Scaling AppScan Source Edition for the Enterprise

Steve Carlucci
Software Architect, IBM
steve.carlucci@us.ibm.com

Duncan Smith
Software Architect, IBM
duncan.smith@ca.ibm.com

Innovate2010
The Rational Software Conference

Let's build a smarter planet.

The premiere software and product delivery event.

Agenda

- AppScan Source Edition Overview
- Workflow Scenario 1 – AppScan Source Edition
- Key improvements in Source Edition 7.0
- Workflow Scenario 2 - AppScan Source Edition with AppScan Reporting Console
- Workflow Scenario 3 - AppScan Source Edition with AppScan Enterprise

AppScan Source Edition Overview

- AppScan Source Edition is a static source code analysis tool for finding security vulnerabilities
- A wide variety of languages are supported
  - Java, .NET, C/C++, PHP, etc
- Various components for hooking into the SDLC
  - Source Edition for Security
  - Developer plugins
  - Build integration tools
  - DTS integration
  - SDK

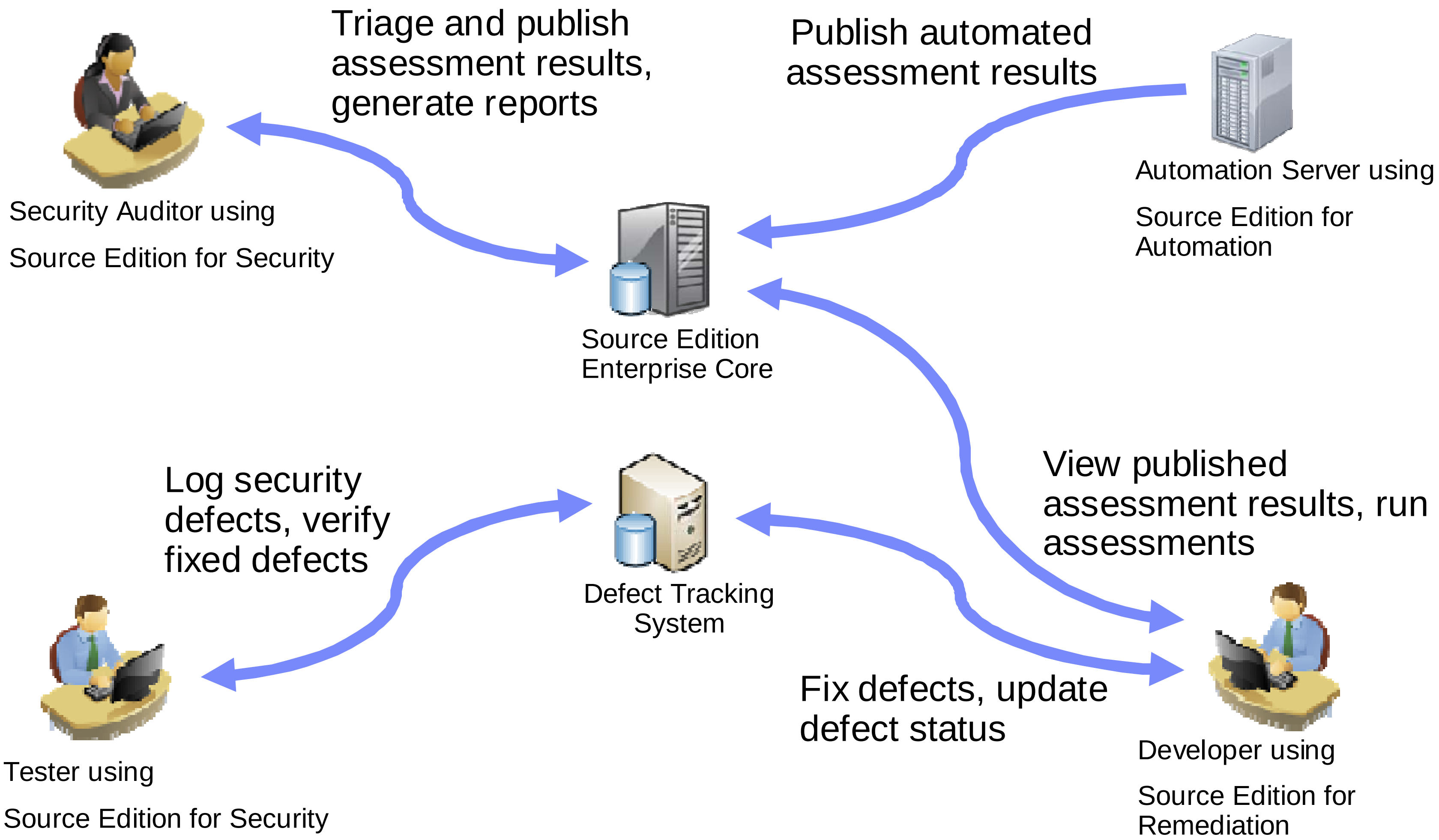
AppScan Source Edition Products

- Source Edition for Core
  - Central repository for shared data
- Source Edition for Security
  - Desktop-based client for configuration, scanning, triage, and analysis
- Source Edition for Remediation
  - IDE plugin that provides developers with remediation capabilities
- Source Edition for Developer
  - IDE plugin with all of the features of Remediation, along with the ability to run scans
- Source Edition for Automation
  - Automate key aspects of the Source Edition workflow
  - Plugins for Make, Ant, and Maven allow the configuration process to be automated

AppScan Source Edition Products vs Roles

Role	Product
Security Auditor	Source Edition for Security
Developer	Source Edition for Security Source Edition for Remediation Source Edition for Developer
Tester	Source Edition for Security
Release Engineer	Source Edition for Automation

Workflow Scenario 1 – AppScan Source Edition



Triage and publish assessment results, generate reports

Publish automated assessment results

Security Auditor using

Source Edition for Security

Automation Server using

Source Edition for Automation

Source Edition Enterprise Core

Log security defects, verify fixed defects

Defect Tracking System

View published assessment results, run assessments

Fix defects, update defect status

Tester using

Source Edition for Security

Developer using

Source Edition for Remediation

Useful Source Edition Definitions

- Taint
  - Untrusted data that has entered a program from an external source
- Source
  - A location where tainted data enters a program
- Sink
  - A location where data exits a program
- Trace
  - Visual representation of the flow of tainted data from source to sink

AppScan Source Edition 7.0 Improvements

- Performance and scalability improvements
  - Redesigned assessment results model
- Triage improvements
  - New Sources and Sinks view
  - New trace filter rule
- Expanded Language support
  - PHP, Perl, ColdFusion, Client-side JavaScript
- AppScan Enterprise and Reporting Console Integration

Performance and Scalability Improvements

- Assessment results model redesigned to optimize memory usage
- In-memory, XML, and DB representation of assessment results reduced by as much as 90% in some cases
- Reduction in memory allows much higher scalability for scanning large applications
- Many operations involving the results are much faster

Triage Improvements

- Trace filter rules
  - Allow powerful filtering of assessment results based on properties of the data-flow trace associated with each finding
  - Findings can be filtered based on properties of the source, sink, and intermediate nodes of the data-flow trace
- Source and Sink View
  - A view dedicated to triaging results based on the sources (inputs) and sinks (outputs) of an application
  - Allows for quick identification of sources and sinks

Expanded Language Support in 7.0

- New language support
  - PHP
  - Perl
  - ColdFusion
  - Client-side JavaScript
- Existing languages
  - C/C++
  - Java/JSP
  - .NET (C#, ASP.NET, VB.NET)
  - Classic ASP (VB6)

AppScan Enterprise Integration

- AppScan Source Edition assessment results can be published to AppScan Enterprise or Reporting Console
- Results can be published from several components
  - AppScan Source Edition for Security
  - AppScan Source Edition for Automation
  - AppScan Source Edition CLI

AppScan Source Edition and 7.0 enhancements

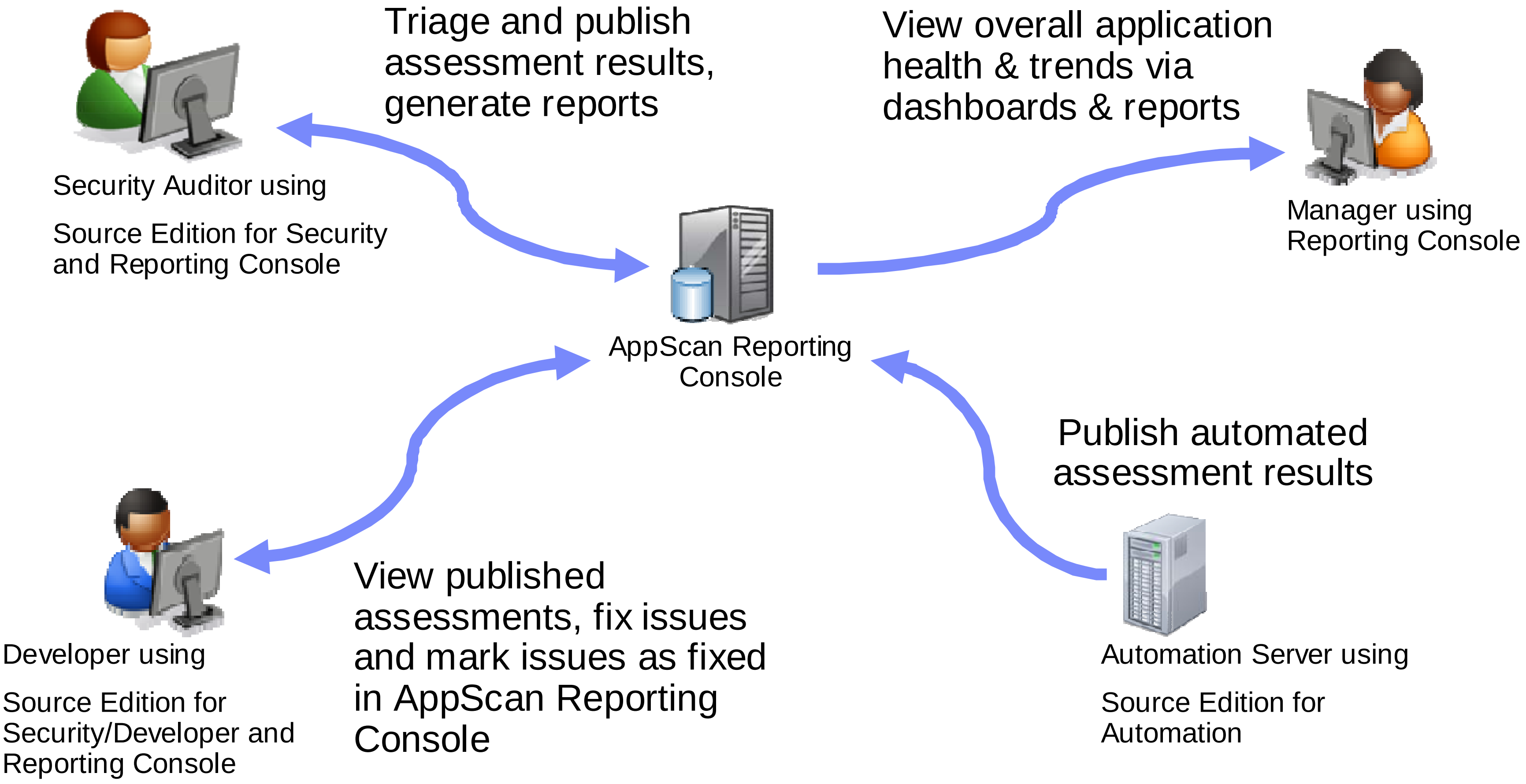
AppScan Reporting Console

- Web-based interface with enterprise reporting capabilities
  - Enables communication and collaboration amongst team members
- Compliance reports identify potential regulation violations
- Access permissions and user roles control how different stakeholders are engaged
- High-level dashboards provide management a sense of the security risk their Web applications present and the progress towards mitigating that risk
- Integrates with some defect tracking systems
  - Exposes RESTful services to enable integrations with other SDLC solutions

AppScan Source with AppScan Reporting Console

- Assessments can be published from AppScan Source Edition to AppScan Reporting Console
- Reports and dashboards can combine the results of multiple assessments
  - Findings merged to prevent duplicates
  - Multiple variations of the same finding grouped in the same issue

Workflow Scenario 2 – AppScan Source + AppScan Reporting Console



Triage and publish assessment results, generate reports

Security Auditor using

Source Edition for Security and Reporting Console

View overall application health & trends via dashboards & reports

Manager using Reporting Console

AppScan Reporting Console

Publish automated assessment results

Developer using

Source Edition for Security/Developer and Reporting Console

View published assessments, fix issues and mark issues as fixed in AppScan Reporting Console

Automation Server using

Source Edition for Automation

AppScan Source with AppScan Reporting Console

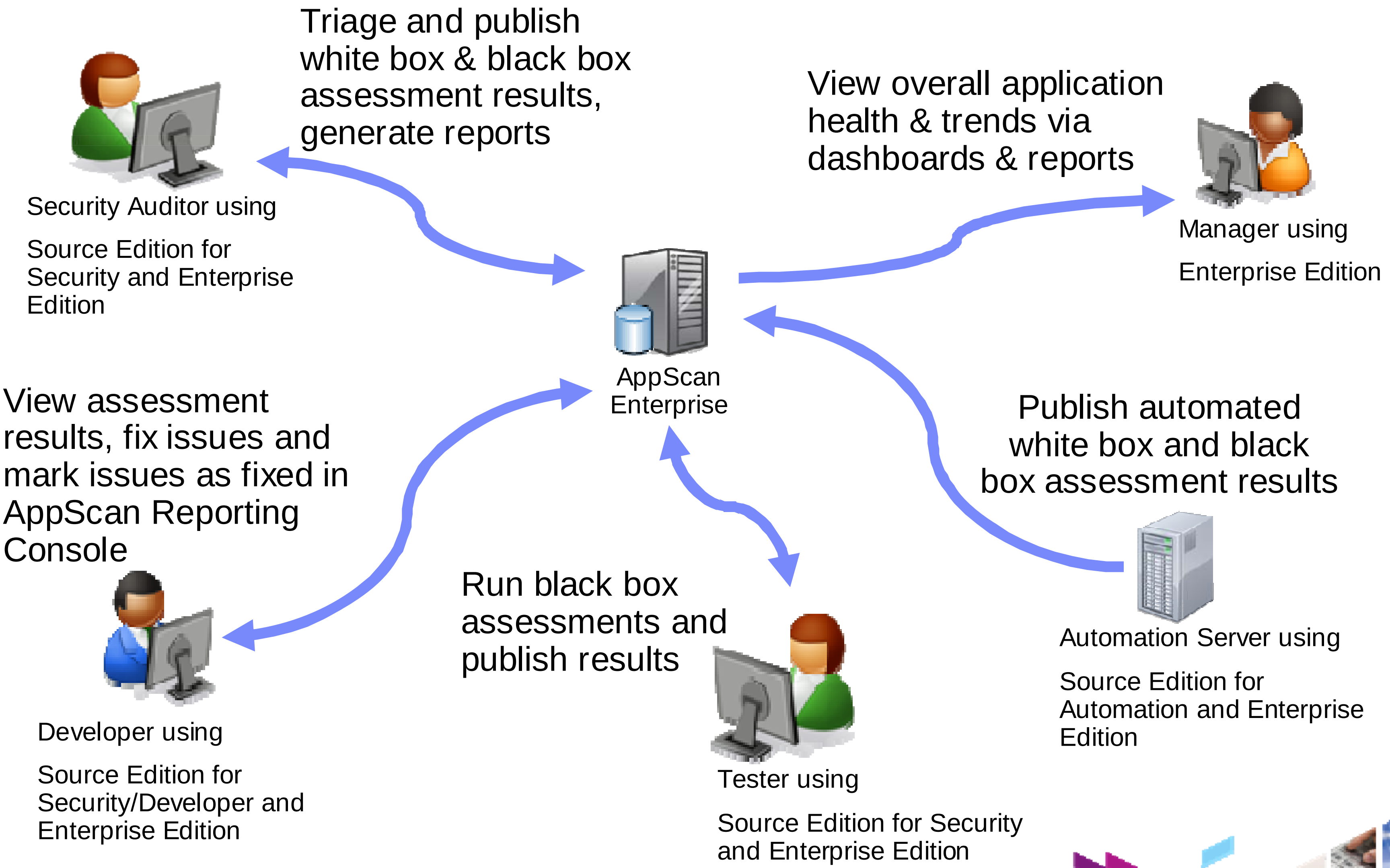
AppScan Enterprise

- Extends AppScan Reporting Console
- Provides dynamic analysis (black box) testing capabilities
  - Handles simultaneous security testing of a large number of Web applications
- Information Security can define the security test policies used by developers and testers for dynamic analysis assessments
- Detailed vulnerability advisories and fix recommendations educate developers about the causes of vulnerabilities and how to avoid them

AppScan Source with AppScan Enterprise

- Extends functionality of AppScan Source with AppScan Reporting Console
- Combines benefits of dynamic analysis and static analysis to provide more comprehensive view of organization’s Web application security picture
  - Dashboards include data for both dynamic and static analysis issues
  - Access permissions and user roles control visibility into both dynamic and static analysis data

Workflow Scenario 3 – AppScan Source + AppScan Enterprise



Triage and publish white box & black box assessment results, generate reports

Security Auditor using

Source Edition for Security and Enterprise Edition

View overall application health & trends via dashboards & reports

Manager using

Enterprise Edition

AppScan Enterprise

View assessment results, fix issues and mark issues as fixed in AppScan Reporting Console

Publish automated white box and black box assessment results

Developer using

Source Edition for Security/Developer and Enterprise Edition

Run black box assessments and publish results

Tester using

Source Edition for Security and Enterprise Edition

Automation Server using

Source Edition for Automation and Enterprise Edition

AppScan Source with AppScan Enterprise

Disclaimer: © Copyright IBM Corporation 2010. All rights reserved. These materials are intended solely to outline our general product direction and should not be relied on in making a purchasing decision. Information pertaining to new product is for informational purposes only, is not a commitment, promise, or legal obligation to deliver any material, code or functionality, and may not be incorporated into any contract. The development, release, and timing of any features or functionality described for our products remains at our sole discretion. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM products. IBM, the IBM logo, Rational, the Rational logo, Telelogic, the Telelogic logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Summary

- AppScan Source and Enterprise are designed with large enterprise applications in mind
- AppScan products provide coverage across many areas of the SDLC
- Automation components allow much of the security analysis process to be automated

Questions

www.ibm.com/software/rational

The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, Rational, the Rational logo, Telelogic, the Telelogic logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.