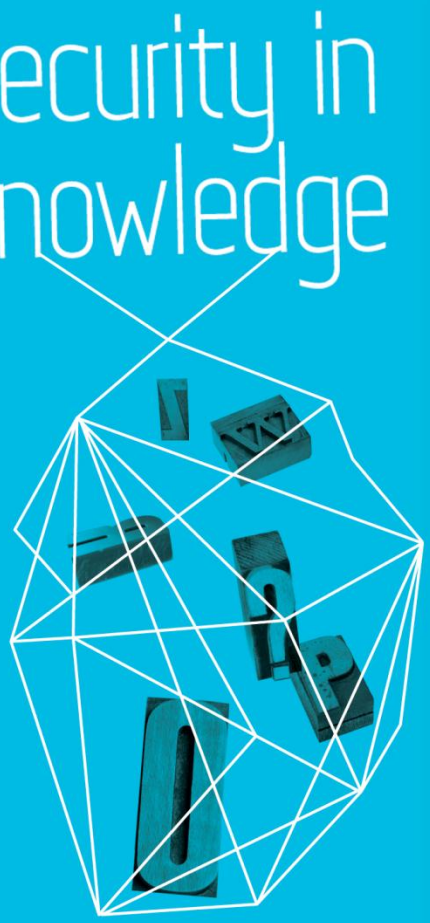
RSA CONFERENCE 2013

Who, What, Where, How: Five Big Questions in Mobile Security



Jacob West
Chief Technology Officer
HP Enterprise Security Products

Session ID: STU-R35A

Session Classification: Intermediate

Why is mobile security an imperative?

Who will be held accountable?

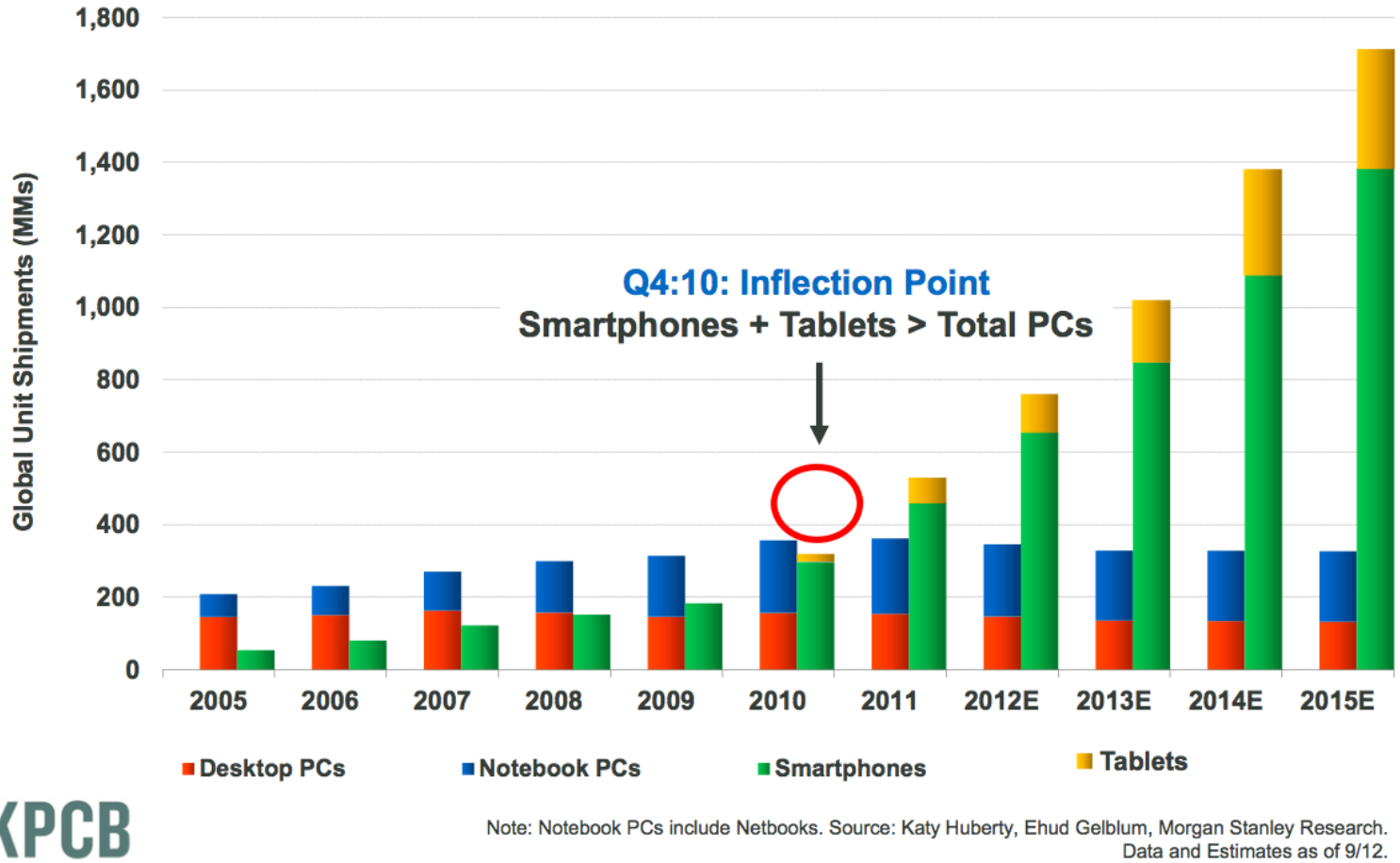
What platform strategy makes sense?

Where are mobile apps developed?

How do we build secure mobile apps?

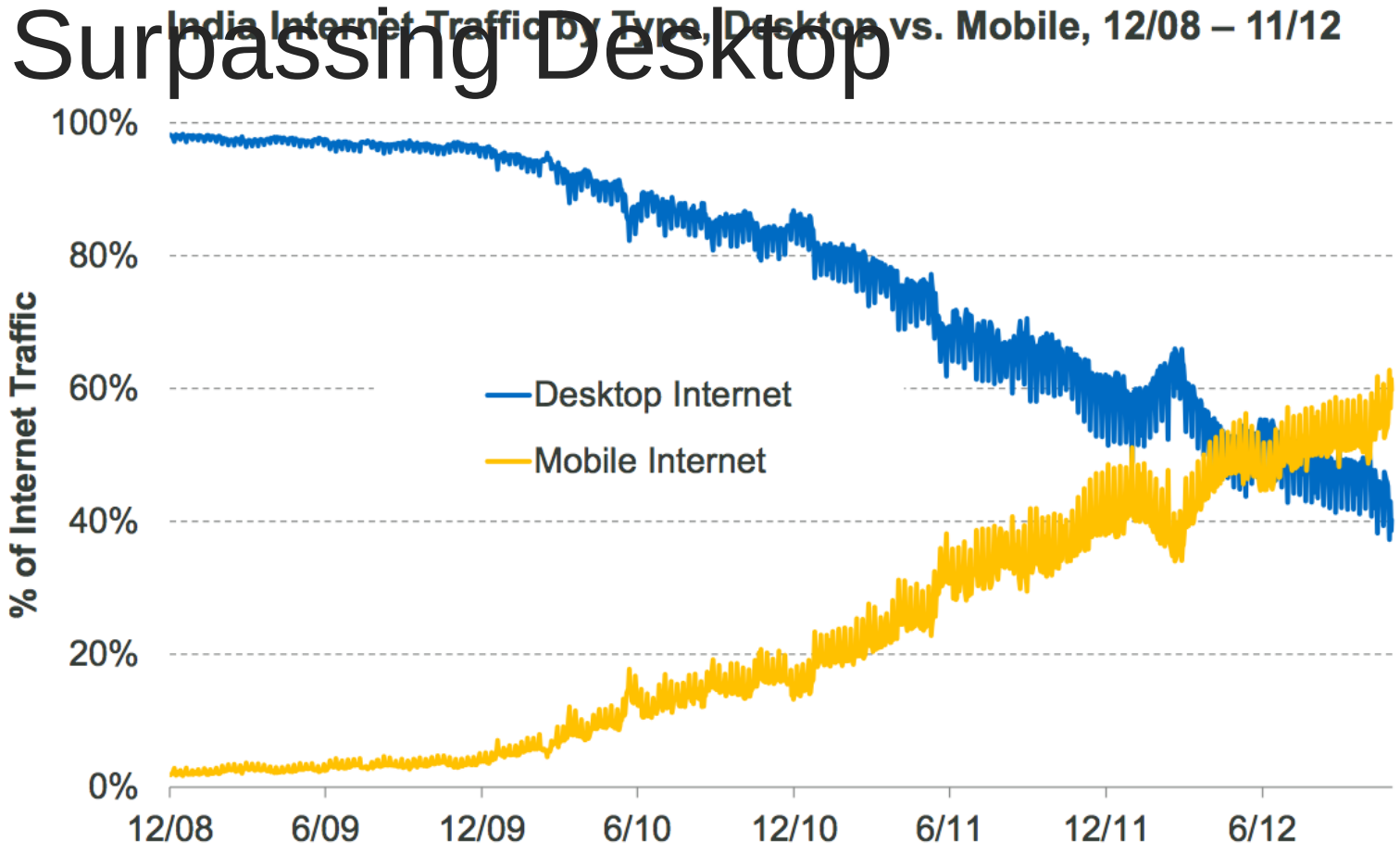
Why is mobile security an imperative?

Mobile Devices are Taking Over



12/12 KPCB Trend Report

Mobile Internet Usage Surpassing Desktop

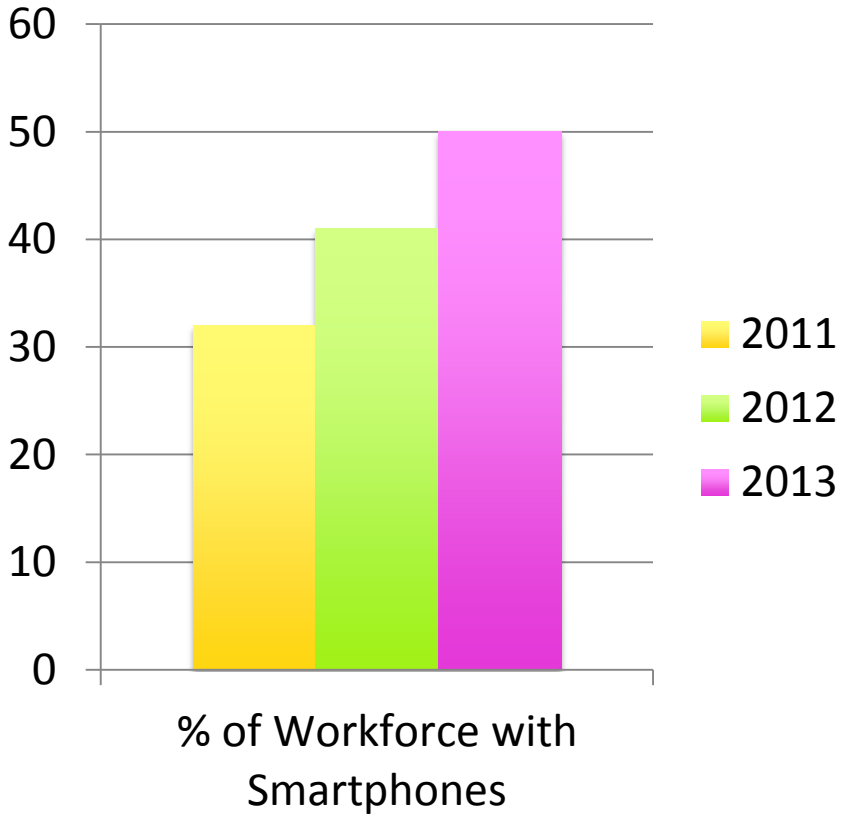


KPCB

12/12 KPCB Trend Report

Source: StatCounter Global Stats, 11/12

Not Just for Consumers



- By 2015, mobile dev projects targeting smartphones and tablets will outnumber native PC projects by a ratio of 4:1

  – Gartner 7/12

- By 2016, > 50 percent of enterprise email users will rely primarily web or mobile.

  – Gartner 12/11

Who will be held accountable?

What *is* Mobile?

device

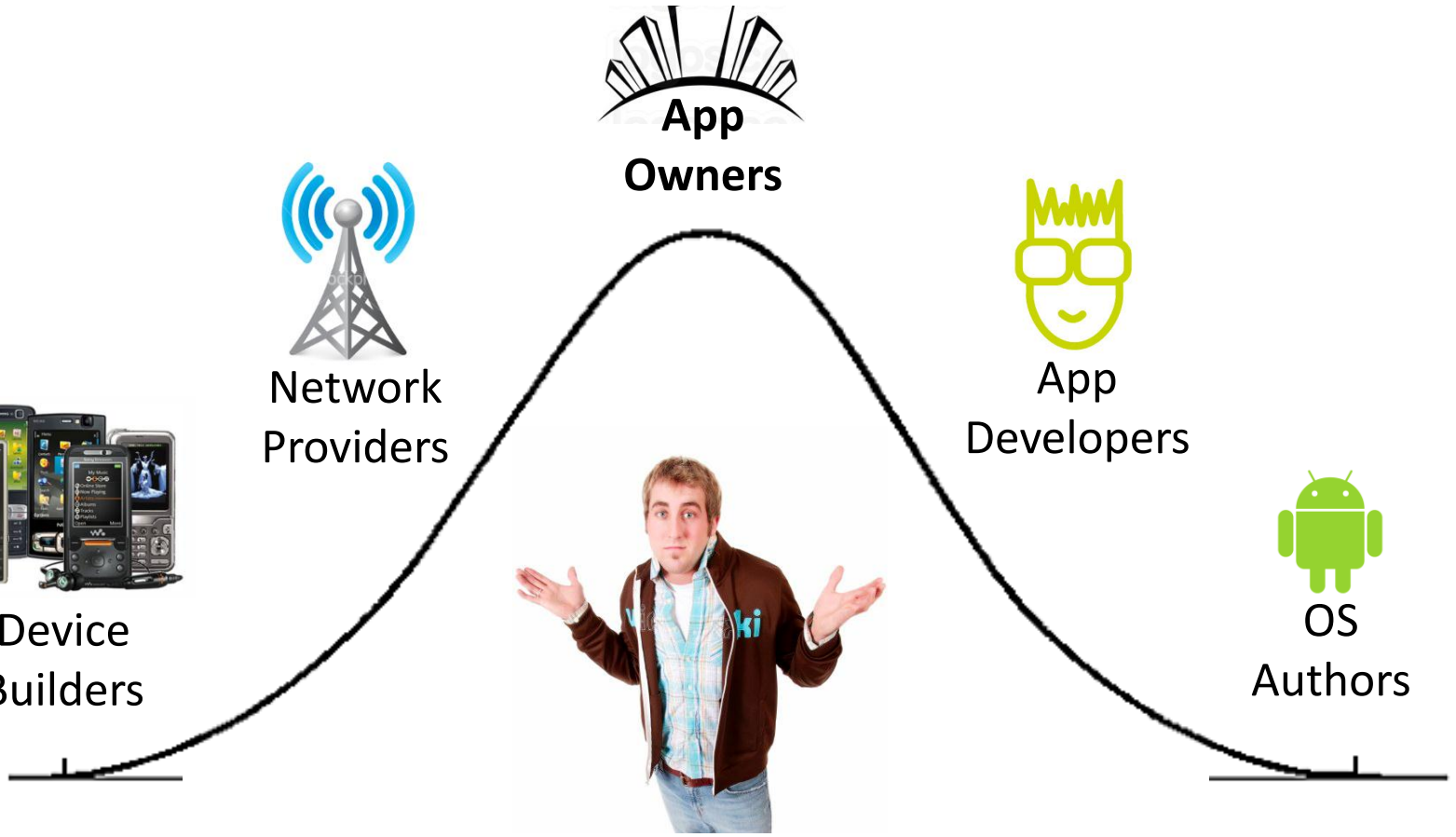
network

server

apps

os

Who Cares?



Who Will Users Hold Accountable?

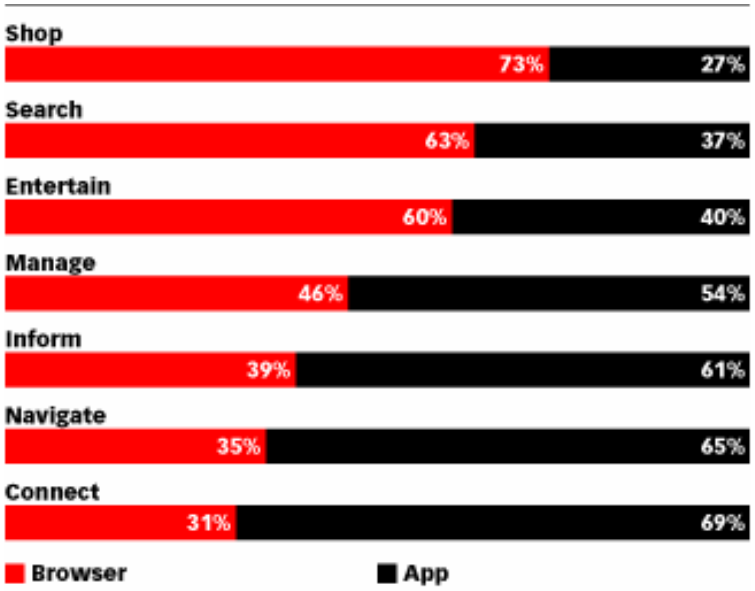
What platform strategy makes sense?

Platform Tradeoffs

- Web, native, hybrid
- Operating systems
- Developer support
- Application delivery
- Programming language

Web Versus Native

- Native mobile applications
  - Persistent
  - Hardware support
  - Flexible
- Mobile-optimized web apps
  - Lightweight
  - Multi-platform
  - Bolt onto legacy apps
- Hybrid?
  - Native container for web content
  - Cross-compiled native apps



80% by 2015
– Gartner 11/12

Application Delivery

- Open app store model (Google Marketplace)
  - Enterprise app stores
  - Security as a differentiator
  - Researcher access?
- Closed app store model (Apple App Store)
  - Controlled ecosystem
  - Revocation capability
  - Compromise: Apple's iOS Developer Enterprise Program

Native Programming Languages

- Objective-C
  - Little-known pre-iOS
  - ‘Unsafe’ language
  - Limited tool support
- Java
  - Widely-known
  - No more buffer overflows
  - Better tool support

Where are mobile apps developed?

Mobile Development

- In-house
- Traditional outsourcers
- Boutique firms

In-House Development

Pros

- Leverage investments
- Easier integration
- Control over full SDLC

Cons

- Must train resources
- Add-ons may add risk
- Hard to outsource security

Traditional Outsourcers

Pros

- Well-known expectations
- Expand on experience
- Control over SDLC

Cons

- Harder to find talent
- Add-ons may add risk
- Outsourcing security (but not accountability)

Boutique Firms

Pros

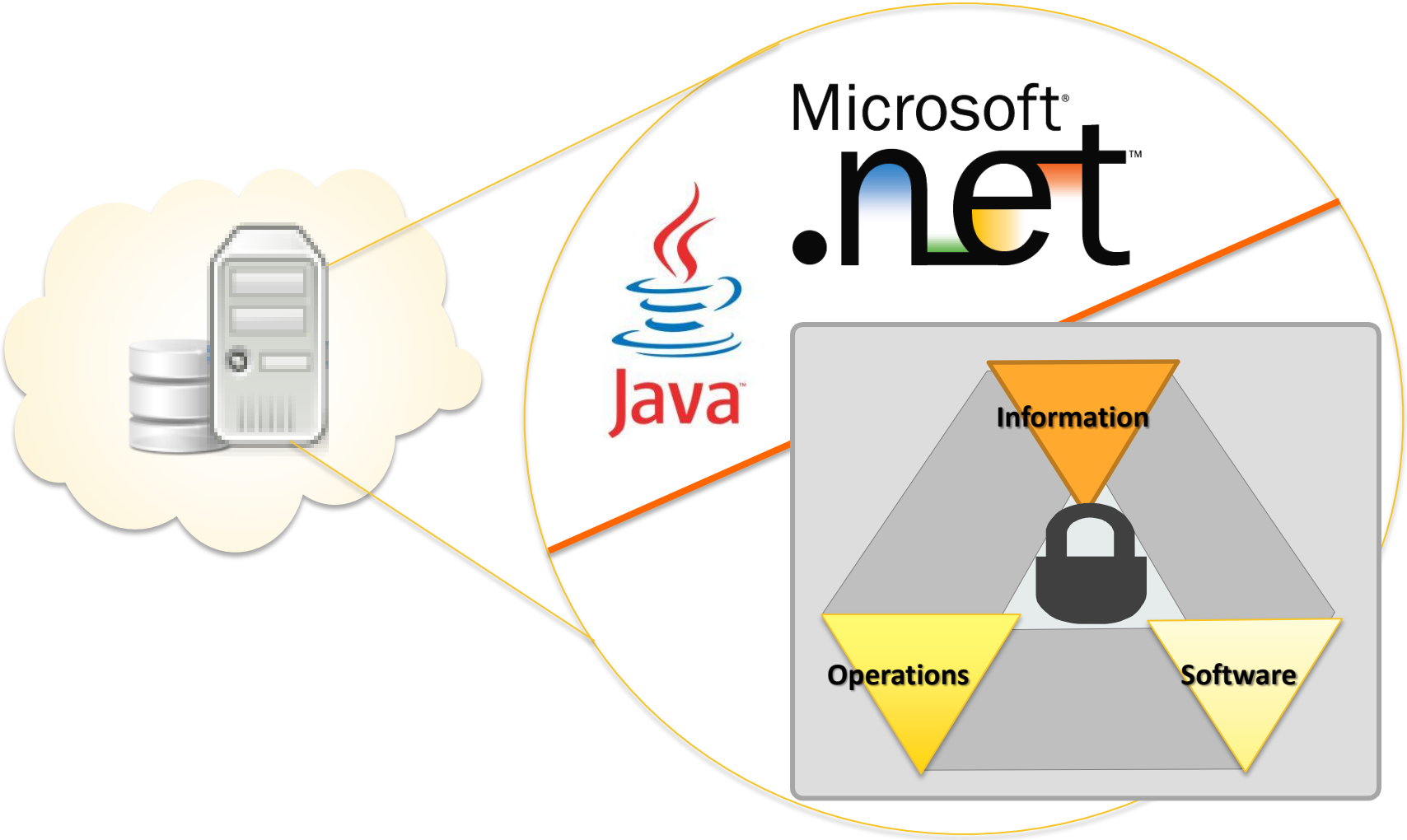
- Specialized talent
- Accelerated delivery
- Low-investment for high-quality result

Cons

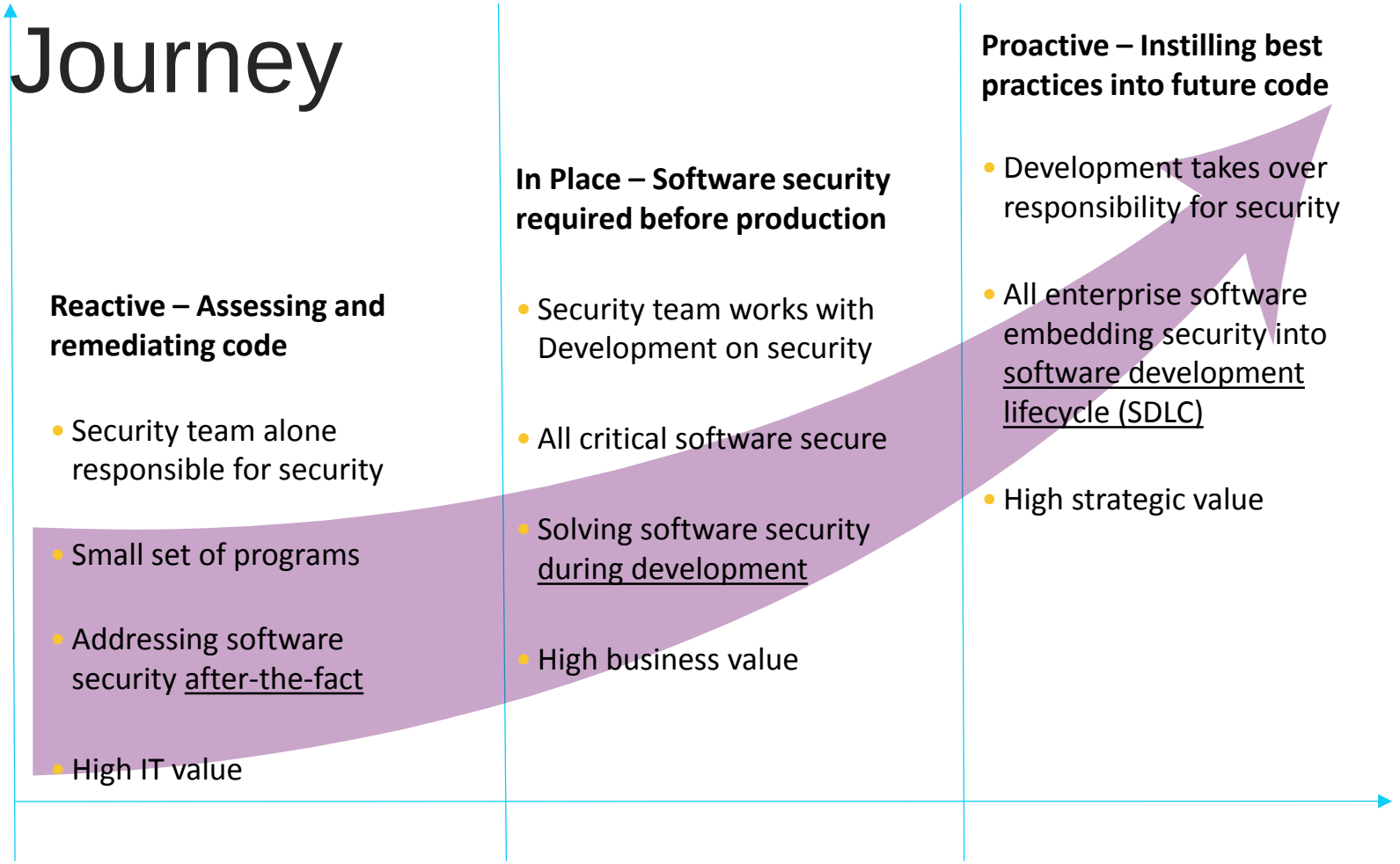
- Lack of security maturity
- Difficult integration
- Little influence over SDLC

How do we build secure mobile apps?

Same Ol' Server



Software Security Assurance Journey



Inspiration from the Industry: BSIMM4

- Real data from (51) real initiatives
- 95 measurements
- 13 repeat measurements
- McGraw, Migues, & West

www.bsimm.com

Parting Thoughts

More Questions to Ask

- What do your apps do and for whom?
- What platform(s) do your apps support and how?
- Who develops your apps and where?
- Is there an existing SDL for other development?
- Do you rely on platform providers or app distributors for any security assurance?
- Are mobile apps prompting back-end changes?