IBM Security AppScan 8.6
Application Security throughout the lifecycle

Tibor Bősze - tibor.boesze@hu.ibm.com
IBM Security Architect for CEE+RCIS
2012-06-12

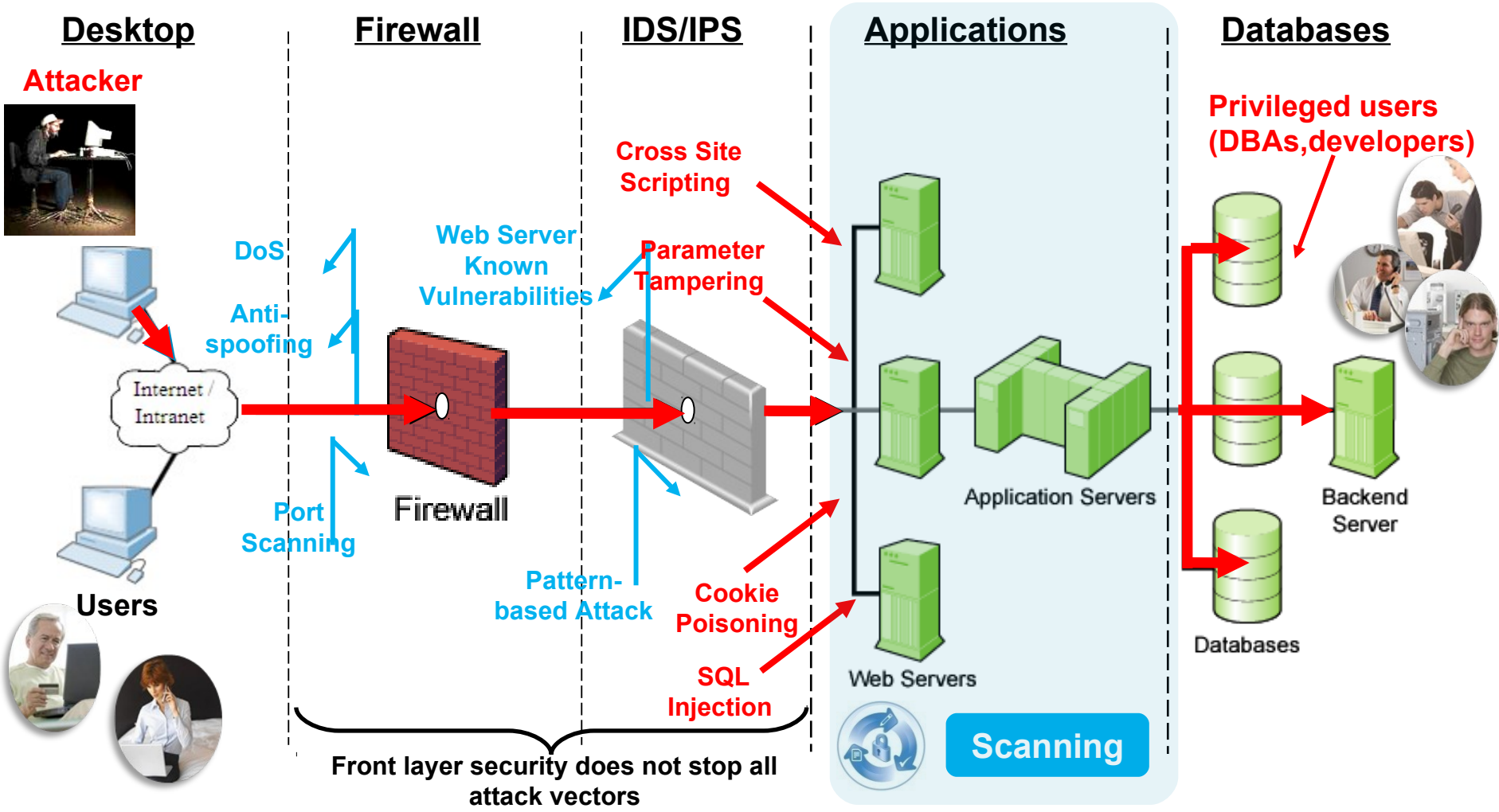
Breaking news!

- **IBM Security AppScan 8.6 available from TODAY (2012-06-12)**
  - GA for electronic delivery: 12 June 2012
  - GA for media delivery: 15 June 2012
- **Key Deliverables:**
  - Nextgen Dynamic Application Security Testing
  - Autolearning JavaScript and XSS analyzers
  - Testing mobile targeted webapps
  - Static Application Security Testing for android
  - Application Discovery Assistant
  - Extended support for JSF and Struts2
  - QRadar integration

Agenda

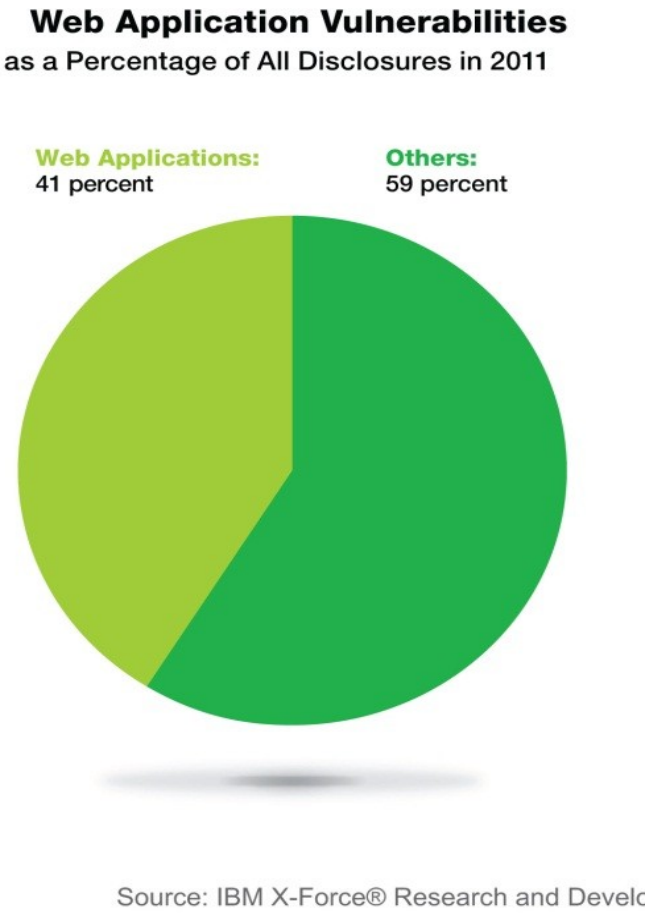
- **Why Application Security is important ?**
- **What is AppScan?**
  - **How AppScan works?**
  - **Dynamic Application Security Testing (DAST)**
  - **Static Application Security Testing (SAST)**
- **AppScan 8.6 Portfolio**
- **What's new in AppScan 8.6**
  - **AppScan Enterprise** ***(Formally known as IBM Rational AppScan Enterprise)***
  - **AppScan Source** ***(Formally known as IBM Rational AppScan Source)***
- **Where can I get help?**

Why Applications Security should be part of a holistic security program

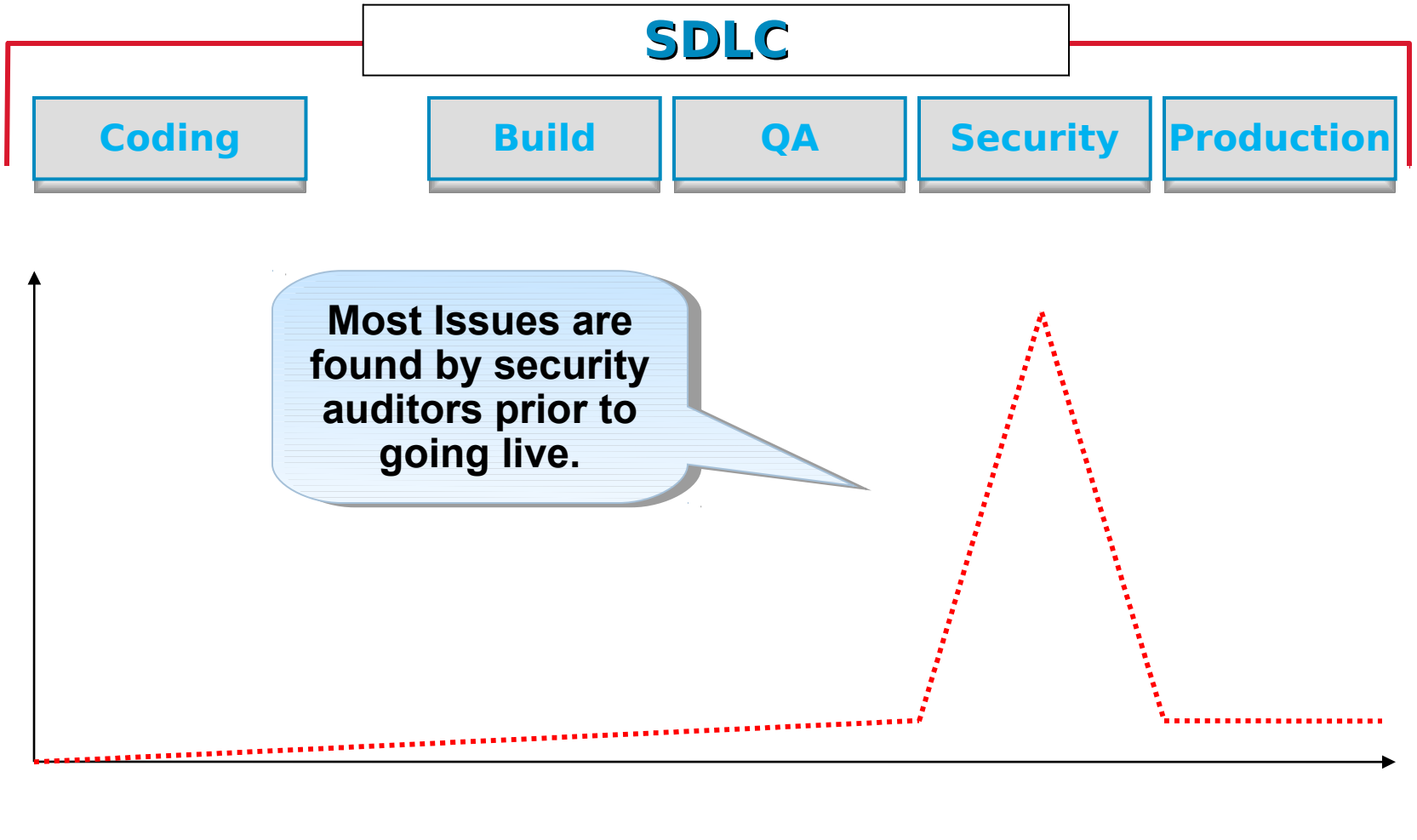


Manage Risks and Compliance/Governance

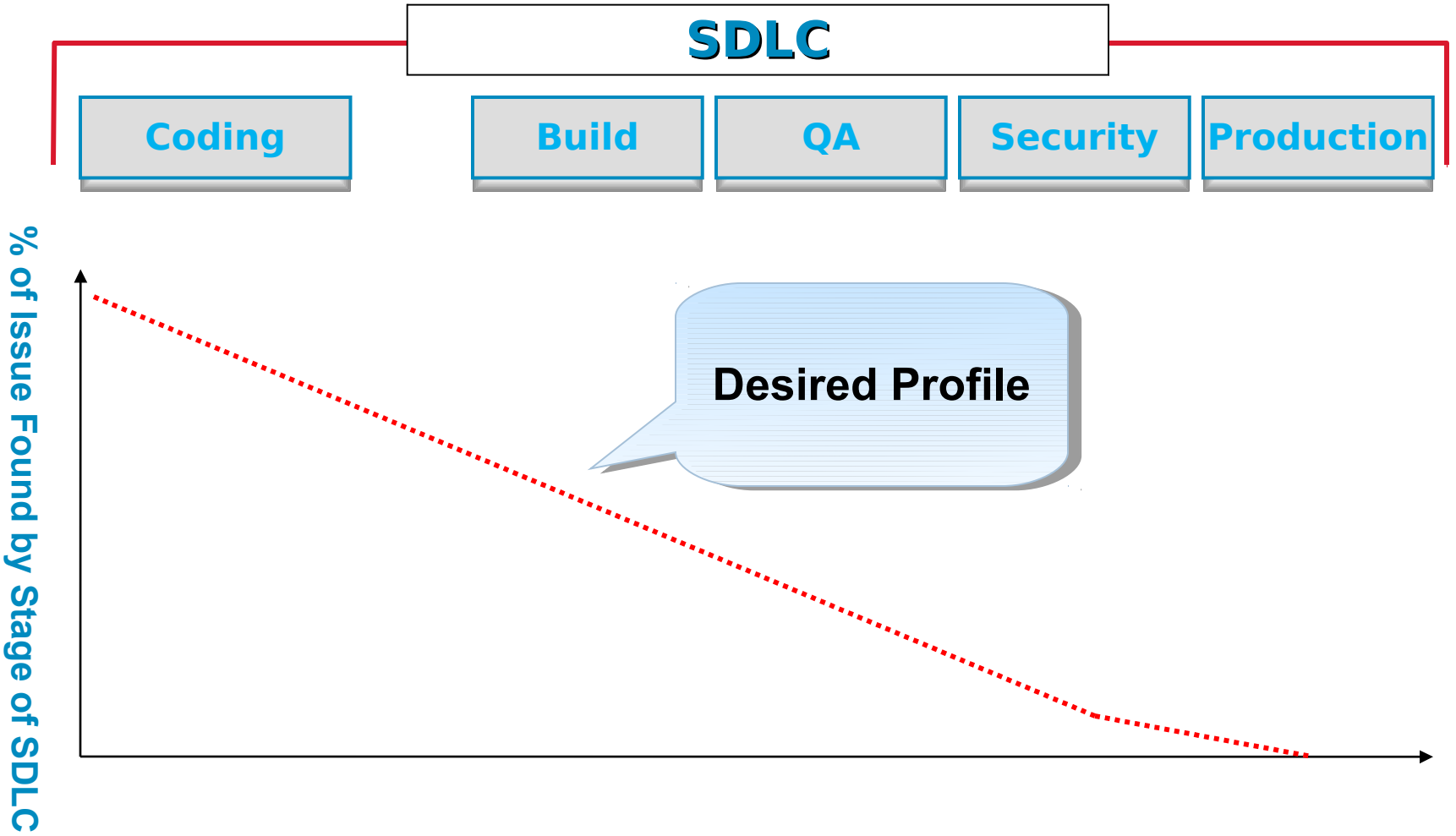
- **55%** of respondents cited mobile security as a primary technology concern over the next two years. (IBM Center for Applied Insights)
- **76%** of CEOs (Ponemo 2010) feel reducing security flaws within business-critical applications is the most important aspect of their data protection programs.
- **41%** of all vulnerabilities are Web application vulnerabilities. (X-Force 2011)
- Cross-Site Scripting & SQL injection vulnerabilities dominate OWASP Top 10.
- **89% of records breached** from hacks were related to SQL Injection flaws
- **79% of breached organizations** subject to PCI were found to be non-compliant (Verizon)
- **79% of compromised records** used Web Apps as the attack pathway Verizon



Security Testing Within the Software Lifecycle



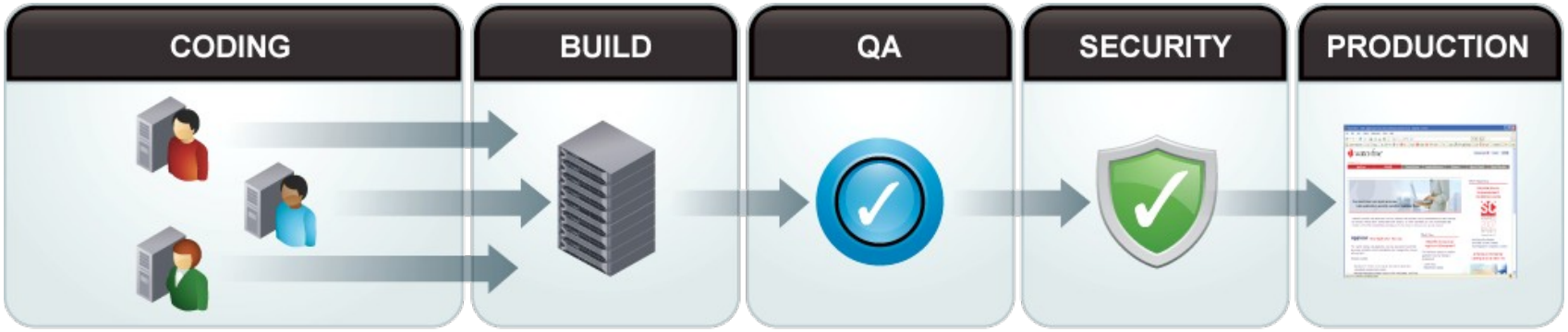
Security Testing Within the Software Lifecycle



Reducing Costs Through a Secure by Design Approach

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

Average Cost of a Data Breach 6M EUR** from law suits, loss of customer trust, damage to brand

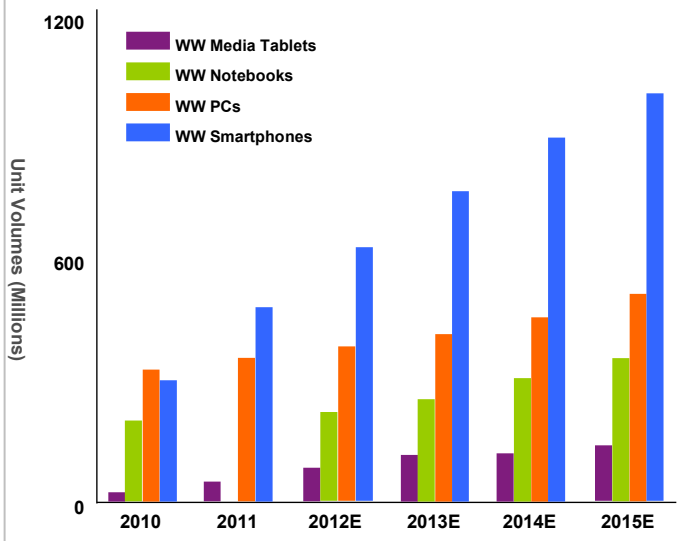


Find during Development	Find during Build	Find during QA/Test	Find in Production
64	200	800	6400
EUR / defect	EUR / defect	EUR / defect	EUR / defect

*** Source: National Institute of Standards and Technology

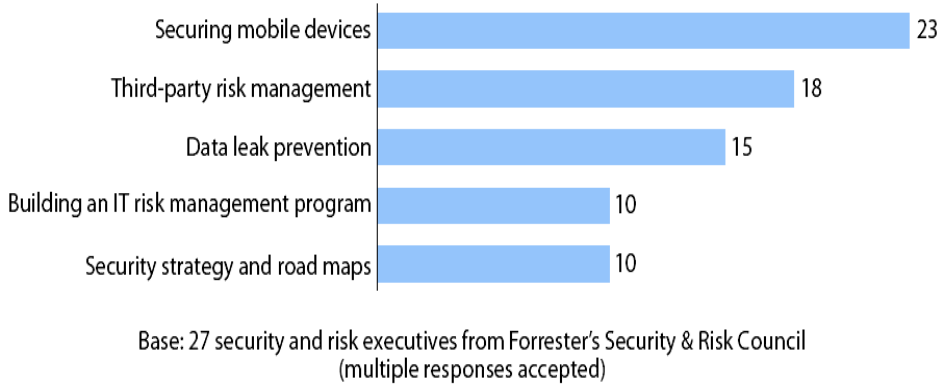
** Source: Ponemon Institute 2009-10

Mobile Security: Organizations are rapidly embracing mobile devices and applications, leading to new security challenges



Source: ***"Fostering the People: The Shift to Engagement Apps"***, Wells Fargo Securities, January 23, 2012

Select five of the *top challenges* you will face over the next six months:



Base: 27 security and risk executives from Forrester's Security & Risk Council (multiple responses accepted)

Source: ***"Executive Spotlight: Top Priorities for Security and Risk Leaders, 1H 2011"***, Forrester, April 2011

Mobile application security is top of mind for customers

Mobile Security: a key driver going forward

Agenda

- Why Application Security is important ?
- What is AppScan?
  - How AppScan works?
  - Dynamic Application Security Testing (DAST)
  - Static Application Security Testing (SAST)
- AppScan 8.6 Portfolio
- What's new in AppScan 8.6
  - AppScan Enterprise *(Formally known as IBM Rational AppScan Enterprise)*
  - AppScan Source *(Formally known as IBM Rational AppScan Source)*
- Where can I get help?

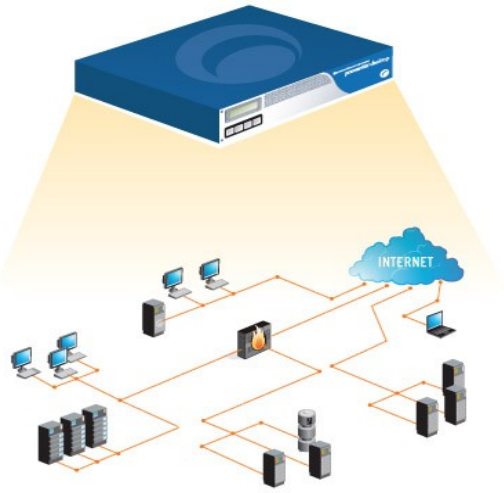
How does AppScan work?

Automates Application Security Testing

Same process for whitebox & blackbox

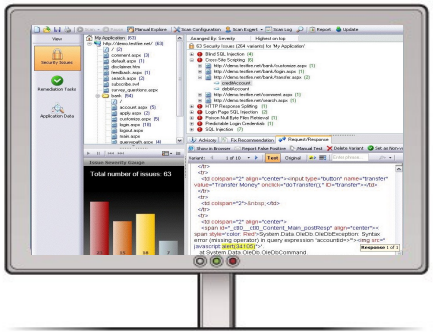
1 → 2 → 3

Scan applications



Analyze

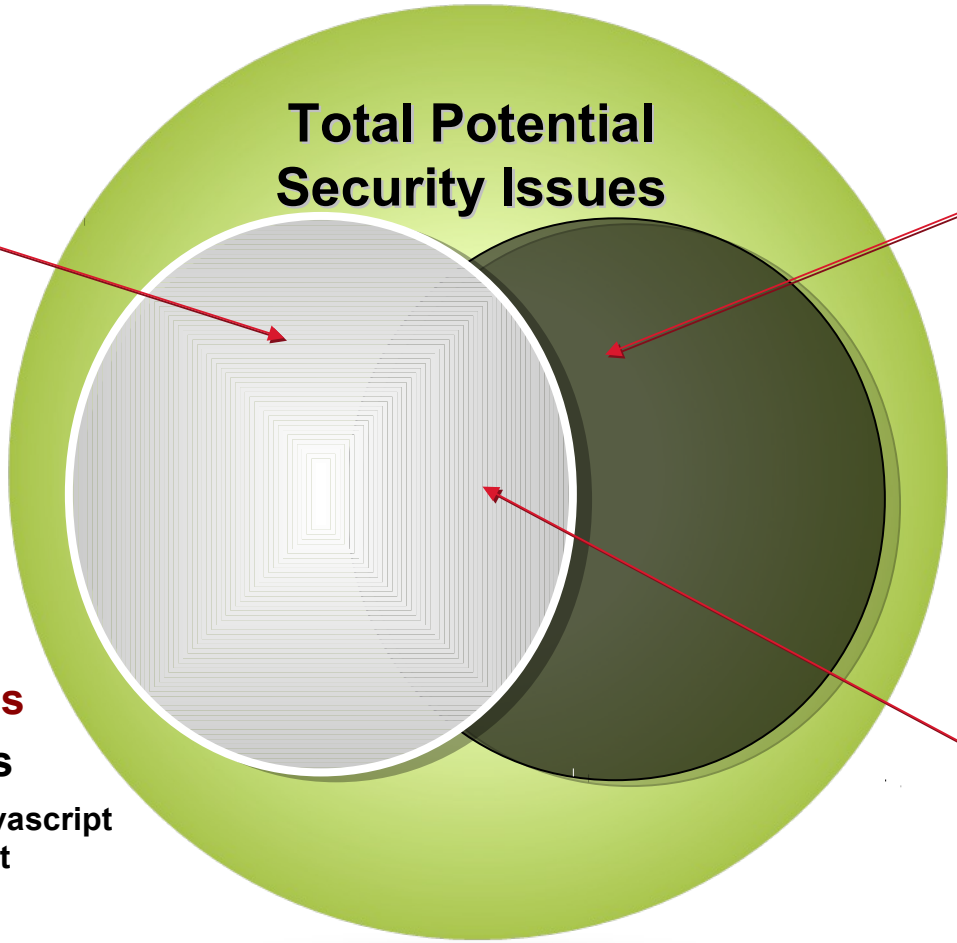
(identify issues)



Report

(detailed & actionable)

Find more vulnerabilities using the most advanced techniques



Static Analysis

- Analyze Source Code
- Use during development
- Uses Taint Analysis / Pattern Matching

Dynamic Analysis

- Analyze Live Web Application
- Use during testing
- Uses HTTP tampering

More adv. Techniques

Client-Side Analysis

- Analyze downloaded Javascript code which runs in client
- Unique in the industry

Run-Time Analysis

- Combines Dynamic Analysis with run-time agent
- More results, better accuracy

Hybrid Analysis

- Correlate Dynamic and Static results
- Assists remediation by identification of line of code

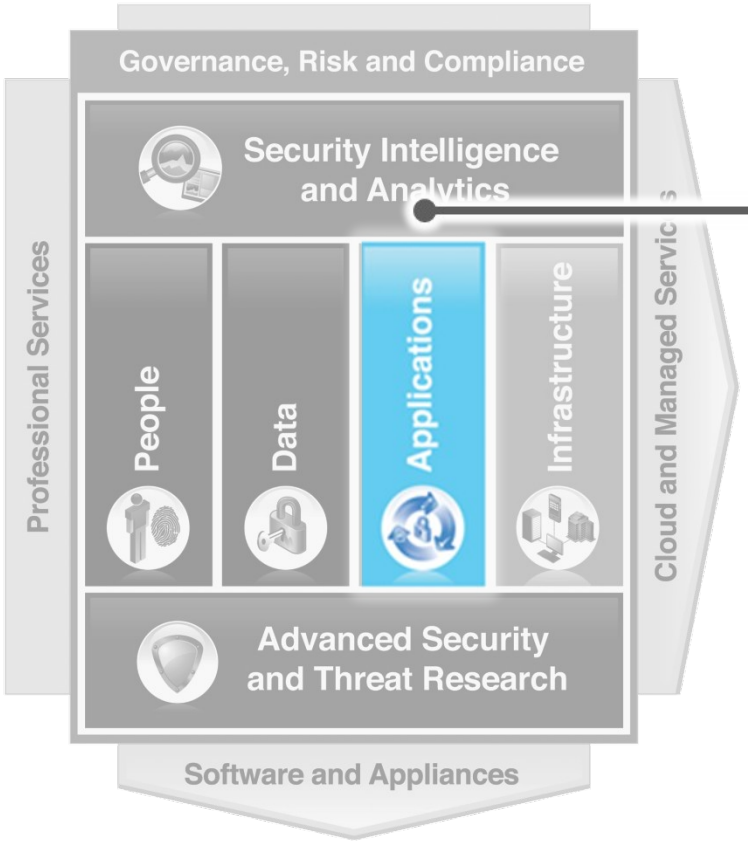
Agenda

- Why Application Security is important ?
- What is AppScan?
  - How AppScan works?
  - Dynamic Application Security Testing (DAST)
  - Static Application Security Testing (SAST)
- AppScan 8.6 Portfolio
- What's new in AppScan 8.6
  - AppScan Enterprise *(Formally known as IBM Rational AppScan Enterprise)*
  - AppScan Source *(Formally known as IBM Rational AppScan Source)*
- Where can I get help?

Portfolio Overview

Area of Focus

Reducing the costs of developing secure applications and assuring the privacy and integrity of trusted information



Portfolio Overview

AppScan Enterprise

- **Enterprise-class solution for implementing and managing an application security program, includes high-level dashboards, test policies, scan templates and issue management capabilities**
- **Multi-user solution providing simultaneous security scanning and centralized reporting**

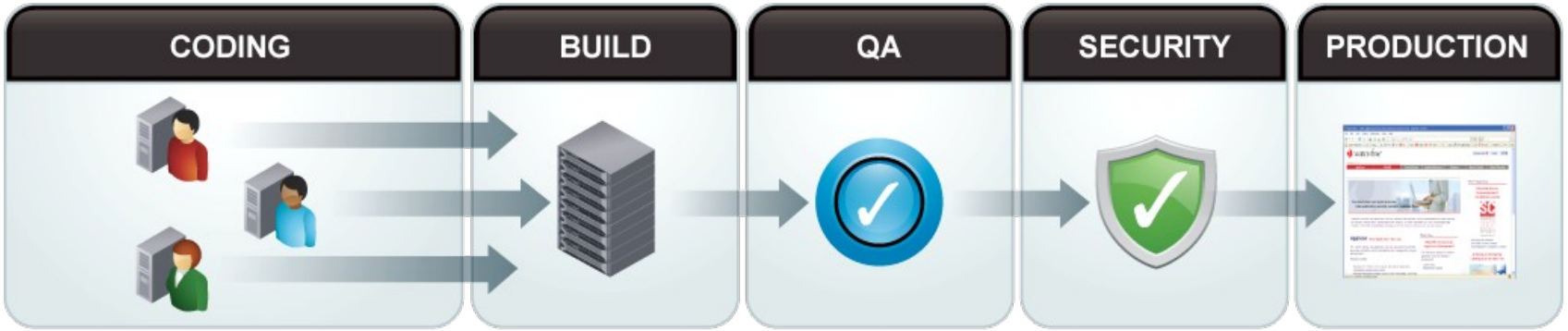
AppScan Standard

- **Desktop solution to Dynamic Application Security testing for IT Security, auditors, and penetration testers**

AppScan Source

- **Static application security testing to identify vulnerabilities at the line of code. Enables early detection within the development life cycle.**

AppScan: advanced security testing collaboration & governance through application lifecycle



Challenge to Share Test Results and Enable Self-Testing in the SDLC

AppScan Standard

AppScan Enterprise

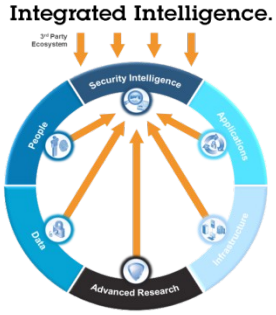
AppScan Source

Announcing AppScan 8.6 – Continuing IBM's history of innovation in application security

1

Extend your application security program to cover mobile applications

- New Static analysis of mobile applications
- Enhanced Dynamic analysis of server components



2

Expand your security intelligence with application vulnerability data

- With over 40% of known vulnerabilities in Applications, QRadar can now raise threat levels of incidents based on application vulnerabilities discovered by AppScan

3

Find more vulnerabilities easily and faster

- XSS analyzer reduces millions of tests to less than 20 by intelligent learning
- Static analysis speeds setup and facilitates a phased approach to test coverage

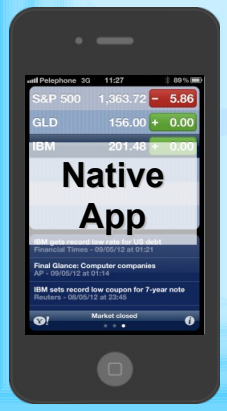
1 Extend: AppScan provides *a new level of support* for mobile application analysis

Mobile Web Apps

JavaScript / HTML5 hybrid analysis	✓ *IBM Innovation*

Server Side Logic

SAST (source code)	✓ *Foundational*
DAST (web interfaces)	✓ *Enhanced*

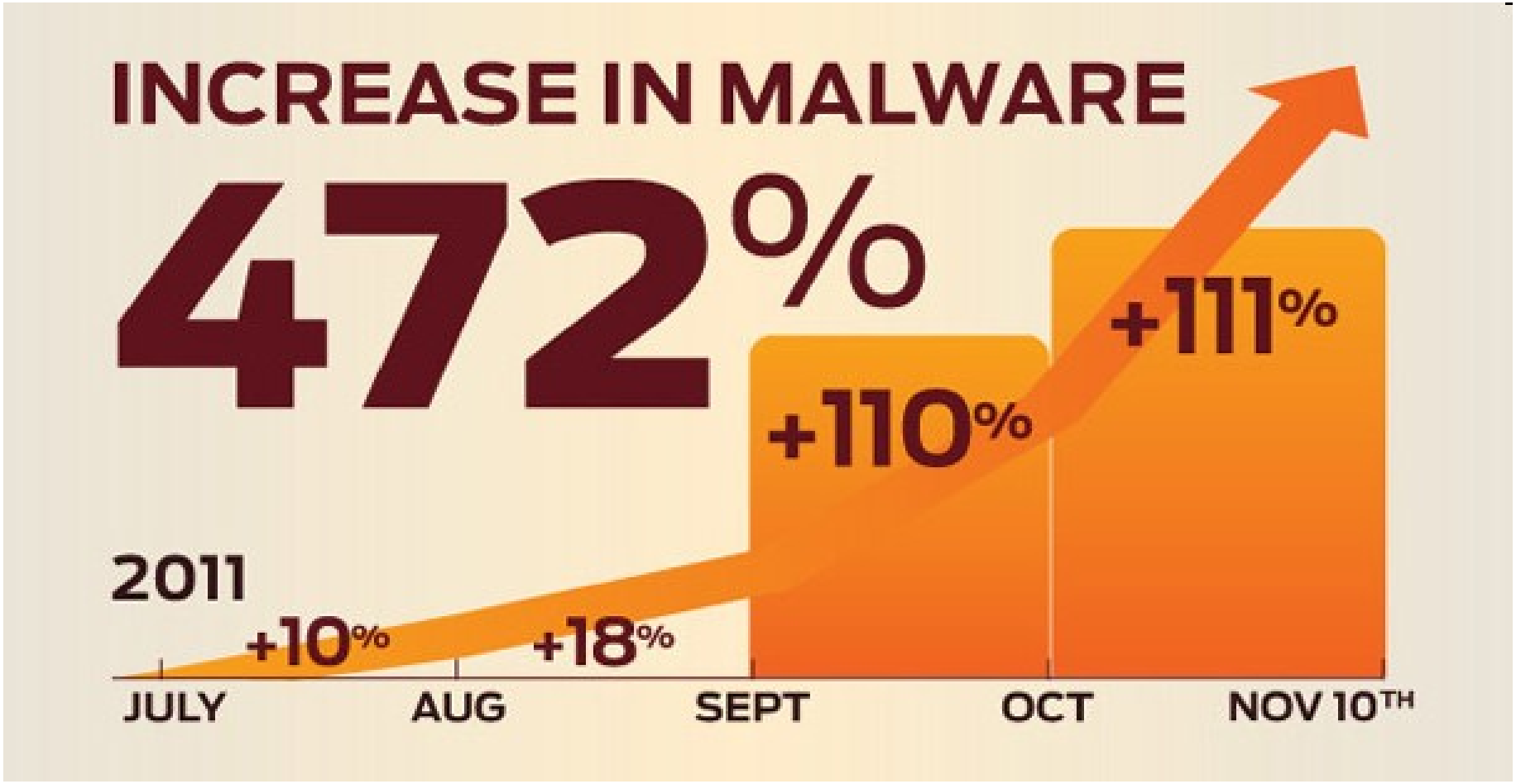


New in AppScan 8.6

Native Apps

Android applications	✓ *Static Analysis*

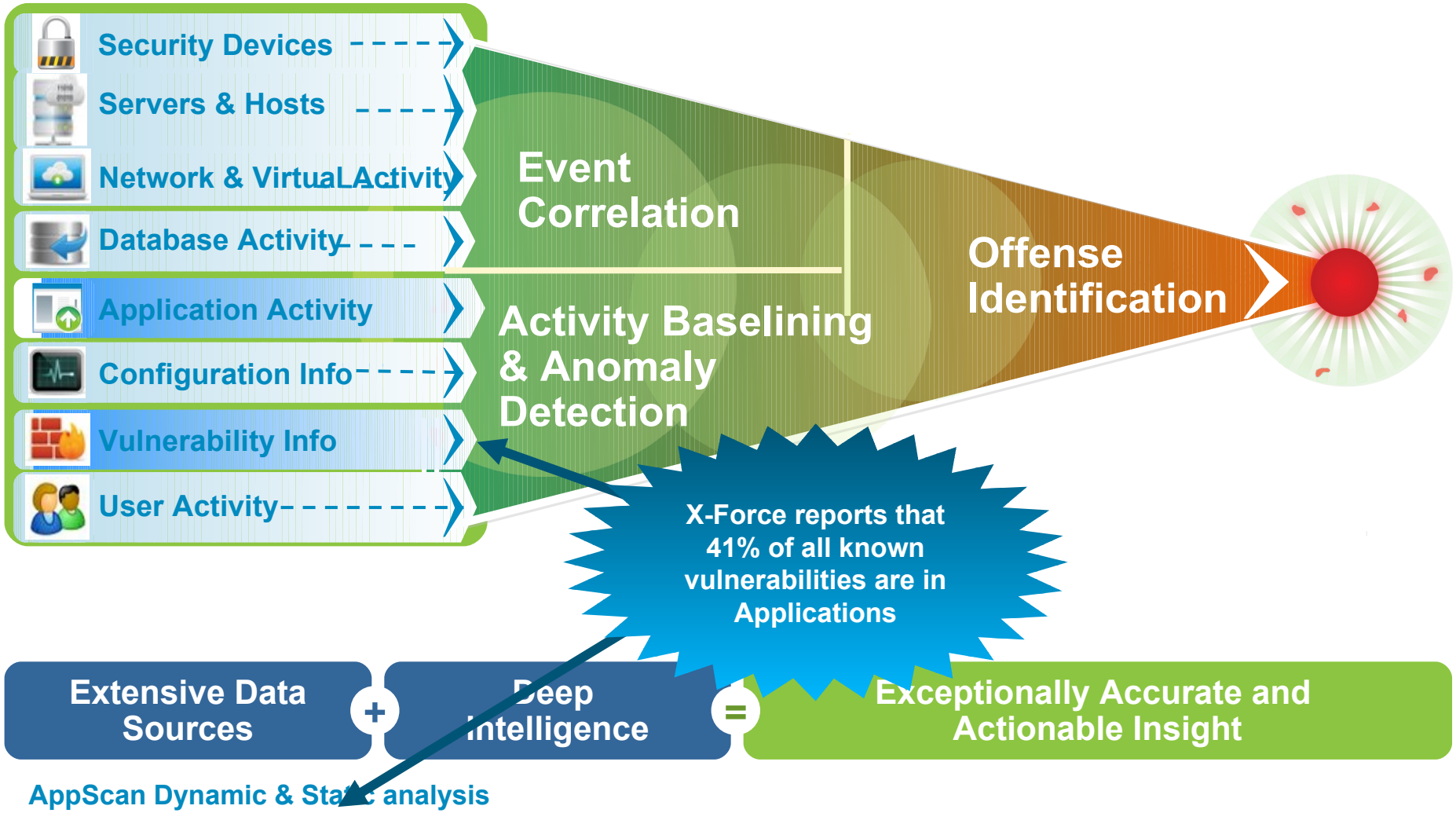
Why Android first?



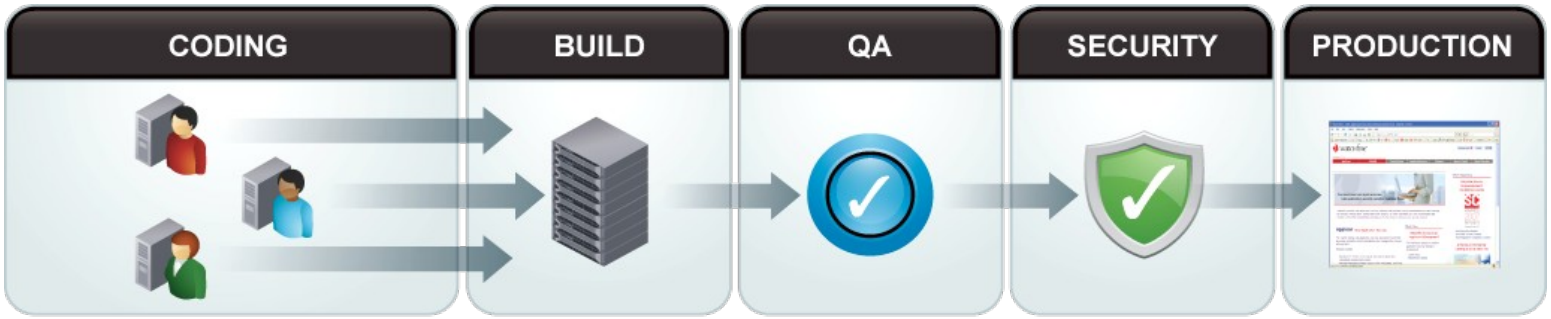
Source: Juniper Mobile Threat Report, 2/12

Android users take note: Researchers have found a whopping 472 percent increase in Android malware samples

2 Expand: AppScan integrates with QRadar to add application vulnerability data to your security intelligence



3 Find: Help find more vulnerabilities more easily in less time



Proactively address vulnerabilities early in the development process

Help improve time to value with *out-of-the-box* scan static analysis templates and *ease of use* features

- ❑ Auto Discovery Assistant helps automatically locate application source files
- ❑ Scan Assistant helps simplify setup with out-of-the-box scan templates

Help find more vulnerabilities with the *next generation Dynamic Analysis scanner* for the enterprise

- ❑ XSS Analyzer
- ❑ JSA in AppScan Enterprise
- ❑ Improved performance

Achieving Security Requires a Layered Approach
AppScan Integrates with QRadar and Network IPS