coverity

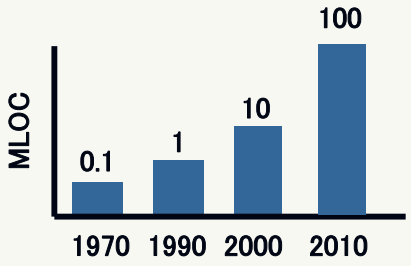
Detecting Critical Defects on the Developer's Desktop

Seth Hallem
CEO
Coverity, Inc.

Significant Challenge: High Quality Software

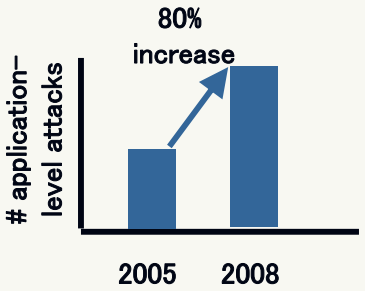
Code is increasingly complex	Code is increasing in size and complexity
The cost of Failure is high	A single defect or security vulnerability can have an enormous impact on the customer
Software bugs are costly	Bugs delay development efforts and impact new feature development

Exponential LOC growth in typical GM car



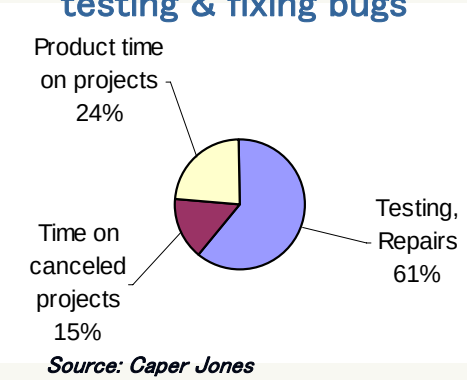
Source: Tony Scott CIO, GM

Application-level security attacks on the rise



Source: Gartner

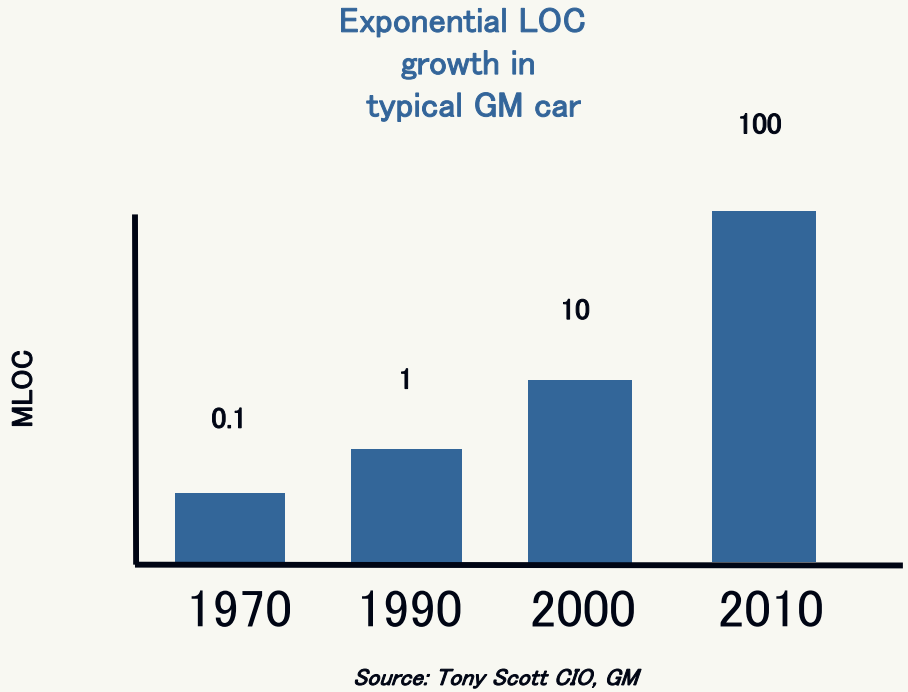
Developers spend significant time testing & fixing bugs



Source: Caper Jones

Software Complexity is Rising

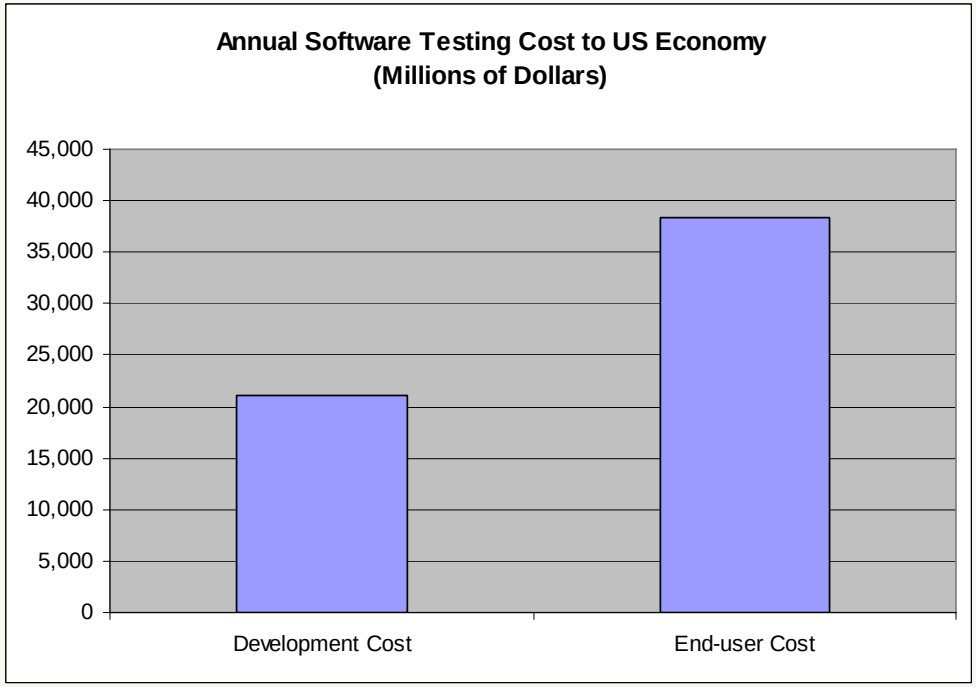
- By 2010, cars will have 100 million lines of code



Source: Tony Scott CIO, GM

Rising Cost

- The cost of inadequate software testing is rising
- In the United States:
  - The annual cost to software developers is over 22 billion dollars
  - The annual cost to end-users is over 35 billion dollars



NIST Planning Report 02-3. May, 2002.

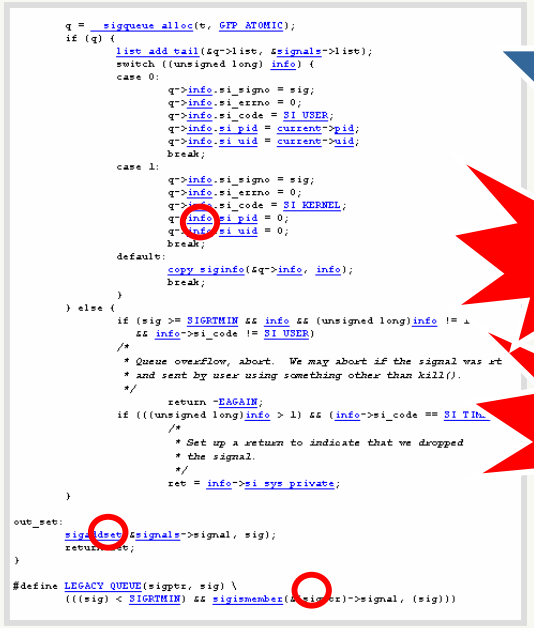
The Promise of Static Analysis Tools

coverity

Software Development Process

Design → Code → Integrate → QA → Release

Static Analysis



Bugs

Security Vulnerabilities

BENEFITS

Detects problems early in SDLC

No test cases required

Points to specific LOC

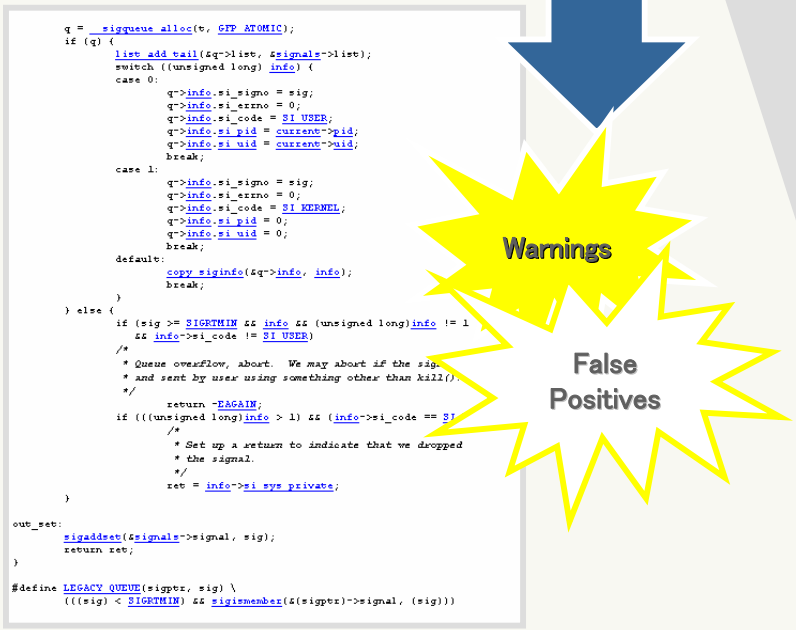
Systematic

Traditional Challenges in Static Analysis

Software Development Process

Design → Code → Integration → QA → Release

Static Analysis



Warnings

False Positives

TRADITIONAL FAILURES

High Cost Of Ownership

- Hard to integrate
- Significant configuration & tuning
- Does not scale

Poor Results

- Partial code path coverage
- Shallow analysis
- Uninteresting results
- Rife with False Positives

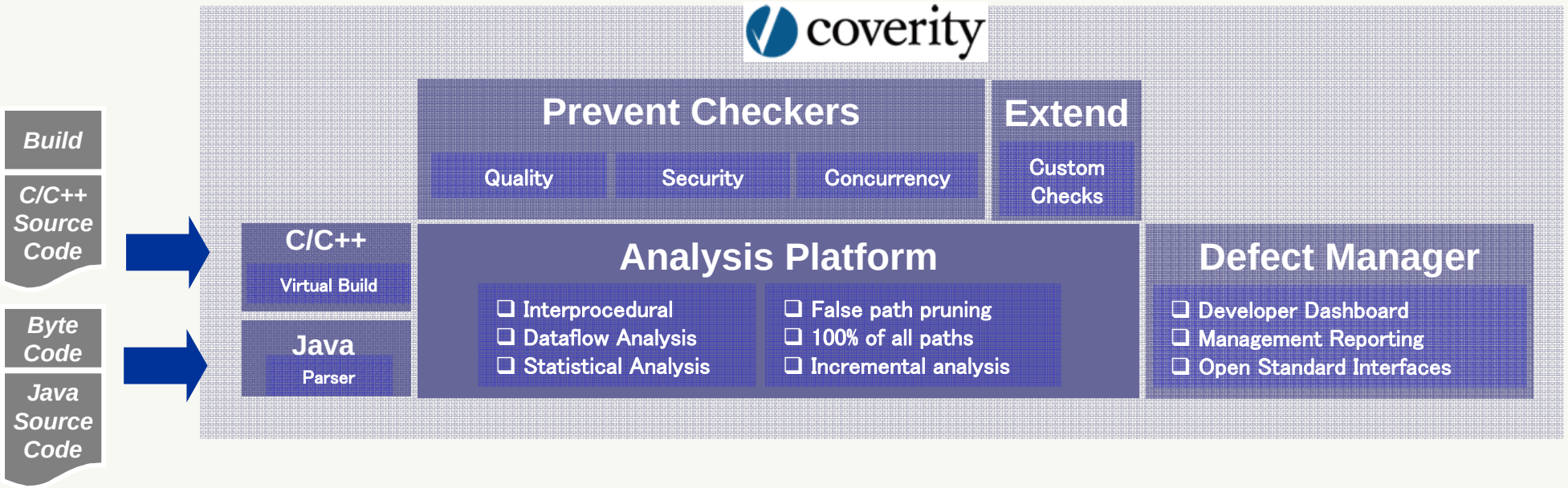
Coverity: Breakthrough Technology

coverity

Breakthrough Research
At Stanford University
Computer Systems Lab

Analysis Depth	• 100% of all code paths • Interprocedural analysis
Analysis Accuracy	• 20% false positive rate
Scalability	• Millions of lines of code

Coverity: Core Technologies



- Uses innovative source code analysis algorithms originating from compiler research
- Performs a whole program analysis
- Integrates easily into the software development process
- Integrated database application enables complete workflow and reporting

Coverity: Core Features

coverity

What defects can it find?

- Security Vulnerabilities
- System and Process Crashes
- Infinite Loops
- Performance Degradations
- Denial of Service
- Privilege Escalation
- Data, Memory and File Corruption
- Unpredictable Behavior
- Concurrency issues

How does it work?

- Do not run the code
- Zero test cases
- Runs at compile time

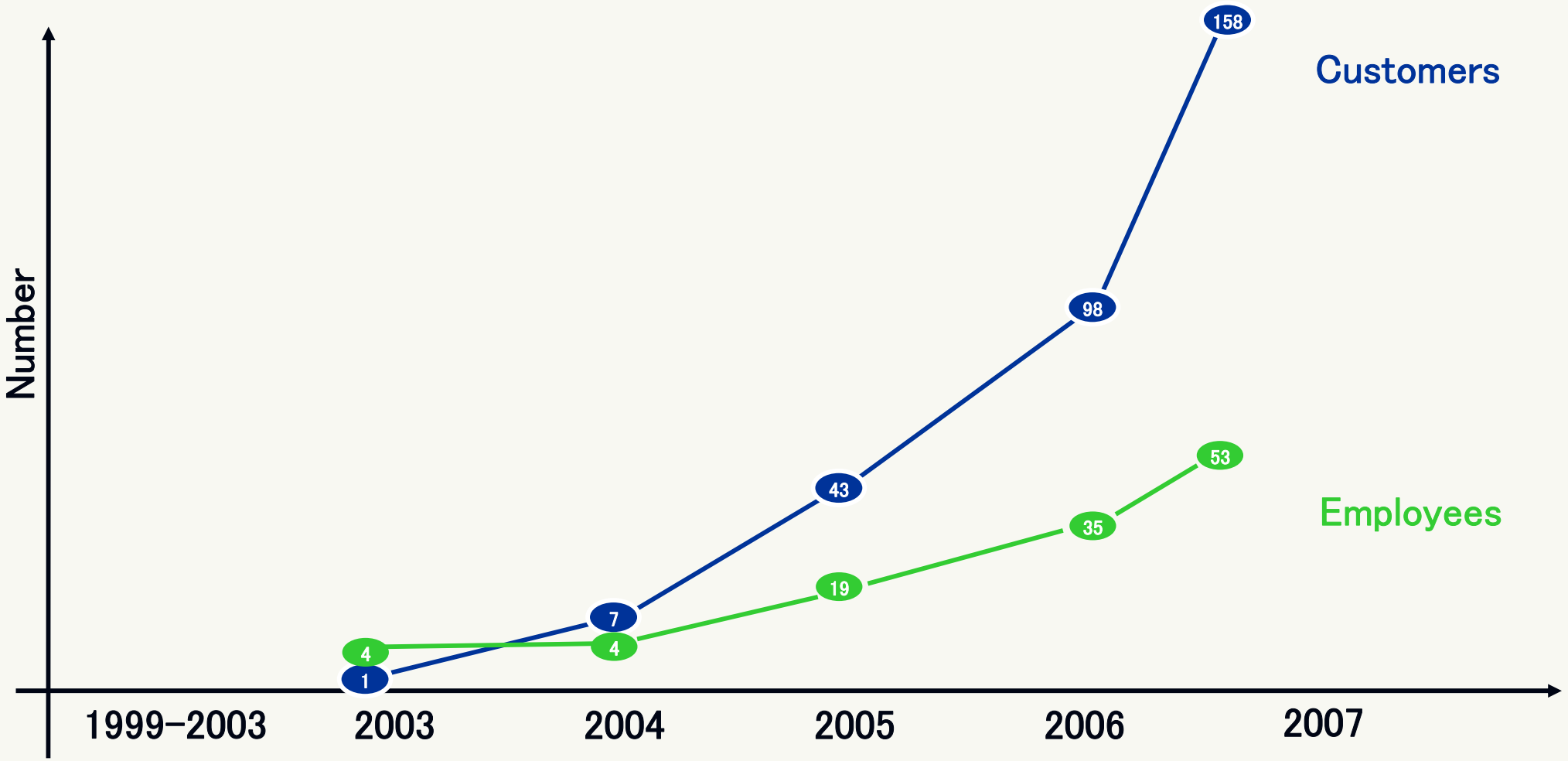
Coverity: Market Leader

coverity

Accuracy	Finds the most valuable flaws in your software
Integration	Minimal impact on the development process
False Positives	Avoids reporting costly noise
Likelihood of use	Built for developers to use and appreciate

Sample of Coverity Customers

Coverity History



coverity

Customer Success: Wall Street Journal

Tech Companies Check Software Earlier for Flaws

“Many companies, including RIM, are teaching programmers to write safer code and test their security as software is built, not afterward.”

Coverity Success: Wall Street Journal

Tech Companies Check Software Earlier for Flaws

By Yukari Iwatani Kane

WHEN BLACKBERRY maker Research in Motion Ltd. developed software in the past, its engineers worked quickly to meet deadlines, sometimes overlooking bugs that were caught later in the process. The result: Holes would crop up after a program had been built, it took extensive time and energy to trace its roots.

RIM wasn't alone. Many companies rushed to beat rivals with new software, and checking for bugs that could later be exploited by hackers was often seen as a waste of time. That has begun to change in the past few years as new laws force the disclosure of security holes and penalties, and companies increasingly instead with customers through the Web, a fruitful door for threats. Now many companies, including RIM, are teaching programmers to write safer code and test their security as software is built, not afterward.

Finding Holes

While the BlackBerry had relayed security vulnerability for security holes, Dave Little, a RIM security director, warned the company hadn't paid enough attention to the software that runs on the BlackBerry and other devices.

"The idea was that we could be doing more," says Mr. Little, who is based at RIM's Waterloo, Ont., headquarters. "We had to raise the bar."

Mr. Little soon discovered Coverity Inc., a San Francisco start-up that sells tools to automatically check for software flaws. Now Mr. Little uses Coverity every night to scan the code turned in by engineers. The tool sends Mr. Little an email listing potential red flags. He figures out which problems are real and tracks down each offending programmer, who has to fix the flaw before moving on. Mr. Little has also ramped up security training and requires programmers to double-check each other's code more regularly.

Software vulnerabilities throughout the industry have been on the rise. In February, for example, the U.S. Computer Emergency Readiness Team, a government organization, posted out a flaw in Apple Computer Inc.'s Safari Web browser that could allow a hacker to take control of a computer by persuading a user to view a specially crafted Web page. Overall, Symantec Corp., a Cupertino, Calif., maker of security software, found 2,156 vulnerabilities in software

Please Turn to Page B3, Column 1

THE WALL STREET JOURNAL.

"Many companies, including RIM, are

"Now, Mr. Little uses Coverity every night to scan the code turned in by engineers. The tool sends Mr. Little an email listing red flags."

– WSJ 05/04/06

Coverity Success: WIND RIVER

coverity

- Quality improvement is top priority designated by executive management
- Complex requirements for development tools:
  - Had to fit into the existing infrastructure
  - Had to fit into the Capability Maturity Model (CMM)
- According to WindRiver's Director of Engineering:
  - "We compared and evaluated a number of programming and error detection tools and Coverity was superior."

Coverity Success: WIND RIVER

coverity

- Ease of integration was critical
  - “integration with Coverity Prevent is seamless and the usage is straightforward. We went from trial to purchase in 3 weeks.”
- Coverity’s impact:
  - Immediate
    - “We found several important defects. It does validate the purchase of the tool.”
  - Ongoing
    - Development productivity up 30%
    - Time to market cut by 20%