

# Case Study:

## Using App Security Ratings to Manage Application Risk

**Matt Moynahan**  
*CEO, Veracode*

**Donna Durkin**  
*CISO, ComputerShare*

**VERACODE**

## For Your Consideration

- Similarity between Software Vulnerabilities and the English Language
- The Undue Burden on Perimeter Defense (Zero Day Quagmire)
- From Credit Cards and SSN to Network Access and “I’m Not Sure What has Happened.”
- The Natural Progression of Asking Questions (opinion) to getting Answers (deterministic)
- What really is 3<sup>rd</sup> party code?
- The Ying and the Yang of Application Security Ratings
  - » Moving from “Trust but Verify” to “Trust Me, I’ll Show You”

# Undeniable Threat to Enterprises' Software Infrastructure

**95%**  
of all vulnerabilities  
are in software

**78%**  
of threats target  
business  
information

**75%**  
of attacks are at the  
application level

**62%**  
have experienced  
security breaches  
due to insecure software  
in the last 12 months



January 2010

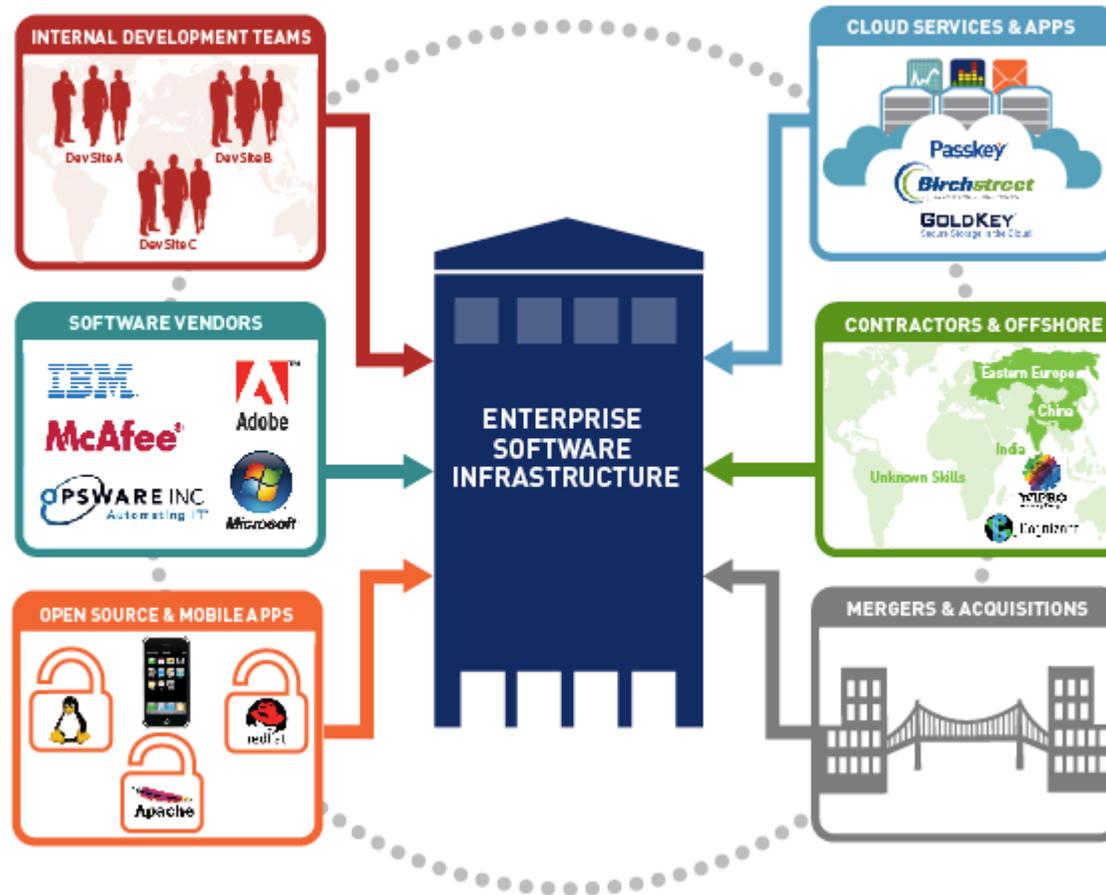
UNITED STATES SECURITIES AND EXCHANGE COMMISSION

Washington, D.C. 20549  
FORM 10-K



We regularly face attempts by others to gain unauthorized access through the Internet to our information technology systems by, for example, masquerading as authorized users or surreptitious introduction of **software**. These attempts, which might be the result of industrial or other espionage, or actions by hackers seeking to harm the company, its products, or end users, are sometimes successful. One recent and sophisticated incident occurred in January 2010 around the same time as the recently publicized security incident reported by **Google**.

# Enterprise Software Infrastructure Risk: Pick Your Favorite Software Target



# Third-party Applications Have Lowest Security Quality



Figure 3: Supplier Performance on First Submission (Adjusted for Business Criticality)

The significant presence of third-party applications identified as critical increases the importance of applying uniform application security verification policies across all supplier types.

Veracode sampling found as much as 76% of code submitted as Internally Developed was identifiably from third-parties, most often in the form of Open Source components and Commercial shared libraries and components. Furthermore, there was a "nesting effect" as third-party components themselves often contained other third-party components.

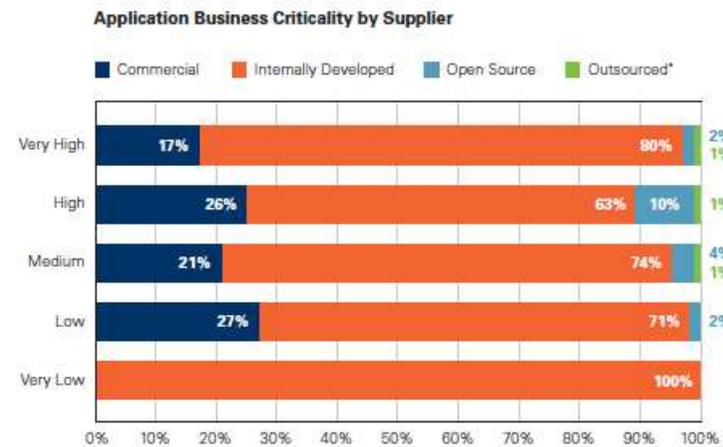


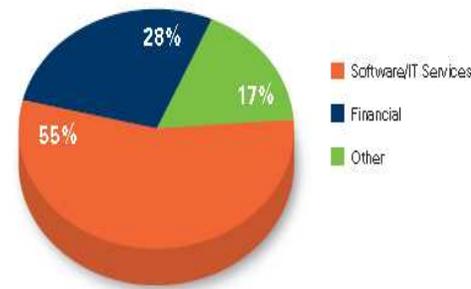
Figure 2: Application Business Criticality by Supplier  
(\* small sample size)

# Suppliers of Cloud/Web Apps Most Frequently Subjected to Third-party Risk Assessments

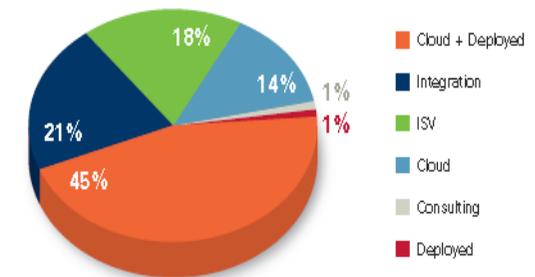
Companies are proactively requiring assessments of applications across a wide variety of internal applications (Operations and Finance) as well as external customer-facing web sites.

Three-quarters of all third-party assessments required less than 11 days to achieve acceptable levels of security quality.

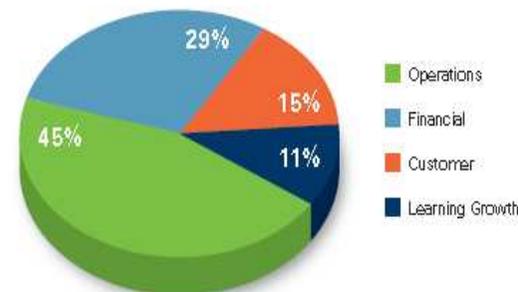
Requester Distribution by Industry



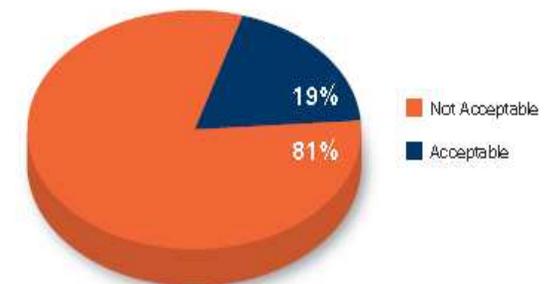
Reviewed Application Count by Vendor Type



Requested Third-party Assessments by Application Purpose



Third-party Assessments: Performance Upon Initial Submission

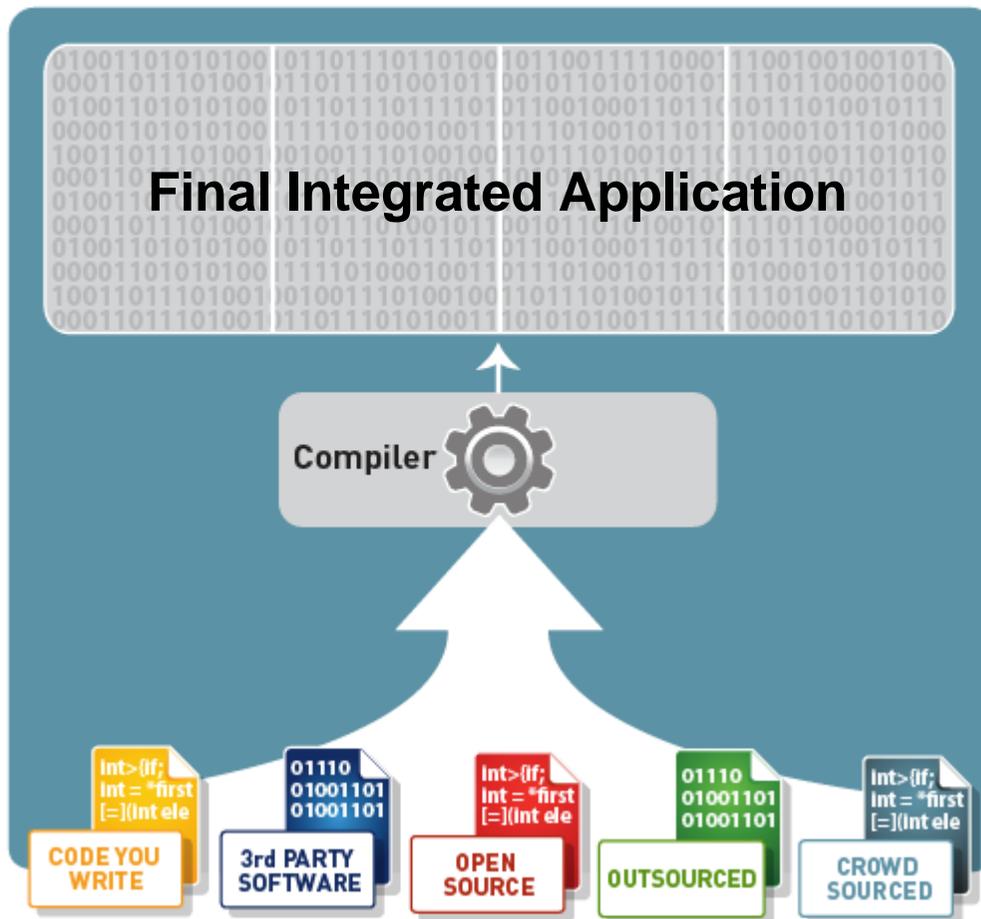


## 3<sup>rd</sup> Party “Security Risk Task” By Moving to Cloud

Cloud App Security Risk	Enterprise App Security Risk	Enterprise 3 <sup>rd</sup> Party Risk Tax!!
81%	54%	= 27%

\* Source: Veracode SOSS Volume 2. Calculated as difference in baseline security risk levels of application security quality upon first submission by type of application.

# Game Changing Service: Binary Scanning in Cloud



*“Only one vendor, Veracode, has an offering that can perform true binary analysis.”*  
**Gartner**

Binaries are the attack surface



Binaries include supply chain risk



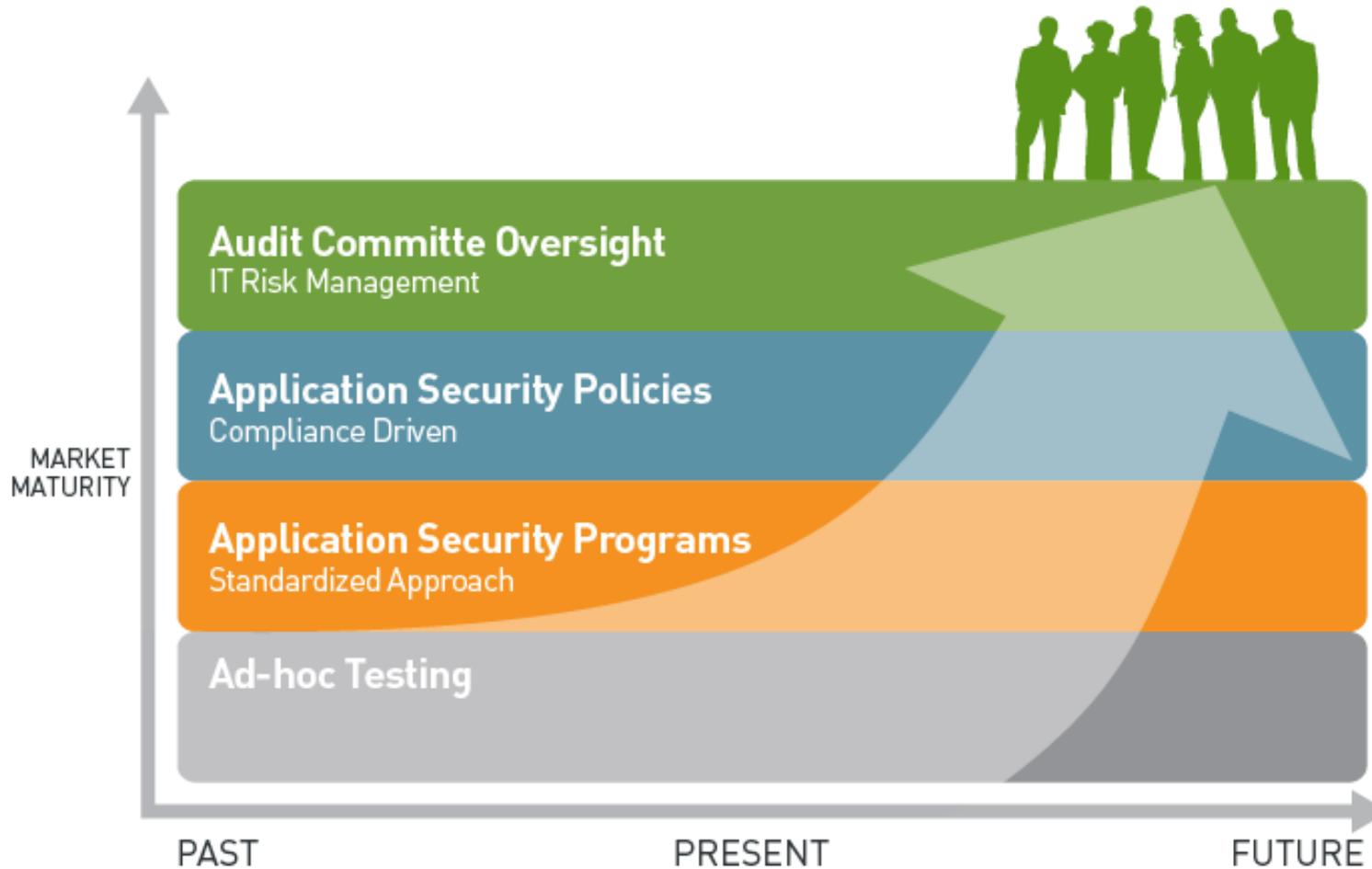
Binaries catch malicious code and backdoors



Binaries enable independent review



# Veracode Cloud Services Enable Firms to Move from Ad-hoc Testing to Technology Risk Management



## Progress is Being Made in 3<sup>rd</sup> Party Risk Management

- Growing public and private database of 3<sup>rd</sup> party ratings
- 50% of Veracode's enterprise customers are using 3<sup>rd</sup> party risk management solutions
- 300% growth quarter over quarter in 3<sup>rd</sup> party scans
- Record quarter in small ISV conversions to subscribing customers
- If you can find it accurately, developers can fix it quickly: less than 1.2 remediation scans required to meet compliance target
- Market leaders like Computershare are setting standards for internal and external quality benchmarking.

## Computershare

- Computershare is considered a world leader in share registration, employee equity plans, proxy solicitation and other specialized financial, governance and stakeholder communication services.
- Computershare provides services in 20 countries and manages over 30,000 Issuer clients and 120 million investor accounts.

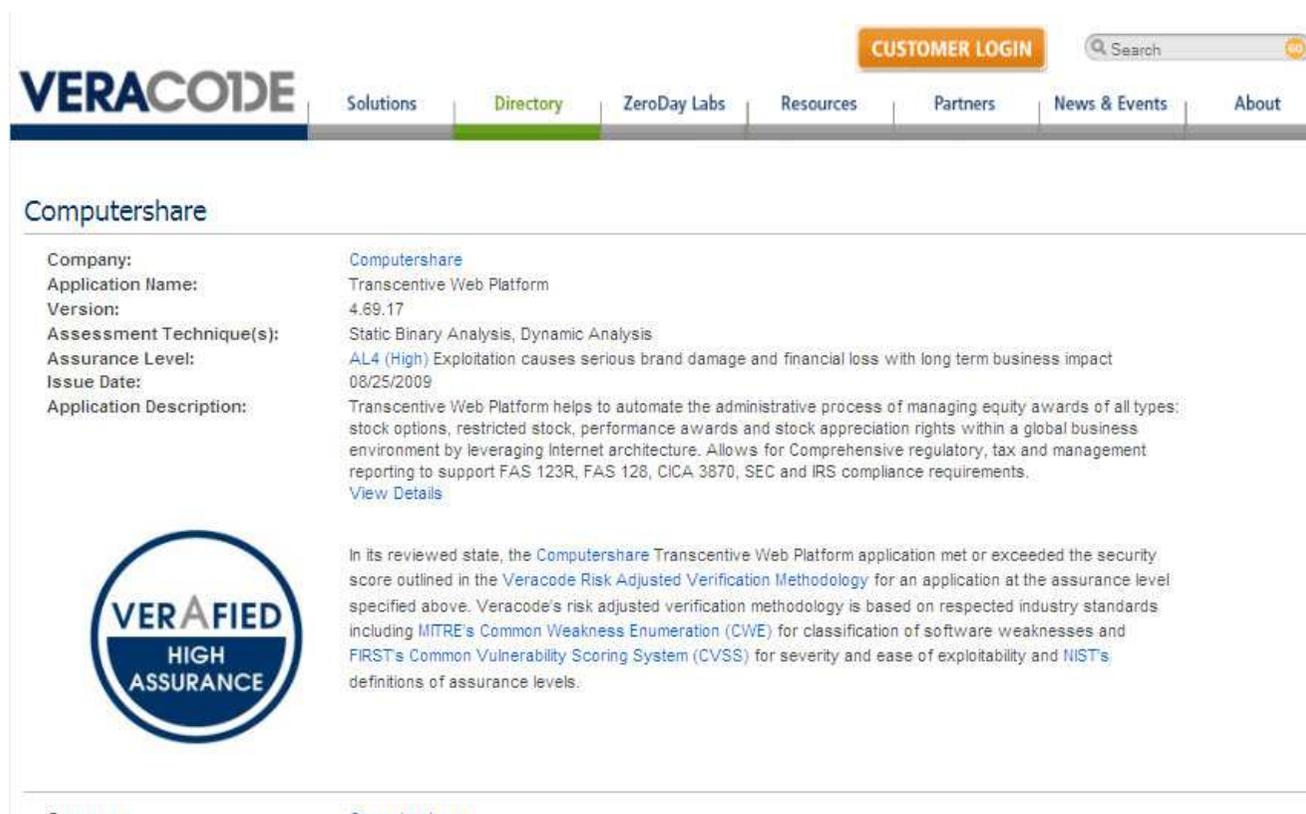


## Computershare – Our Application Security Drivers

- **Fraud, Privacy and Security** are converging very quickly
  - » “Closing the circle” is becoming crucial to understanding the total state of security and software assurance has become a major component in achieving this.
  
- **Need for Transparency in a Distributed Organization**
  - » Lack of visibility into multi-regional development processes with distributed development teams and differing SDLC approaches is always going to be a challenge.
  
- **Customer Confidence in Data Management**
  - » Value of getting scanned once to improve customer confidence in Computershare security posture as we manage personal and financial data.

# Computershare – Our Software Assurance Approach

- Approaching applications in terms of assurance levels.
- Implementation of eLearning Curriculum and developer education
  - » We're starting to see the benefits of Elearning through more secure coding and thus better ratings.



The screenshot displays the Veracode website's directory page for the Computershare Transcendive Web Platform. The page features a navigation bar with the Veracode logo and menu items: Solutions, Directory (highlighted), ZeroDay Labs, Resources, Partners, News & Events, and About. A search bar and a 'CUSTOMER LOGIN' button are also visible. The main content area is titled 'Computershare' and contains a table of application details:

Company:	Computershare
Application Name:	Transcendive Web Platform
Version:	4.69.17
Assessment Technique(s):	Static Binary Analysis, Dynamic Analysis
Assurance Level:	AL4 (High) Exploitation causes serious brand damage and financial loss with long term business impact
Issue Date:	08/25/2009
Application Description:	Transcendive Web Platform helps to automate the administrative process of managing equity awards of all types: stock options, restricted stock, performance awards and stock appreciation rights within a global business environment by leveraging Internet architecture. Allows for Comprehensive regulatory, tax and management reporting to support FAS 123R, FAS 126, CICA 3870, SEC and IRS compliance requirements. <a href="#">View Details</a>

Below the table, there is a circular 'VERIFIED HIGH ASSURANCE' badge and a paragraph of text:

In its reviewed state, the [Computershare Transcendive Web Platform](#) application met or exceeded the security score outlined in the [Veracode Risk Adjusted Verification Methodology](#) for an application at the assurance level specified above. Veracode's risk adjusted verification methodology is based on respected industry standards including MITRE's [Common Weakness Enumeration \(CWE\)](#) for classification of software weaknesses and FIRST's [Common Vulnerability Scoring System \(CVSS\)](#) for severity and ease of exploitability and NIST's definitions of assurance levels.

## Benefits of Implementing an Application Security Policy

- Coverage of more apps and just broader coverage
- Greater confidence in the software acquired and distributed
- Higher security quality code and higher security conscious development organization
- Greater alignment of security with development organizations



# Stakeholders: How Do Interested Parties Mitigate The Risk?

Recognize security verification as critical customer requirement and competitive differentiator



Drives best economic value while minimizing risk for organization

Recognize third-party risk as real and develop collaborative approach

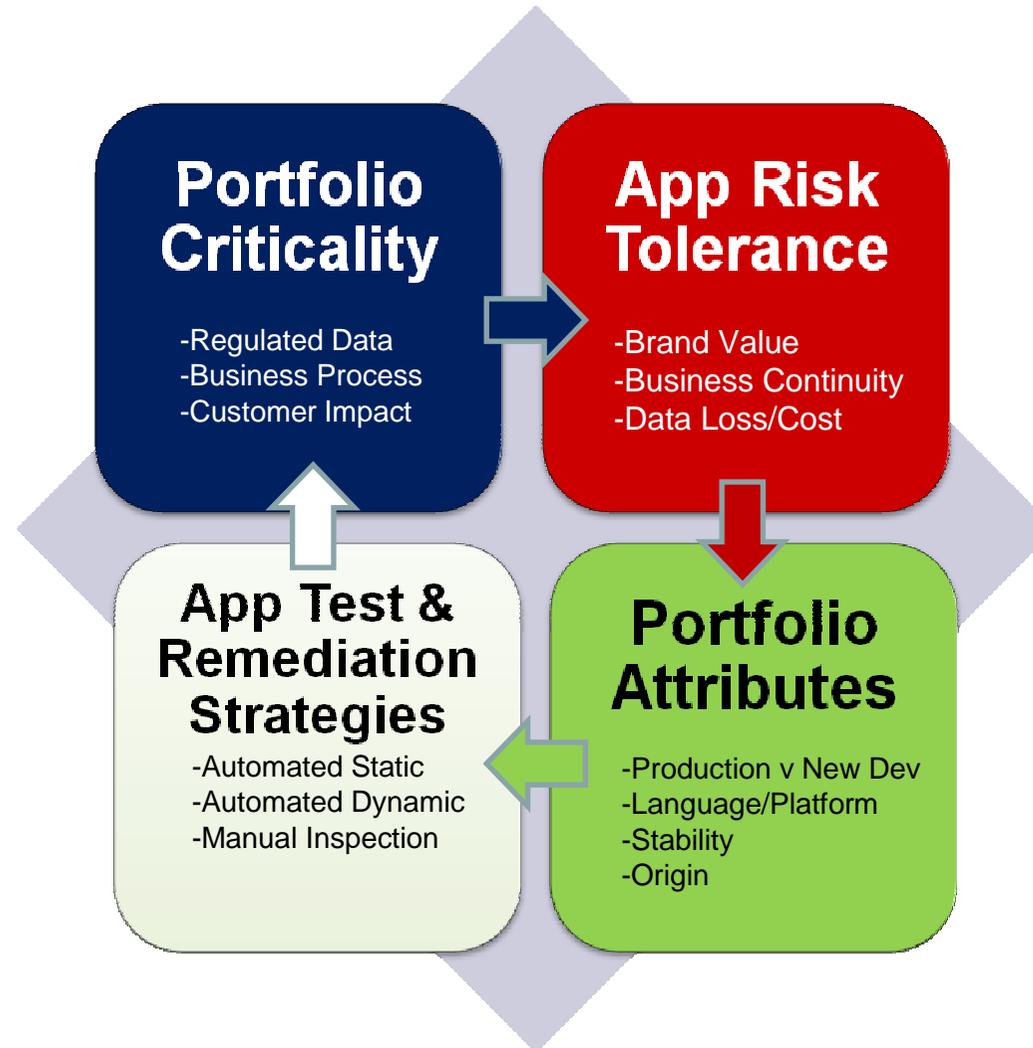
Facilitate multi-party transaction in a transparent way while respecting IP ownership

Thank you!

**Matthew Moynahan, CEO**  
mmoynahan@veracode.com

**VERACODE**

# Flexible, Risk-Based Application Security Policies and Remediation Guidance



# Best Practice: Embed Security Acceptance Testing into Contracts

- Software contracts typically focus on features, functions, maintenance and delivery timeframes
- Enterprises can embed security language into contracts
  - » New purchases or maintenance renewals are optimal times to introduce security
- Security testing is not functional testing, the contract should specify:
  - » Specific security measures (for example, static analysis dynamic testing, penetration testing)
  - » Testing process (independent, standards-based)
  - » Acceptance thresholds
  - » Vulnerability correction rules

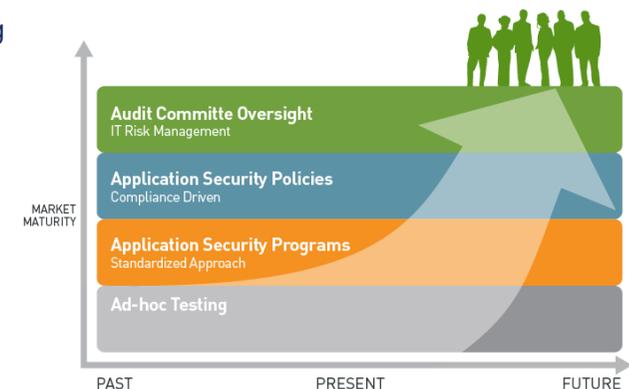


## Gartner Analyst Neil MacDonald Jan 2010

.....ensure that any code we produce **or procure** is more secure right from the beginning. Many of the clients I talk with are highly focused on the 'produce' part.....**What about the 'procure' part?**

# Process Changes Climbing the AppSec Maturity Stack

- **Governance, Risk, and Compliance Based (Audit Committee)**
  - » Enterprise risk-adjusted polices for all software (MATURITY SLIDE)
  - » Enforced by audit committee, CFO/CIO accountable, CISO managed, SOP in Purchasing, M&A, and Development processes
  - » Automated, real-time, enterprise application security intelligence
- **Policy Based**
  - » Line of business driven risk-adjusted policies for all software (MATURITY SLIDE...)
  - » Enforced by LOB CIO/CFO, LOB CISO accountable, SOP in Purchasing, M&A, and Development processes
  - » Automated, real-time, LOB application risk management
- **Systematic**
  - » Program-specific application security testing as part of software development and/or software acquisition processes.
  - » Enforced by CISO, Department (Purchasing, M&A, Development team) accountability
  - » Increasingly automated SDLC and 3<sup>rd</sup> Party application security testing
- **Ad hoc**
  - » Project-specific application security testing mandated by security team
  - » Enforced by Security professional, Development team accountability
  - » Semi-Automated or Consultant-dependent SDLC and 3<sup>rd</sup> Party application security testing



## Finding Reason Ground – Remediation Policy

App Type/Deployment				