

Application Security Use Case: Securing the Supply Chain to Manage Technology Risk

Matt Moynahan
CEO, Veracode

VERACODE

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

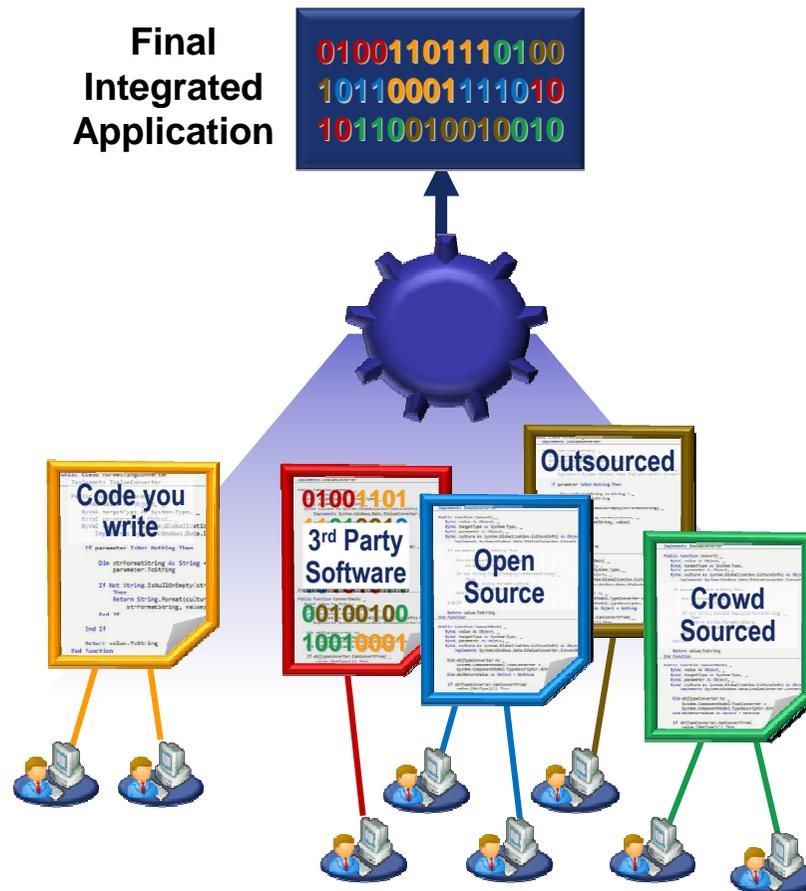
UNITED STATES SECURITIES AND EXCHANGE COMMISSION

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**.

Keys to Addressing the Challenge



- Analyze the Attack Surface
 - » Because you don't have or can't get the source code
 - » It is what represents the real application
- Leverage scalable delivery models (e.g. cloud-based testing)
- Technology alone doesn't solve the problem – involve the right people within the right framework

Stakeholders: How Do Interested Parties Mitigate The Risk?

Recognize security verification as critical customer requirement and competitive differentiator

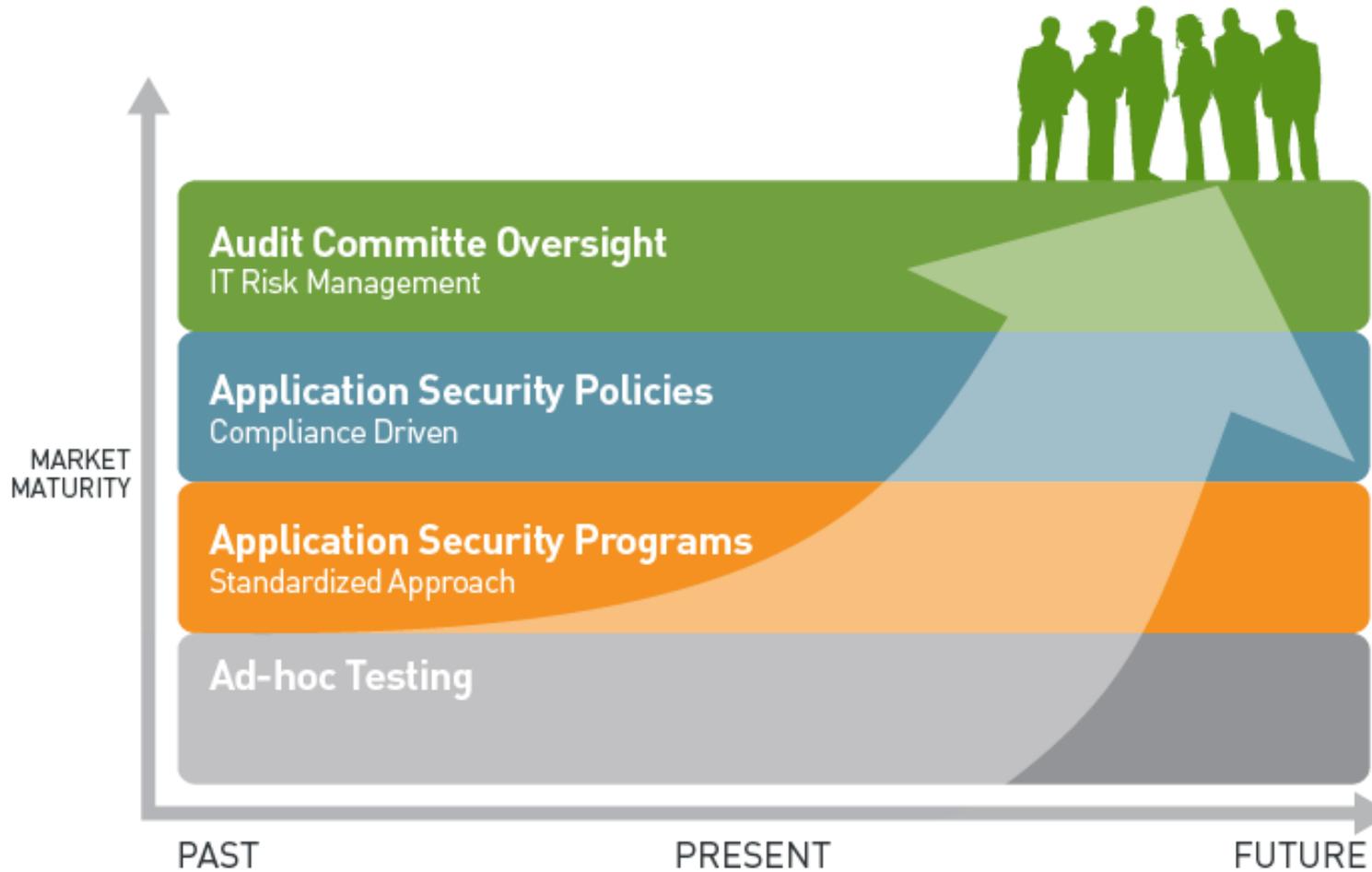


Drives best economic value while minimizing risk for organization

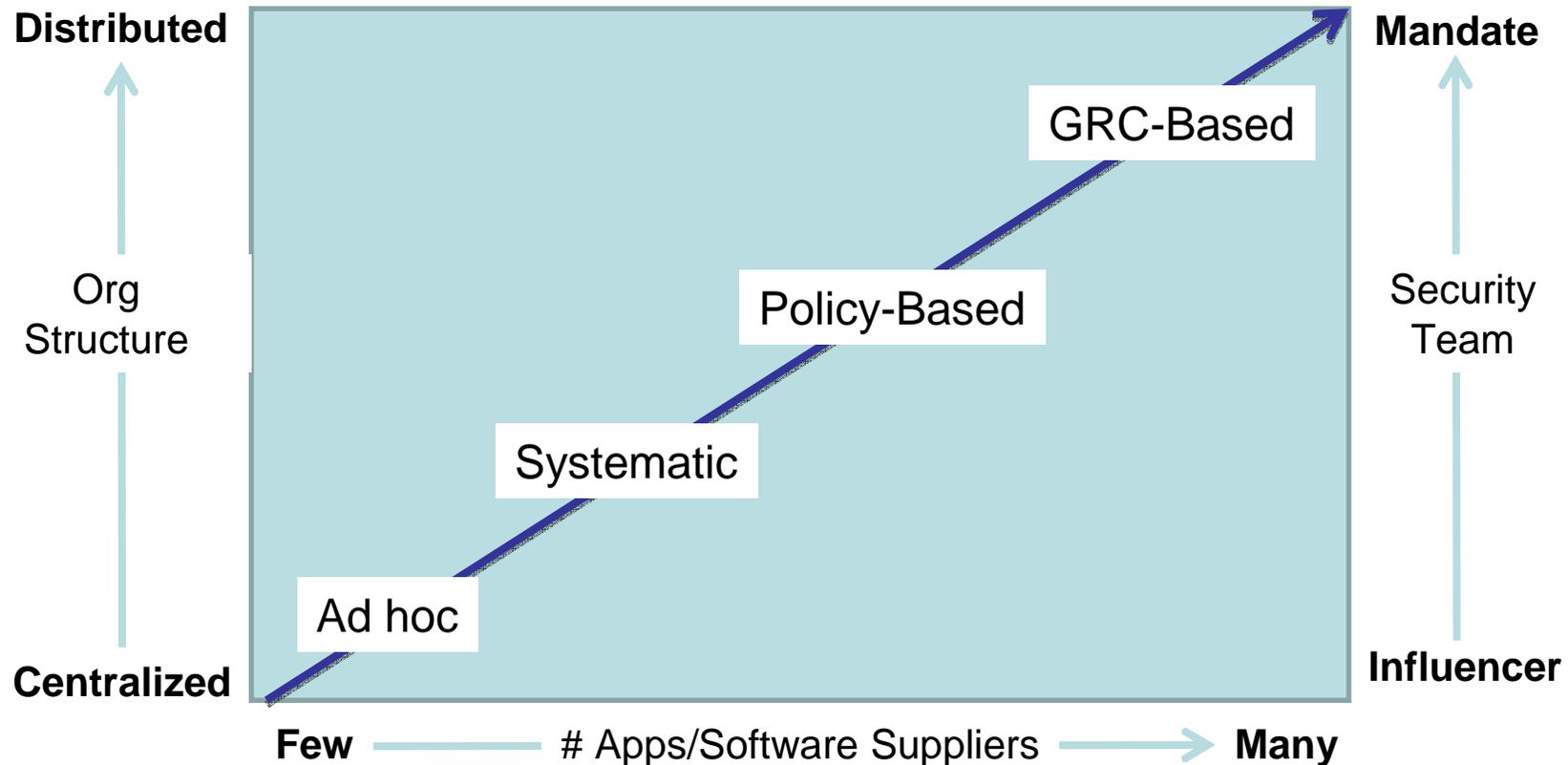
Recognize third-party risk as real and develop collaborative approach

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

Ad-hoc Testing to Technology Risk Management



Implementing ARM: The Challenge within Enterprise Environments



Application Policy in Practice

- European Bank
 - Very low risk tolerance for strategic application developed by offshore vendor
 - Policy was set for AA rating static/dynamic and ALL backdoor flaws had to be removed for have mitigating comments
- Fortune 100 Financial Firm
 - Low risk tolerance for up to 100 external sites created/hosted by 3rd parties
 - Policy was set to hit AA rating and PCI compliance by completing first tests in a 3 month window and then one month to comply with policy
- Fortune 100 Insurance Firm
 - Clearly set risk levels with many testing assets for 500+ applications
 - IT leadership launched Application Security Policy and timeframe to comply. Provided tools and lead time to empower development teams

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

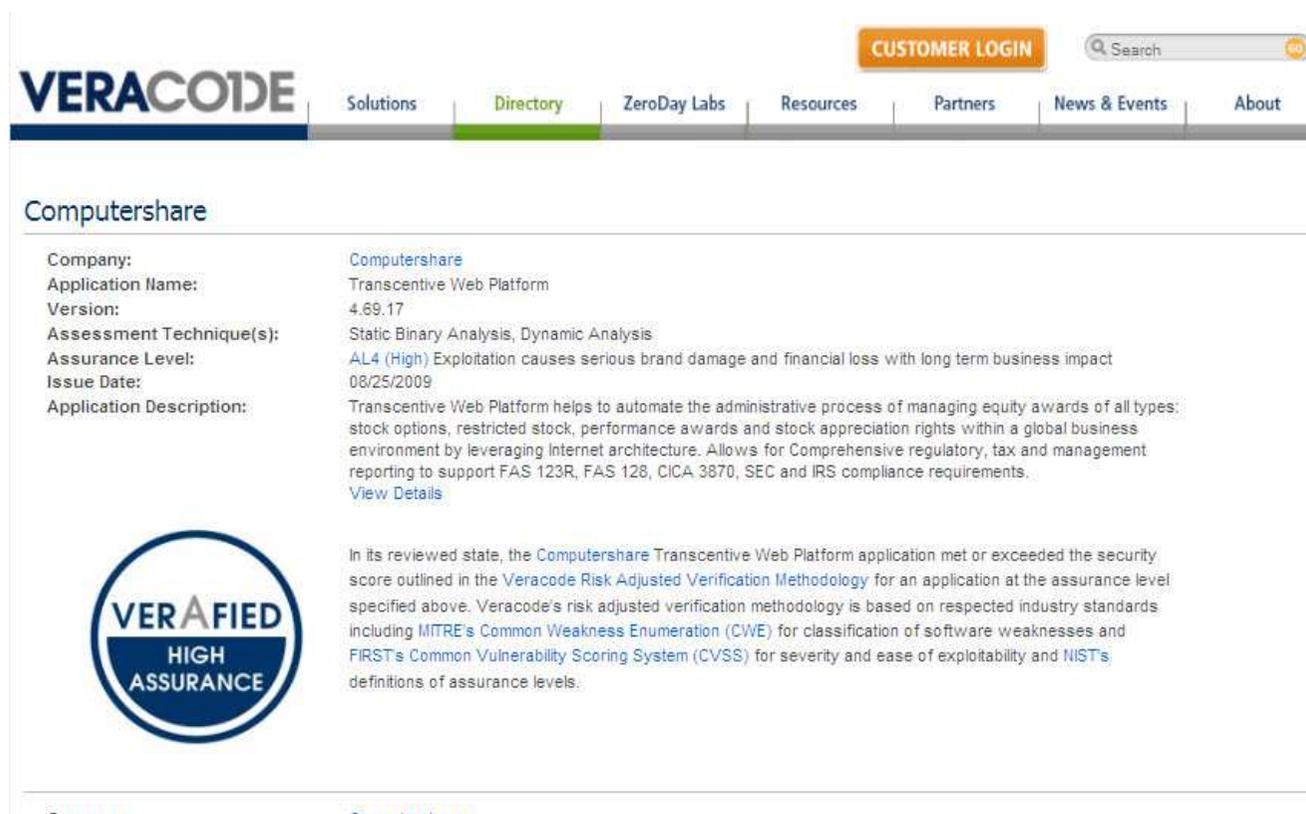
- **Fraud, Privacy and Security** are converging very quickly
 - » “Closing the circle” is becoming crucial to understanding the total state of security and software assurance has become a major component in achieving this.

- **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 shows the Veracode Directory page for the Computershare Transcendive Web Platform. The page features a navigation bar with the Veracode logo, a search bar, and a 'CUSTOMER LOGIN' button. The main content area displays the following information:

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. View Details

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

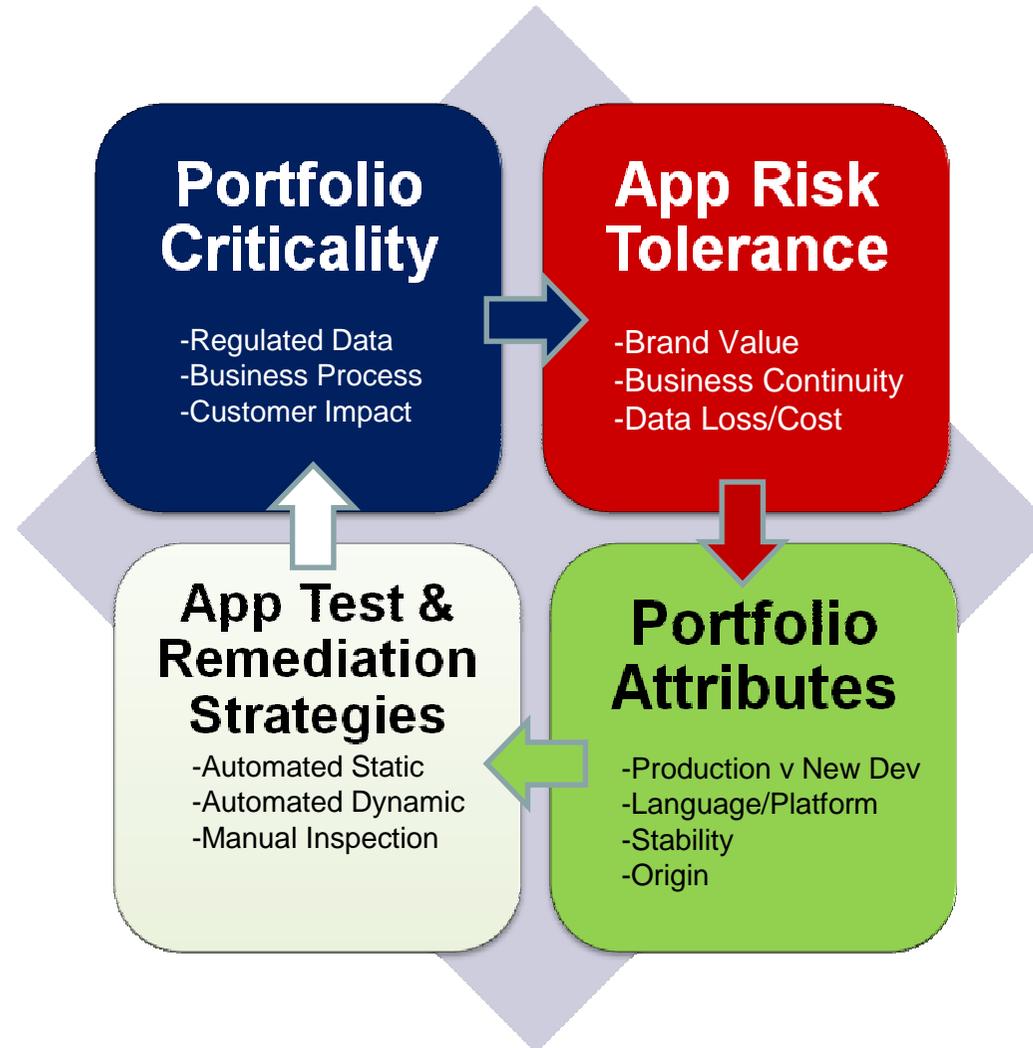
In its reviewed state, the [Computershare Transcendive Web Platform](#) application met or exceeded the security score outlined in the [Veracode Risk Adjusted Verification Methodology](#) for an application at the assurance level specified above. Veracode's risk adjusted verification methodology is based 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



Flexible, Risk-Based Application Security Policies and Remediation Guidance



Thank you!

Matthew Moynahan, CEO
mmoynahan@veracode.com

VERACODE

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

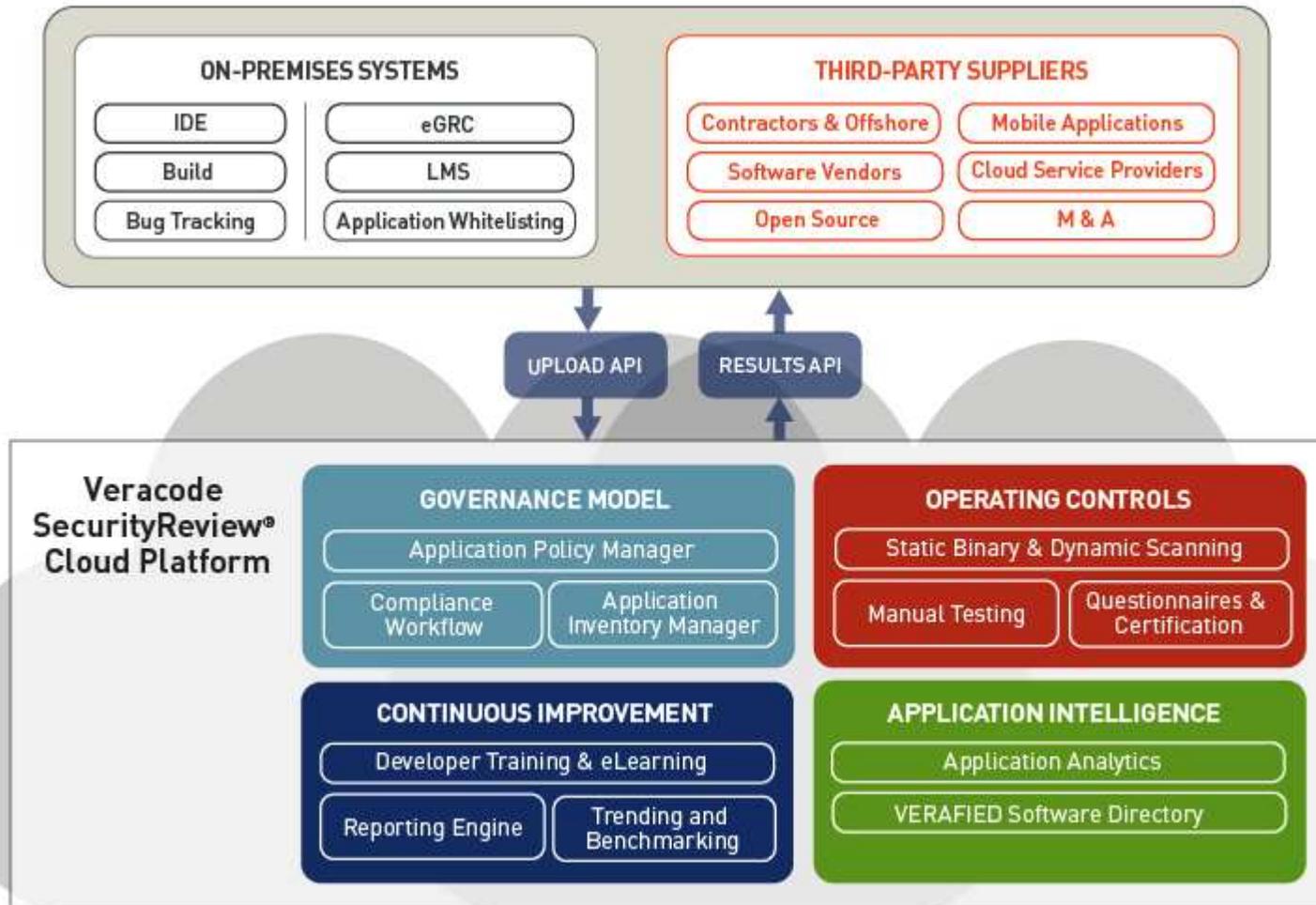
.....ensure that any code we produce **or procure** is more secure right from the beginning. Many of the clients I talk with are highly focused on the 'produce' part.....**What about the 'procure' part?**

INTRODUCTORY REMARKS

As the security threat against the enterprise and our federal government becomes increasingly visible, **enforcement and accountability is moving from security and development teams to audit committees and C-level executives (CIO, CRO, CISO, CFO).**

As a result, controlling this unbounded risk will require ARM processes to become more defined and cover more of the software infrastructure. This is what we are here to encourage and facilitate with your help.

Veracode Solution Architecture



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 3rd 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 3rd Party application security testing

