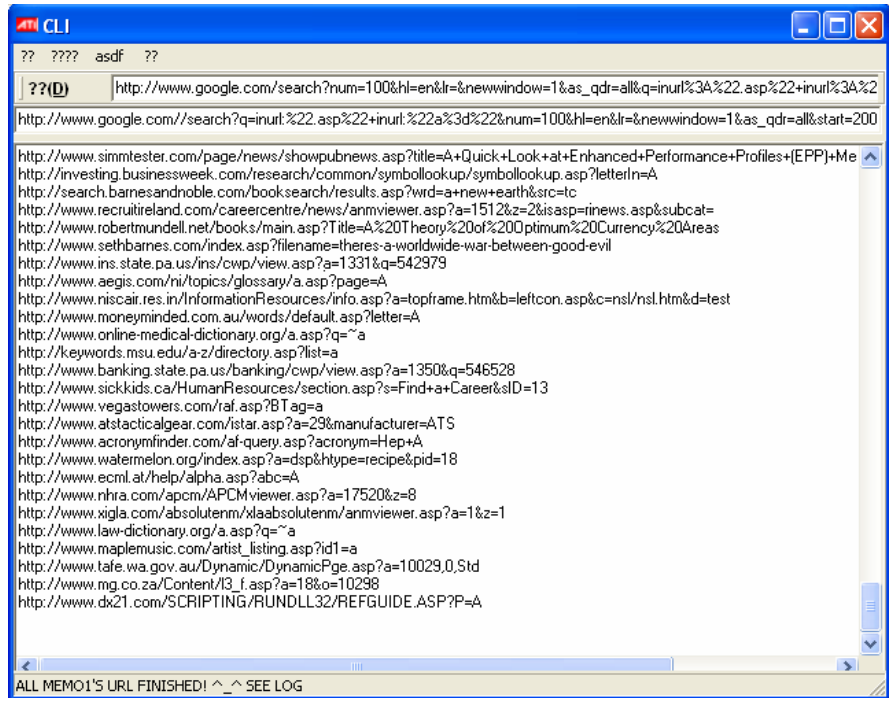
SQL injection used to plant Malware

- SQL injection has been used to extract information from databases
- Now SQL Injection is used to add info to databases
  - Database is being updated with malicious script
  - Users who browse the web application are being infected by script which takes advantage of browser/plug flows to install malware from malicious sites

Web Application hacks have replaced email as the number 1 delivery mechanism for malware

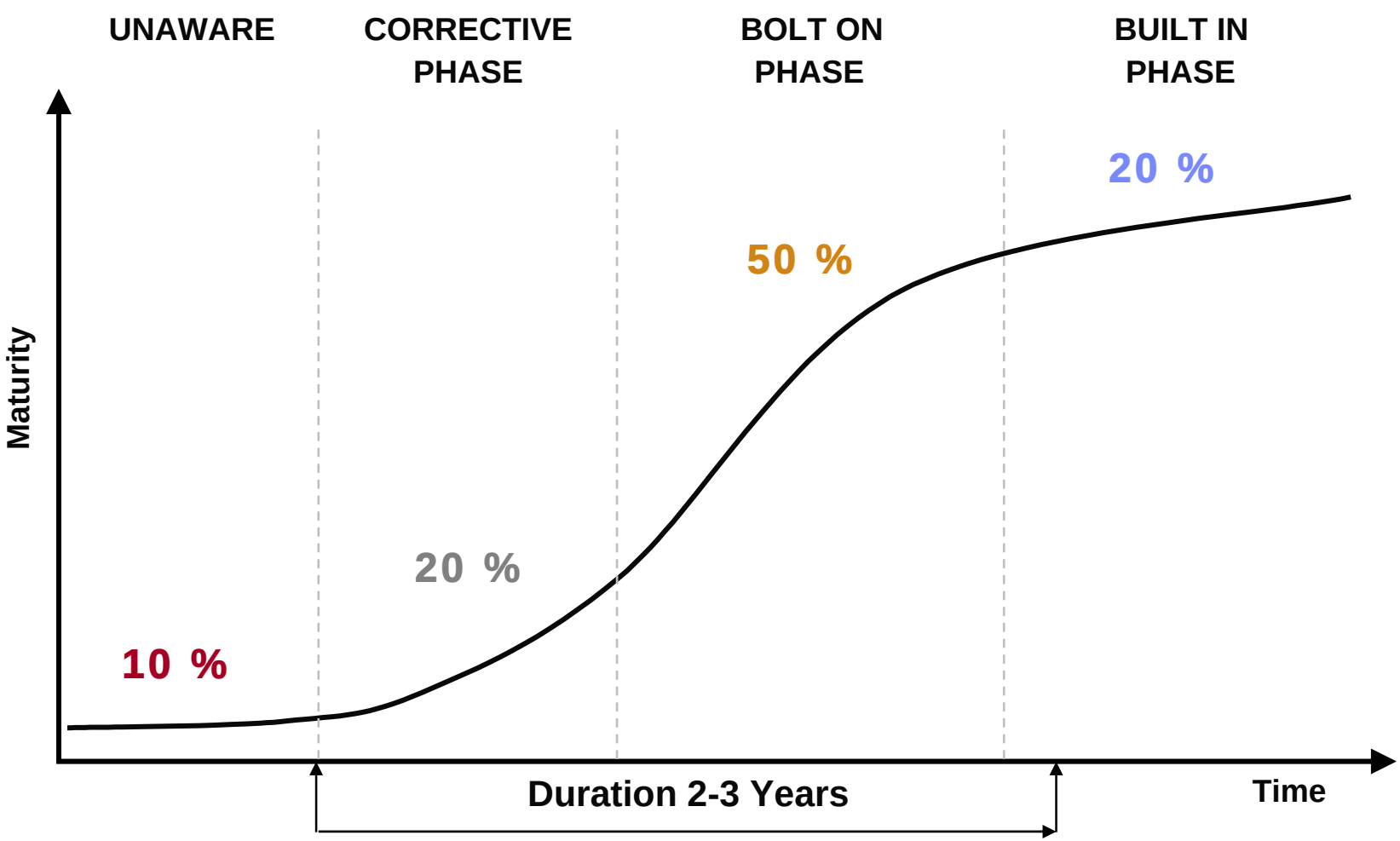
Subscription Based SQL Injection Tools

- Automating the SQL Injection attacks
  - User specifies the custom payload to inject
  - Tool checks a site in China to verify subscription fees
  - Connects to Google to search for vulnerable sites ***inurl:".asp" inurl:"a="***
    - *Site regularly updated with new SQL Injection vulnerabilities*
  - Starts SQL injection
    - *Uses vulnerability-specific payloads to inject required commands*
  - Botnets used to deliver attack

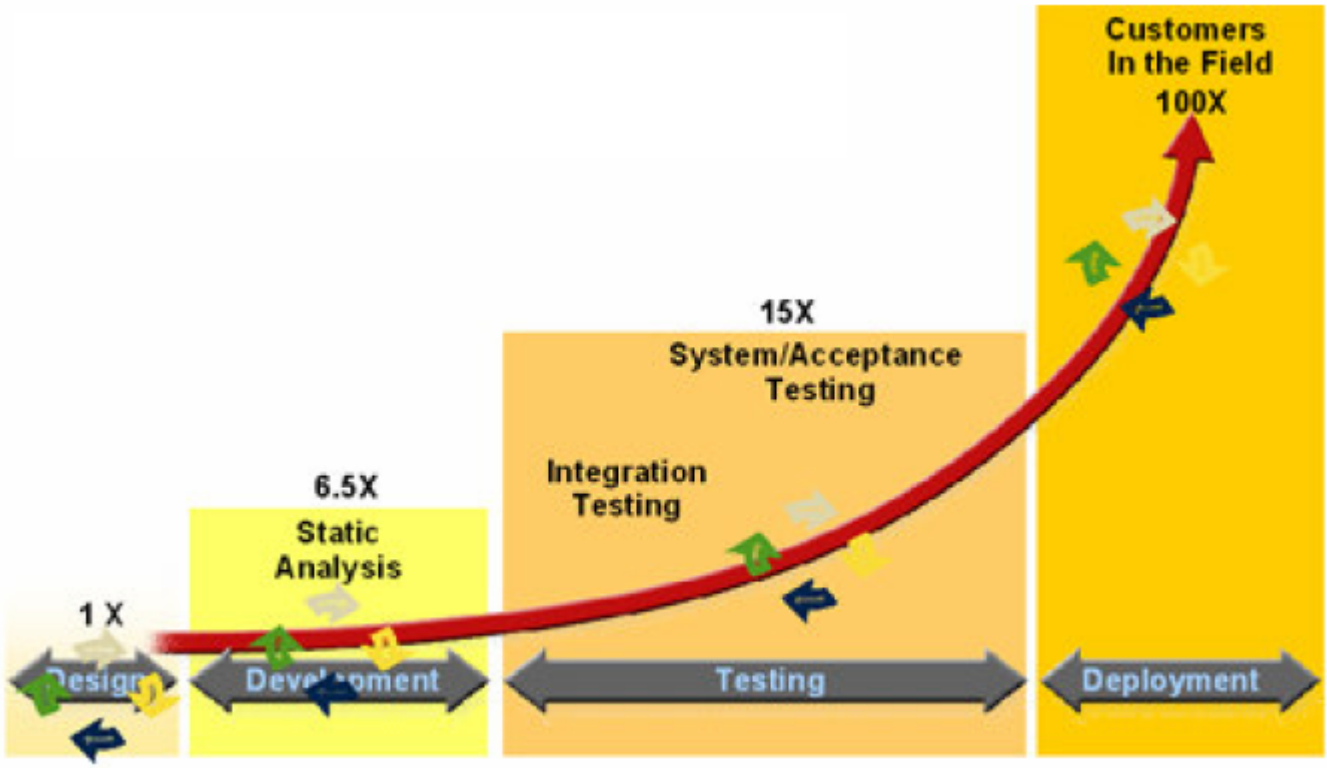


- Opportunistic attack: Sites not specifically targeted

Application Security Maturity Model

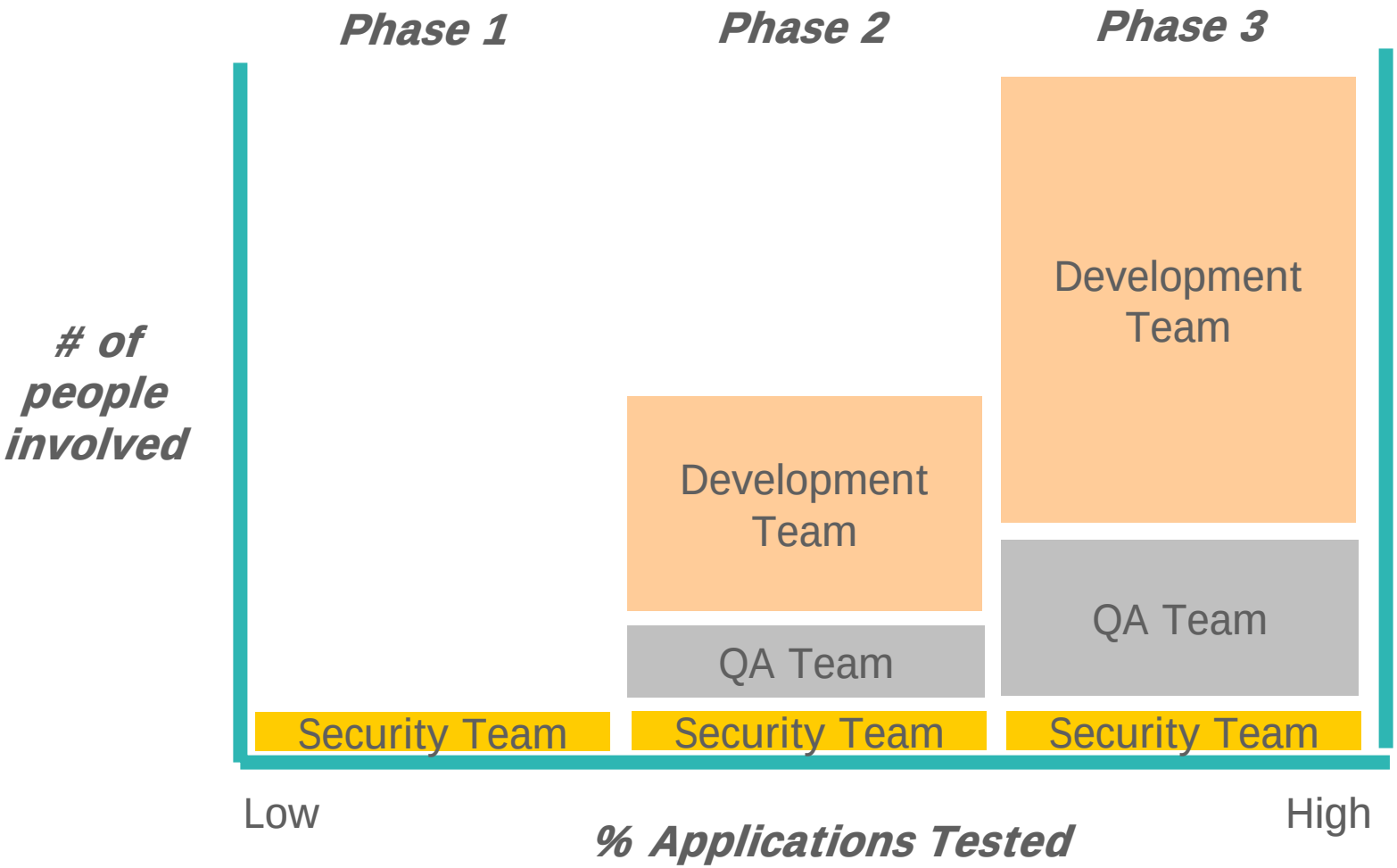


Driver #1 – Cost Benefits of Early Detection



Source: IBM Systems Sciences Institute

Driver #2 – Need to Scale

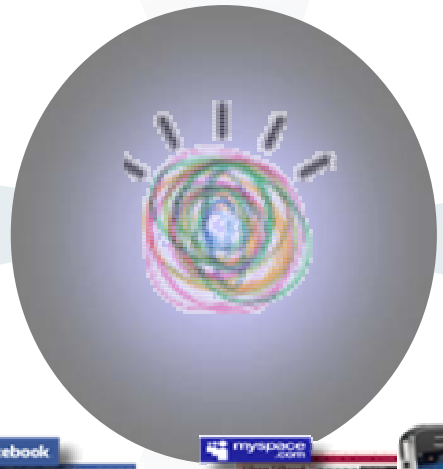


IBM Rational Vision and Roadmap for Application Security

Securing a smarter planet

Globalization and Globally Available Resources

Billions of mobile devices accessing the Web



Access to streams of information in the Real Time

New Forms of Collaboration

New possibilities.
New complexities.
New risks.

Key Focus Areas

1. Build security into the development lifecycle
   - Development, QA, Security audit, Production monitoring and defense
2. Simplify tools to match security expertise of current users
3. Leverage IBM's research and technology
4. Provide multiple delivery options
   - Software, software as service, consulting, appliance/IPS

Rational AppScan End-to-End Web Application Security

REQUIREMENTS	CODE	BUILD	QA	SECURITY	PRODUCTION
Req'ts Definition (security templates)	**AppScan Developer** (desktop)	**AppScan Build** (scanning agent)	**AppScan Tester** (scan agent & clients)	**AppScan Standard** (desktop)	**AppScan OnDemand** (SaaS)
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, audits**	**Outsourced testing for security audits & production site monitoring**

AppScan Enterprise / Reporting Console
(enterprise-wide scanning and reporting)

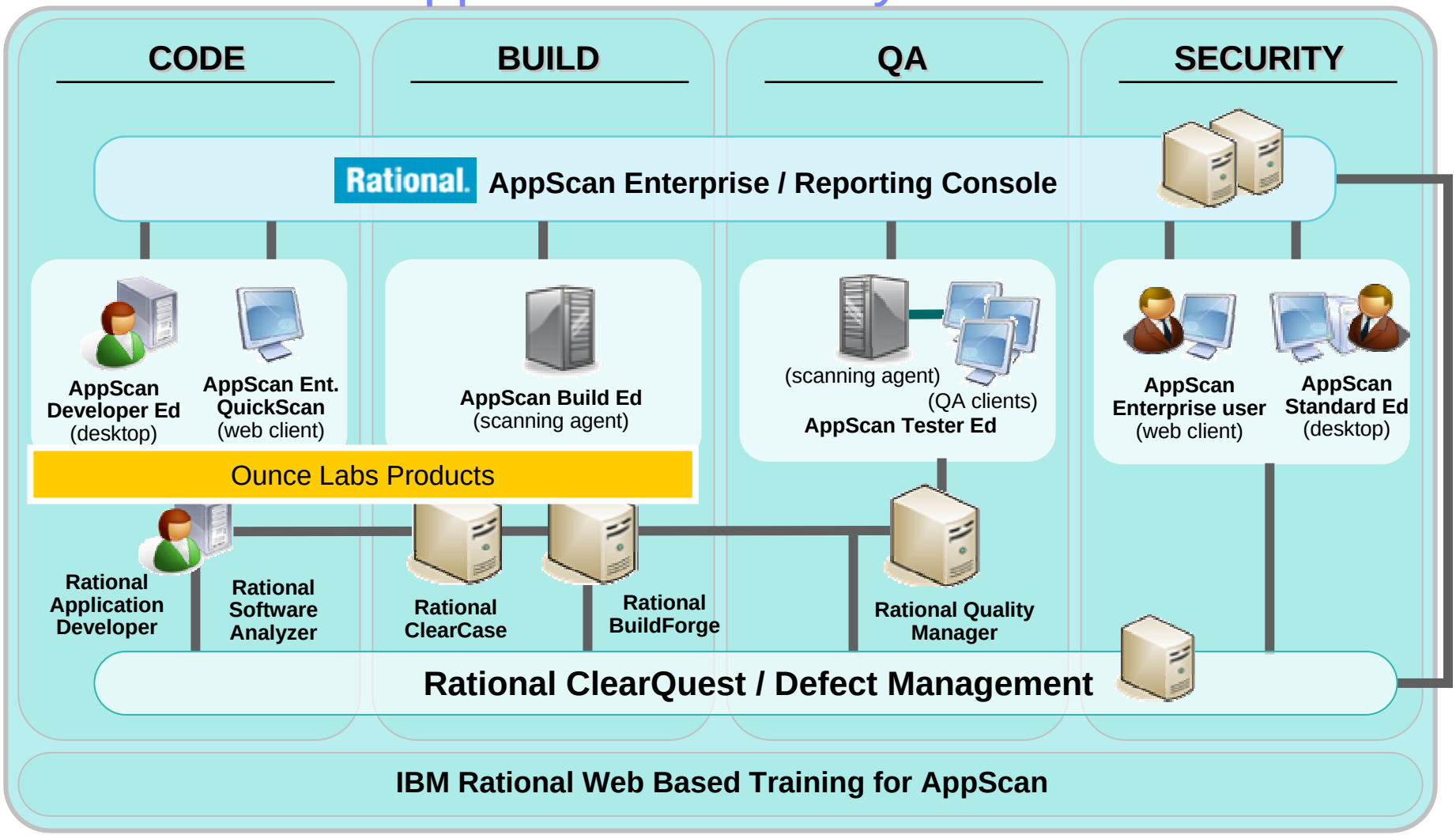
Application Security Best Practices

Address security from the start

Security audit solutions for IT Security

Security for the development lifecycle

IBM Rational AppScan – Security in the SDLC



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, audits

Who is Ounce Labs?

- Ounce is a proven leader in Static Code Analysis Security
  - Named “leader” in Gartner’s 1st Magic Quadrant for SAST (Static Application Security Testing)
  - Software developer founded 2002
  - Headquarters: Waltham, MA
  - Source code security experts

Products	• **Identifies** security vulnerabilities in application source code • **Automates and integrates** security analysis in the SDLC • **Connects** source code analysis to enterprise security and GRC platforms
Technology	• 4 **granted** source code security patents, 3 pending • **Superior** architecture for scalable enterprise deployments • **Community leadership**: Multiple solutions released into open source, senior-level contributions to PCI, SANS, CWE, OWASP, and more
Customers	• 150+ customers; 98% renewal rate • **Marquee** financial, government, retail and e-commerce customers • Solution of choice for security SIs and consultant community

Why has IBM acquired Ounce Labs?

Ounce Labs provides application source code testing tools to help enterprises reduce risk and cost associated with online security and compliance breaches.

- Application security is the largest category of vulnerability disclosures (55% in 2008)
- Rational acquired Watchfire in 2007 to address customers' Application Security Testing needs
  - AppScan continues to be recognized as the leader in Dynamic Analysis Security Testing (DAST)
  - Ounce Labs is a recognized leader in Static Analysis Security Testing (SAST)
- Application security markets are converging
  - The combination of these two industry leading technologies provides the most accurate solution in the market
  - Ounce's technology enables Rational to fulfill our vision of moving testing earlier in the development process
- Continues to add to our competitive advantage in the application security testing segment
  - Only vendor to offer complete solutions for both SAST & DAST
  - Only vendor to offer complete integration across the software delivery lifecycle
  - Only vendor to offer a complete IT security solution across all major domains (IBM Security Framework)
- Ounce is a good fit
  - Mature technology that supports all key development technologies and languages (Java, .NET, C/C++)
  - Excellent integrations with Rational SDLC products and for the developer – Rational's traditional user base

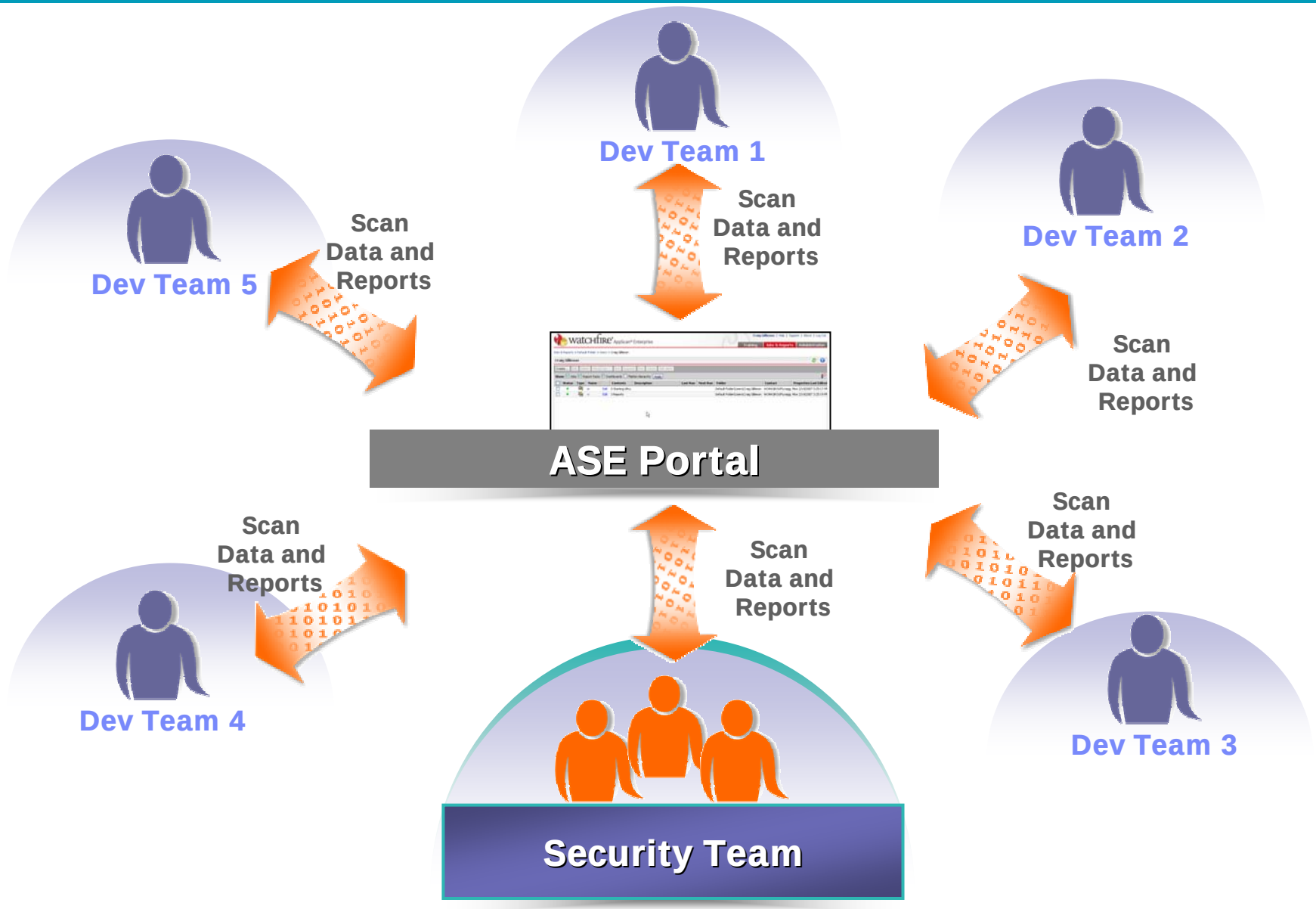
Application Security in: Code/Build

REQUIREMENTS	CODE	BUILD	QA	SECURITY	PRODUCTION
Req'ts Definition (security templates)	**AppScan Developer**	**AppScan Build**	**AppScan Tester** (scan agent & clients)	**AppScan Standard** (desktop)	**AppScan OnDemand** (SaaS)
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, audits**	**Outsourced testing for security audits & production site monitoring**

Ounce Labs Products

AppScan Enterprise / Reporting Console (enterprise-wide scanning and reporting)

Application Security Best Practices


Dev Team 1
Scan
Data and
Reports
Dev Team 2
Scan
Data and
Reports
Dev Team 5
Scan
Data and
Reports
ASE Portal
Scan
Data and
Reports
Scan
Data and
Reports
Dev Team 4
Scan
Data and
Reports
Dev Team 3
Security Team

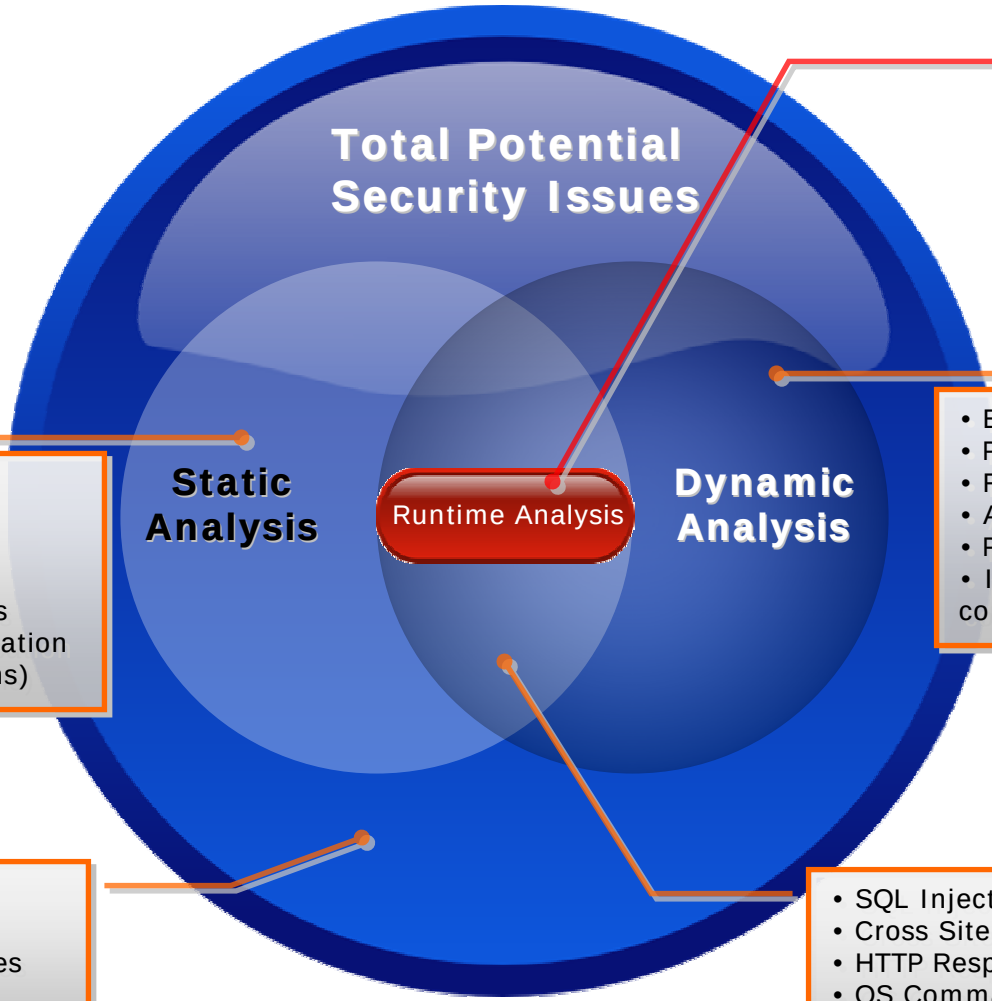
IBM Rational AppScan Developer & Build Editions

- Web Application Security Solutions for Development
  - ***The most efficient place in the SDLC to find and fix security issues***

- Developer Solution **Empowers** Developers to do Security Testing
  - *Desktop IDE-Integrated Solution for Developers*
  - *Also helps build a developer's web appsec awareness*

- Build Solution **Ensures** All Code is Scanned
  - *Many dev environments do automated regression tests in their regular build process*
    - *Now can include Security tests in regression tests*
  - *Automation-Friendly, Build time oriented solution*
  - *Key Stakeholder/User – Build Engineer*

Security Issues Coverage



Runtime Analysis serves as the “glue” between Static & Dynamic Analysis. It helps correlate results and improve overall accuracy & actionability

- Null Pointer Dereference
- Threading Issues
- Code Quality Issues
- Issues in Dead Code
- Insecure Crypto Functions
- Issues in Back-End Application Code (Multi-Tier Applications)

- Environment Configuration Issues
- Patch Level Issues
- Runtime Privileges Issues
- Authentication Issues
- Protocol Parser/Serializer Issues
- Issues in external 3rd party components

- Application Logic Issues

- SQL Injection
- Cross Site Scripting
- HTTP Response Splitting
- OS Commanding
- LDAP Injection
- ...

Roadmap Highlights: Code/Build

- Add new language support
  - Current product only supports Java, In 2009 we will add .NET Support
  - analysis of Web Applications built on .NET; using both black box and white box testing techniques
- String Analysis
  - Provides automatic detection of user defined sanitizers – automating parts of the configuration to contain false positive issues from static analysis
  - Included to-date as a Tech Preview; will improve accuracy and performance, modify detection methodology, and be turned on by default
- Enhanced Static Analysis engine
  - Support for all Java frameworks (including Portal and services)
- Evolve performance, scalability and usability
  - Responding to customer feedback to date
- Tighter integration with Code Quality tools (Software Analyzer and Logiscope)

Application Security in: QA

REQUIREMENTS	CODE	BUILD	QA	SECURITY	PRODUCTION
 *Req'ts Definition* (security templates)	 **AppScan Developer** (desktop)	 **AppScan Build** (scanning agent)	 **AppScan Tester** (scan agent & clients)	 **AppScan Standard** (desktop)	 **AppScan OnDemand** (SaaS)
			AppScan Enterprise / Reporting Console (enterprise-wide scanning and reporting)		
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, audits**	**Outsourced testing for security audits & production site monitoring**

Application Security Best Practices

Introducing AppScan Tester Edition for RQM

RQM - Rational Quality Manager

✓ Embedd Security Testing into the QA Process

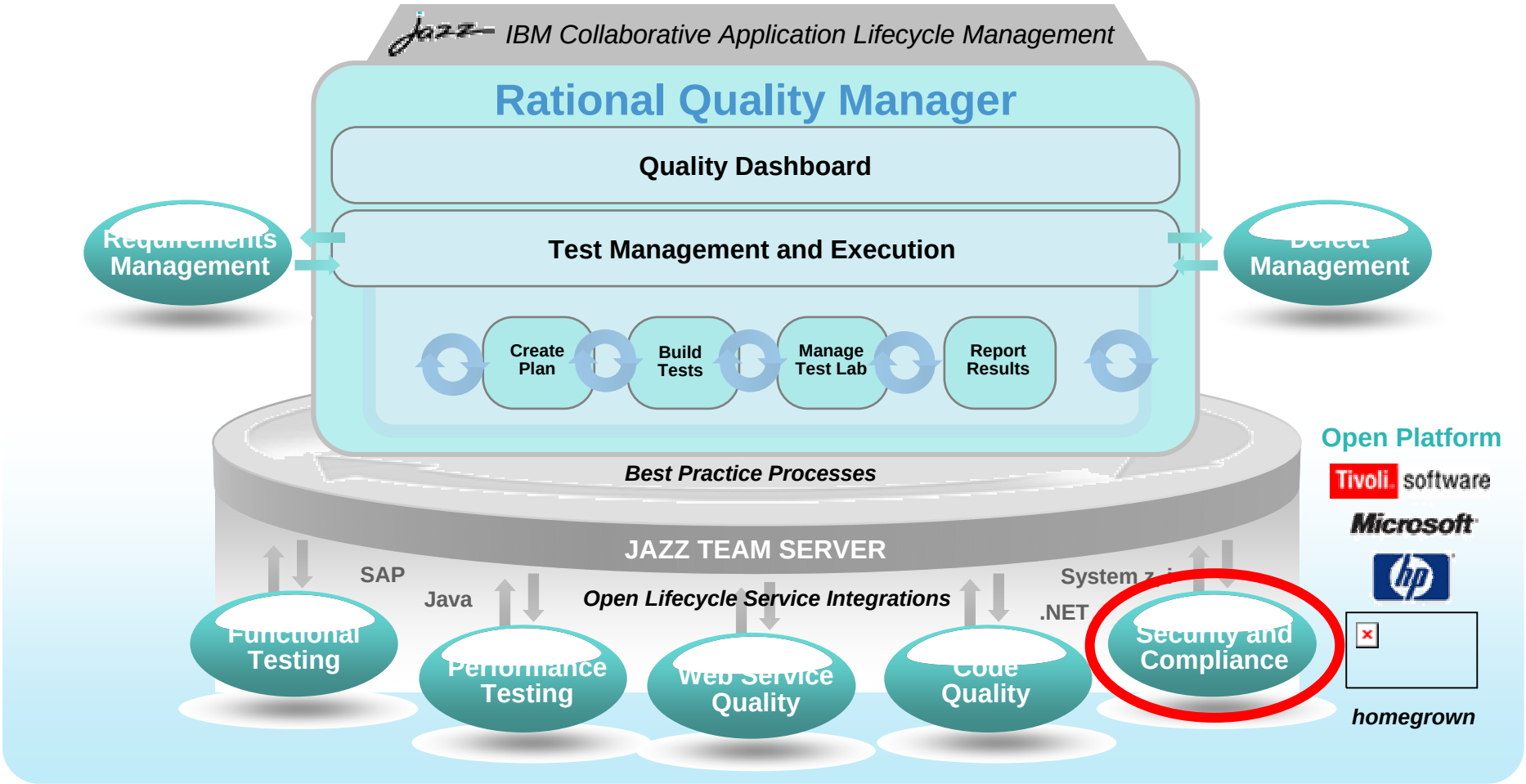
- Ideal way to scale security testing
- Integrated into the QA environment to enable the adoption of security testing alongside functional and performance testing

✓ Delivering the building blocks to help customers build a process to address security & compliance

- Leverage existing compliance mechanisms in the QA process
- Provides collaboration tools for security testing between development, QA and security teams

<u>The Result</u>: Seamless integration of security testing to provide Collaboration, Automation and Reporting

Rational Quality Manager – Test Management Hub



Application Security in: Security Team

REQUIREMENTS	CODE	BUILD	QA	SECURITY	PRODUCTION
 *Req'ts Definition* (security templates)	 **AppScan Developer** (desktop)	 **AppScan Build** (scanning agent)	 **AppScan Tester** (scan agent & clients)	 **AppScan Standard** (desktop)	 **AppScan OnDemand** (SaaS)
		AppScan Enterprise / Reporting Console (enterprise-wide scanning and reporting)			
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, audits**	**Outsourced testing for security audits & production site monitoring**

Application Security Best Practices

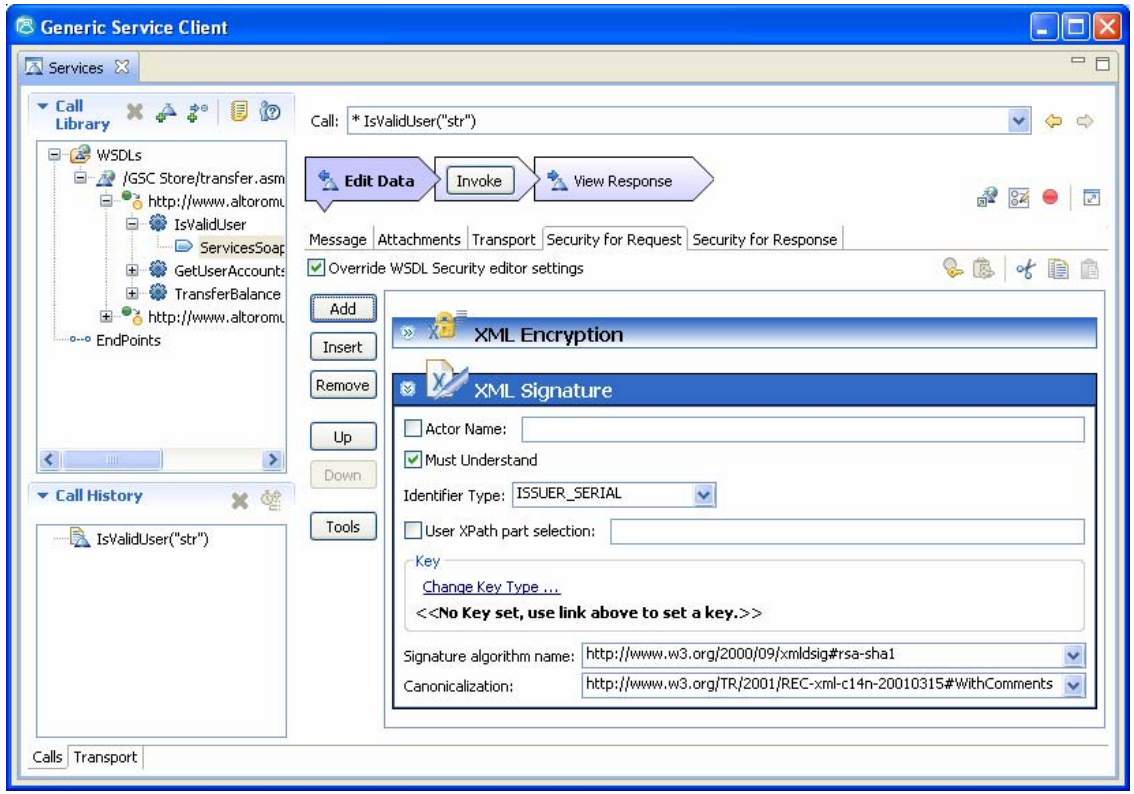
Advancing Web 2.0 Security: automatically auditing Adobe Flash Applications

- Evolution of Flash support
  - First generation tools partially explored through Flash applications
  - Second generation (emerging now) can fully explore and audit Flash applications
- Rational AppScan automatically scans Flash-based applications
  - Is the first to introduce automatic Flash Execution (first “Second Generation” scanner)
  - Similar to AJAX: 1st gen was parsing, 2nd gen was execution
- Automatically explores deep and complex Flash applications
- Identifies traditional, as well as Flash-specific security issues
  - Cross-Site Flashing, Cross-Site Scripting through Flash, Phishing…
- Supports Flash & Flex applications
  - Includes server-side testing of Flex applications (only scanner to support AMF protocol)
- Continued leadership in Flash application security
  - Flash Execution is now a strategic & evolving component of AppScan

Extending AppScan's lead in Web Services security testing

- Web Services momentum continues
  - Enterprise Modernization allows organizations to transition legacy applications to sophisticated **Web 2.0** and **SOA** solutions, driven by user demand
  - Legacy applications were not designed with Web security considerations
  - SOA deployments present a complex and rich technology heavy scanning environments

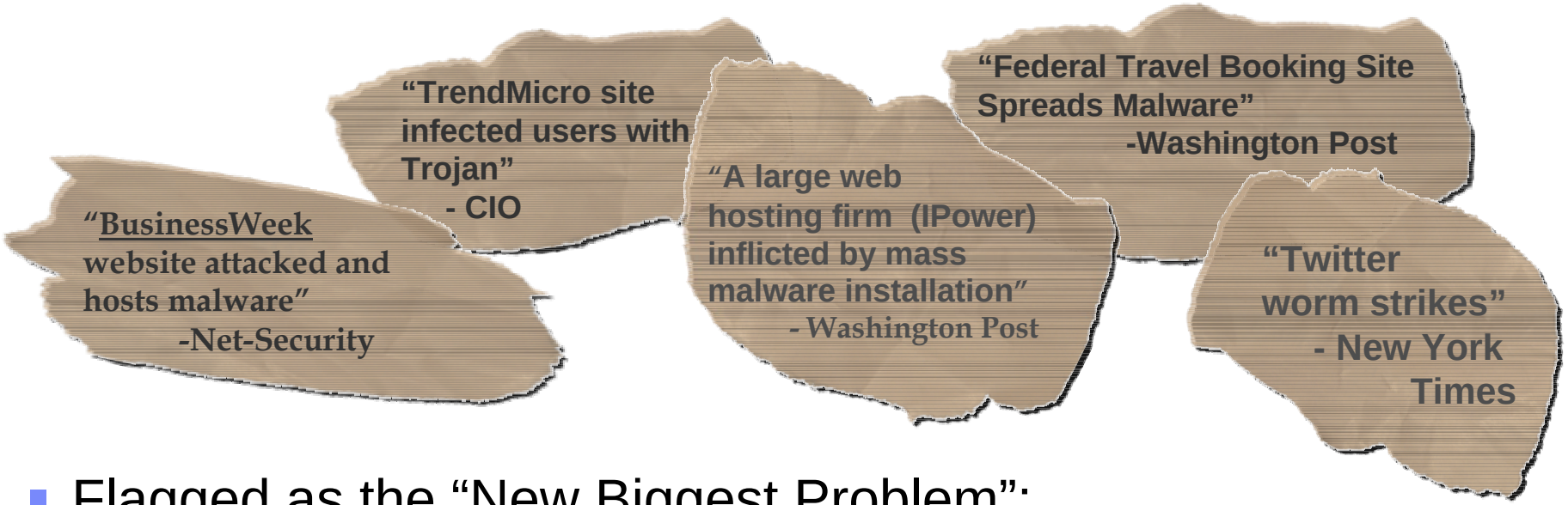
- Leveraging IBM's rich investment in SOA
  - Using established Rational SOA Tester capabilities
  - Powerful functional & performance testing for SOA
  - AppScan to include GSC: General SOA Client
- Testing Custom Web Services code
  - Identifies business logic vulnerabilities
- Support complex Web Services deployments
  - XML Signatures
  - XML Encryption
  - Complex Types in WSDL
  - …




Cross-Site Scripting
CVSS support provides industry standard severity rating
URL: http://local/altoro/comment.asp
Entity: comment.aspx
Security Risk: It is possible to steal or manipulate customer session and cookies, which may be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
High
CVSS Metrics Scoring (8)
Base
Temporal
Environmental
The script AppScan injected seems to be included in the response. If the screen shot below shows a simulation of the pop-up that the injected script produced, this is proof that the application is vulnerable to Cross-Site Scripting. If not, to verify this vulnerability: 1) Open the Request/Response tab and click Show in Browser, and see if a pop-up appears. (Note that some script syntaxes are browser specific, so if the injected alert doesn't pop up, try a different browser (View Source > Save As...). 2) Check the validity of the alert script(s) in the raw test response.
Guides user through verifying that the issue is a legitimate vulnerability
Click to View Full Size
Sign Off | Contact Us | Feedback | Search Go
DEMO SITE ONLY
8172
OK
Simulation of the pop-up that will appear when this page is opened in a browser
MY ACCOUNT
PERSONAL
INSIDE ALTORO MUTUAL
PERSONAL
Deposit Product
Checking
Loan Products
Cards
Investments & Insurance
Other Services
SMALL BUSINESS
Deposit Products
Lending Services
Cards
Integrated screenshots with explanations immediately demonstrate whether an issue truly exists, saving time and effort

The Problem: Legitimate Sites serving Malware

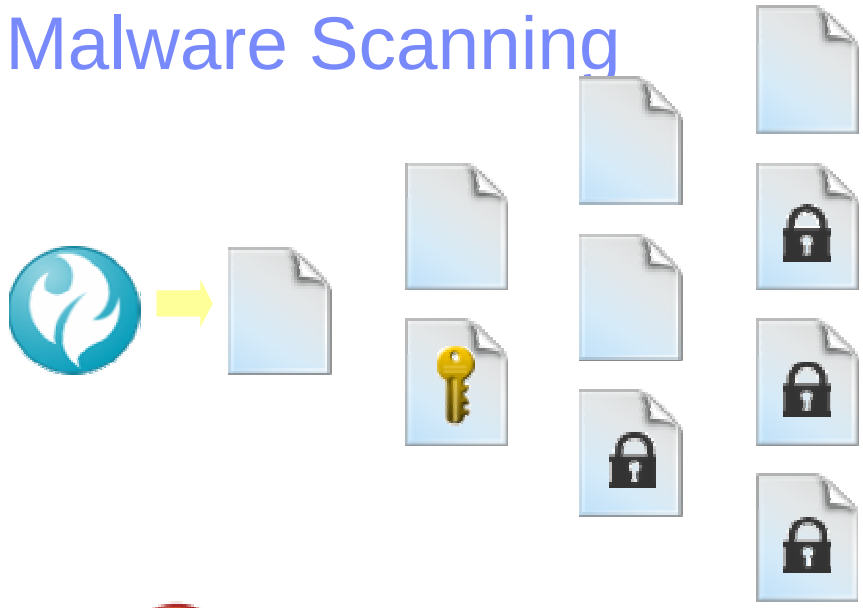
- Malware is served or linked primarily from **Legitimate Sites!**



- Flagged as the "New Biggest Problem":
  - WebSense: "Legitimate Sites Carry Increasing Portion Of Malware" (Jan, '09)
  - ScanSafe: "Web-based malware up 400%, 68% hosted on legitimate websites" (June, '08)
  - Blog: "Online Trust: A Thing of the Past?" (Jan, '09)
  - X-Force: "Are Legitimate Sites the Next Malware Threat?" (Feb, '09)
  - Breach: "SQL Injection Attacks Planting Malware on Web Sites Ranks #1 in Breach Security's 2008 Web Hacking Incidents Database Report" (Feb, '09)

AppScan's HTTP-Based Malware Scanning

1. **Discover all content and links in a Web Application**
   - Execute JavaScript & Flash
   - Fill forms and login sequences
   - Analyze secure pages
   - …



2. **Analyze all content for malicious behavior indicators**

3. **Compare all links to comprehensive black-lists**

Application Security in: Production

REQUIREMENTS	CODE	BUILD	QA	SECURITY	PRODUCTION
Req'ts Definition (security templates)	**AppScan Developer** (desktop)	**AppScan Build** (scanning agent)	**AppScan Tester** (scan agent & clients)	**AppScan Standard** (desktop)	**AppScan OnDemand** (SaaS)
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, audits**	**Outsourced testing for security audits & production site monitoring**

AppScan Enterprise / Reporting Console (enterprise-wide scanning and reporting)

Application Security Best Practices

Expanded Options for Production Testing and Defense

1. Testing solutions:
   - AppScan Enterprise
   - AppScan OnDemand
   - ISS Managed Security Services
2. Defensive solutions:
   - ISS Proventia IPS with New Web Protection
   - DataPower SOA Appliance
3. Combined approach
   - Integrated scanning and defense

Introducing expanded Rational AppScan OnDemand

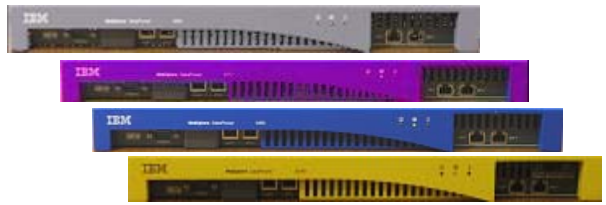
- **AppScan OnDemand:**
  - Comprehensive testing of pre-production applications
  - Periodic assessment of applications in QA or Security
  - Monthly scans
  - Flexible offerings base on organization (Small/Medium/Large)

- **AppScan OnDemand Production Site Monitoring:**
  - Continuous scanning of production Web sites for vulnerabilities that may have been introduced after the app went live
  - Dynamic or interactive content and forms, online registrations
  - Weekly scans

<u>The Result</u>: Ability to address online risk without in-house resources with the faster route to actionable information

Policy Testing OnDemand is also available to support website compliance management for Privacy, Quality & Accessibility

WebSphere DataPower SOA Appliances



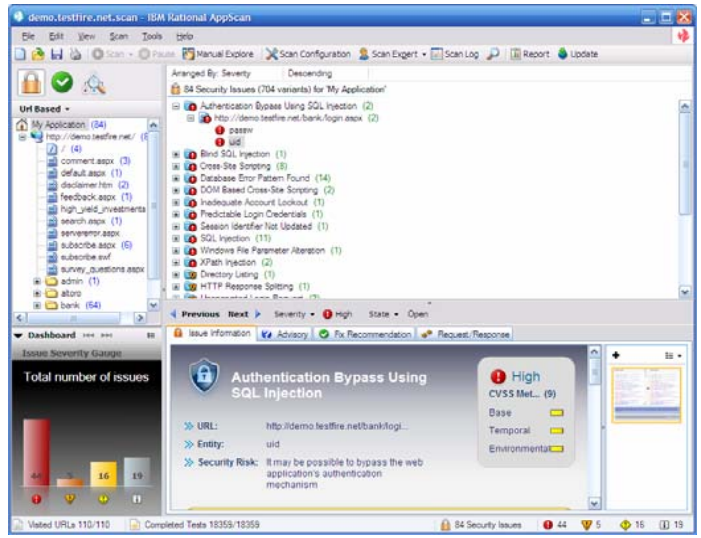
Creating customer value through extreme SOA connectivity, performance and security

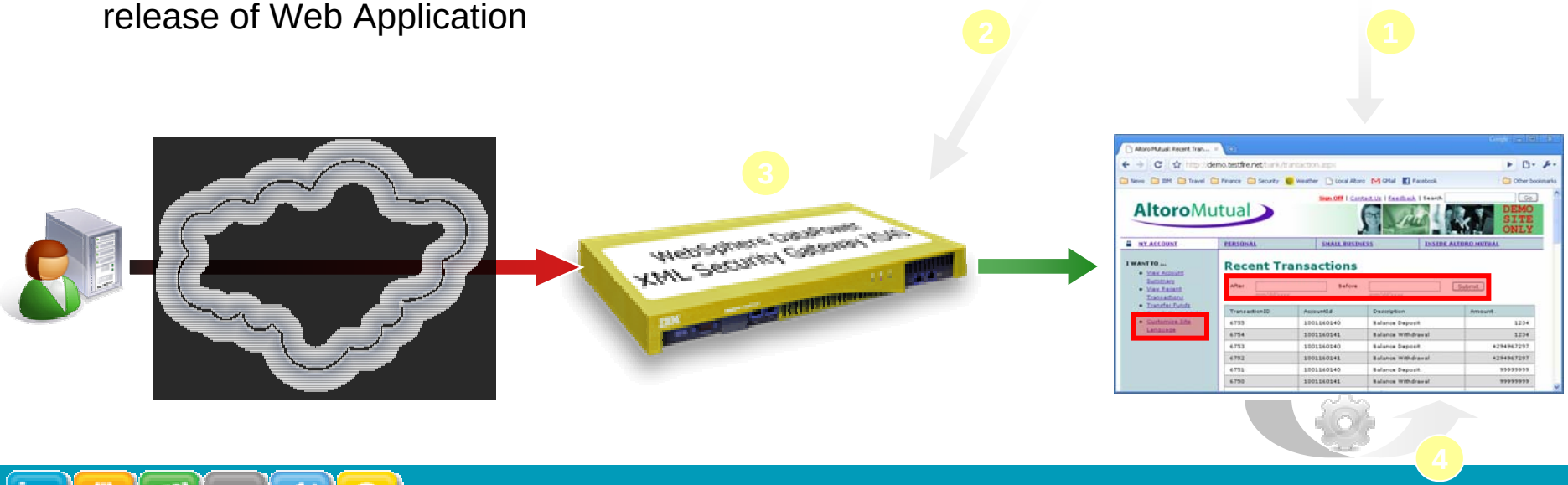
- **Simplifies** SOA and accelerates time to value
- **Helps secure** SOA XML implementations
- **Governs and enforces** SOA/Web services policies

WebSphere DataPower SOA Appliances redefine the boundaries of middleware extending the SOA Foundation with **specialized, consumable, dedicated SOA appliances** that combine **superior performance and hardened security** for SOA implementations.

Virtual Application Security Patch

1. Rational AppScan Scans Web Application, Uncovers Security Issues
2. WebSphere DataPower Rules are Auto-Created, Based on Found Issues
3. Custom protection blocks exploits on vulnerable locations, blocking where required while avoiding False Positives
4. Vulnerabilities are remediated in the next release of Web Application





Rational/ISS Vision: Application & Network Security Ecosystem

Site Protector

Proventia IDS/IPS

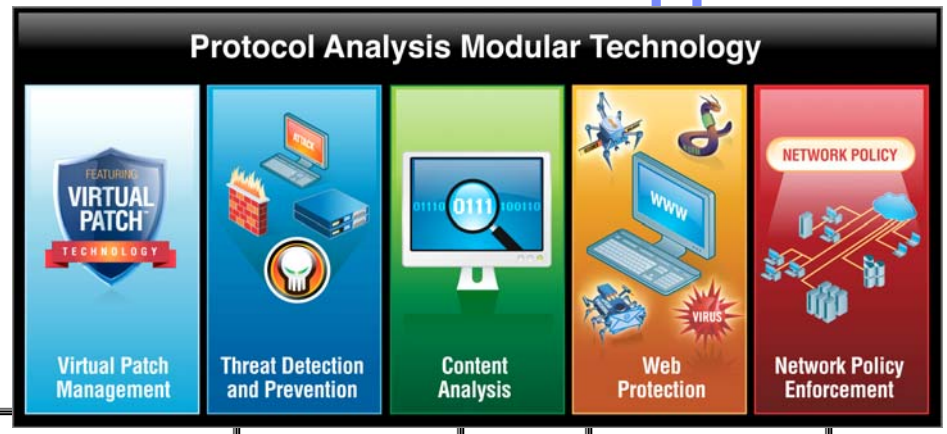
Enterprise Scanner

AppScan Agent

- Joint interface for Application & Network Security
- Collaborative flow of product usage
- Mutual leveraging of technology

Block attacks in real-time with Proventia Web application security

Intrusion prevention just got smarter with web application protection backed by the power of X-Force



Virtual Patch

What It Does:
Shields vulnerabilities from exploitation independent of a software patch, and enables a responsible patch management process that can be adhered to without fear of a breach

Why Important:
At the end of 2008, **53%** of all vulnerabilities disclosed during the year had no vendor-supplied patches available to remedy the vulnerability

Threat Detection & Prevention

What It Does:
Detects and prevents entire classes of threats as opposed to a specific exploit or vulnerability.

Why Important:
Eliminates need of constant signature updates. Protection includes the proprietary Shellcode Heuristics (SCH) technology, which has an unbeatable track record of protecting against zero day vulnerabilities.

Content Analysis

What It Does:
Monitors and identifies unencrypted personally identifiable information (PII) and other confidential information for data awareness. Also provides capability to explore data flow through the network to help determine if any potential risks exist.

Why Important:
Flexible and scalable customized data search criteria; serves as a complement to data security strategy

Web Protection

What It Does:
Protects web applications against sophisticated application-level attacks such as SQL Injection, XSS (Cross-site scripting), PHP file-includes, CSRF (Cross-site request forgery).

Why Important:
Expands security capabilities to meet both compliance requirements and threat evolution.

Network Policy Enforcement

What It Does:
Manages security policy and risks within defined segments of the network, such as ActiveX fingerprinting, Peer To Peer, Instant Messaging, and tunneling.

Why Important:
Enforces network application and service access based on corporate policy and governance.

2009 Roadmap

Q1

- New AppScan Releases
  - AppScan Standard, Express, Developer, Build
- Product Translations
  - Available for all products
  - Japanese, Korean, Traditional Chinese, Simplified Chinese, French, Italian, and German
- Expanded SaaS offering
  - Production Site Monitoring

Q3

- Web-based Malware Detection & Scanning
- AppScan-ISS SiteProtector Integration

Q4

- Portfolio-wide release (including Ounce)
- Joint ISS initiatives


Questions