

# Actionable Strategies to Secure Your Third Party Software

*Solutions enterprises can use to lower the risk of outsourced & COTS software*

## Audio Information

Dial-In: +1 (877) 636-8062

Int'l Dial In: +1 (706) 634-1283

Conference ID: 71803401

**VERACODE**

**FORRESTER®**

## Today's Speakers



Chenxi Wang, Ph.D., serves as Forrester's Principal Analyst, Security and Risk Mgmt. She is a leading expert on content security, application security, and vulnerability management. Chenxi leads the effort at Forrester to build the application security and Web 2.0 security research portfolio. Chenxi's research builds on her in-depth technical insights and her years of research experience. Chenxi covers topics such as best practices for content and application security, emerging threats, and operational aspects of security deployment.

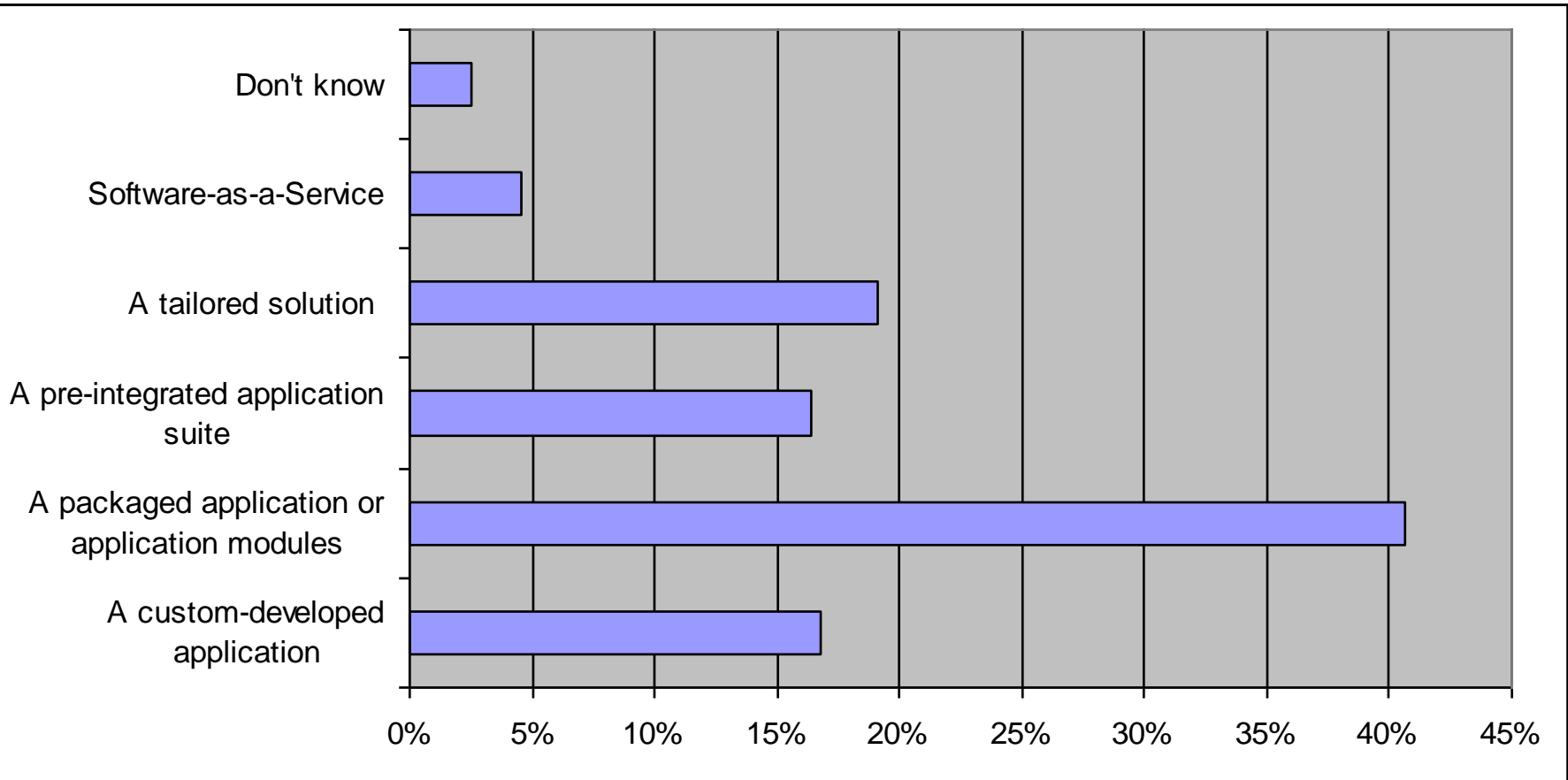


Chris Wysopal, Veracode's CTO and Co-Founder, is responsible for the company's software security analysis capabilities. In 2008 he was named one of InfoWorld's Top 25 CTO's and one of the 100 most influential people in IT by eWeek. One of the original vulnerability researchers, he has testified on Capitol Hill in the US on the subjects of government computer security and how vulnerabilities are discovered in software.

# Agenda

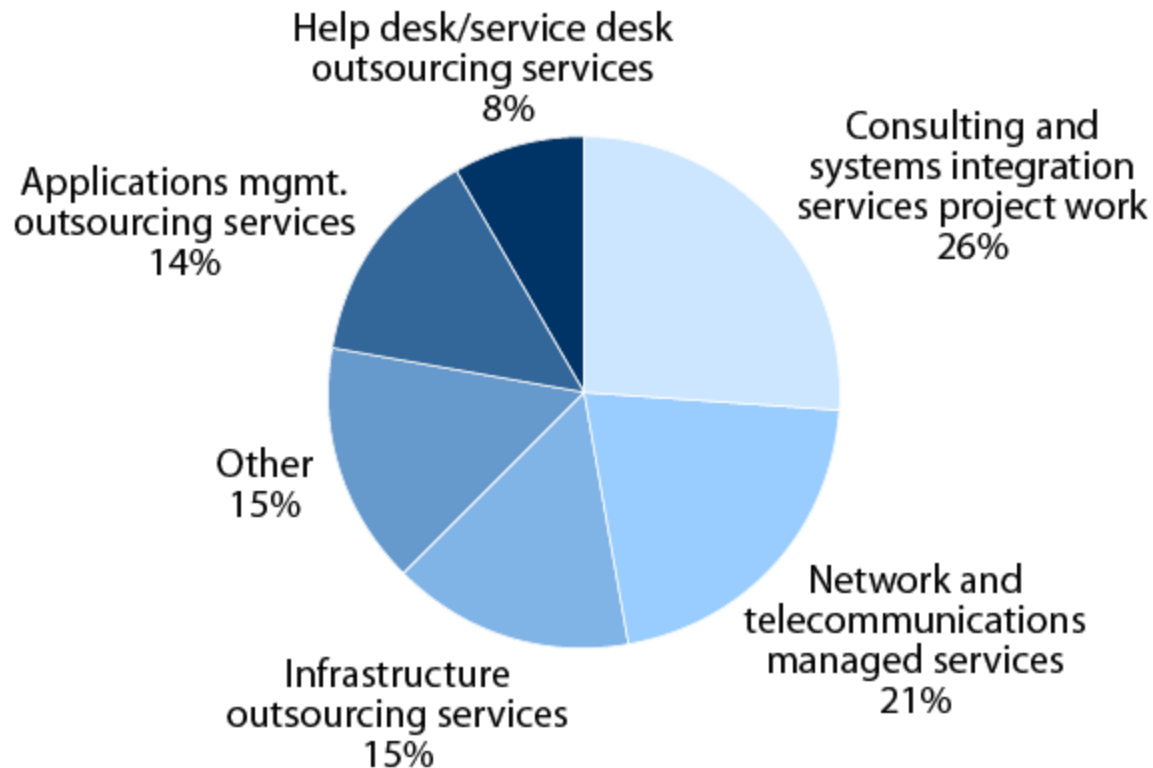
1. The state of software outsourcing and security of outsourced and commercial applications
2. Why should you be concerned about security for software?
3. Best practices to mitigate your risks
4. Forrester Recommendations
5. Actionable strategies to secure your applications
6. Case Study: Automating security acceptance testing of outsourced & COTS software

# The state of software implementation



- Leveraging packaged and outsourced code is an increasingly common practice

**“In 2007, what percent of your IT services budget will be spent on the following?”**



Base: 603 services decision-makers at North American and European enterprises

Source: Enterprise IT Services Survey, North America And Europe, Q2 2007

# Security risks for packaged and outsourced code

- Do you know your outsourcing provider's capability in security programming?
- Are you confident that their software security practices match your requirements?
- Do you know how to evaluate the security of outsourced code?
- Do you have a recourse plan when security incidents occur due to outsourced code?

## The reality is ...

- Many software firms do not practice secure programming
- Majority of software engineers are not versed in secure development
- Not every organization has established rigorous security testing alongside of quality testing
- Microsoft's newest server service vulnerability affects over 800 million computers worldwide [Oct 08]
- Oracle's critical patch update consistently include highly critical vulnerabilities

## As a result ...

- You are often left with software with security bugs
- You alone have to deal with the consequences, not your outsourcing provider
  - » Data breaches - \$100 to \$300 per record
  - » Loss of business reputation and customer confidence – difficult to calculate
  - » Fixes often incur additional cost

So what should you do?



## More concretely: You need to catch security flaws before production

### Selection

Be judicious  
about  
vendor's  
security  
practice

### Education

Help your  
vendor  
establish  
secure  
coding  
practice

### Contracts

Establish  
contractual  
protection

### Third-party

Get an  
independent  
evaluation

## Vendor selection

- Evaluate your vendor's software development practice
  - » CMMI is a good metric.
  - » Ask your vendor for the code development/review practice
  - » Ask if they have any secure coding training program
- Caveat
  - » You are only as secure as your vendor cares to be

## Contractually - Seek a risk-mitigating SLA

- Many outsourcers would not sign on to an SLA that includes penalty terms for security flaws
- So what can you reasonably expect?
  - » Demand thorough and rigorous code acceptance terms
  - » Seek third-party, independent evaluation for code security
  - » Build in your contract critical security fixes and subsequent reviews

## More specifically ...

- Understand and exercise your jurisdictional rights
  - » Especially important for off-shoring
  - » E.g., Safe Harbor certification
- Specify the inclusion of third-party evaluator from the start
- Clearly articulate accountability
- Communicate problem-solving processes

## For COTS software

- You often don't have an SLA
- The best you can do is rigorous evaluation
  - » In house
  - » Independent third party
- In-house evaluation requires expertise and time
  - » Do you have the required security expertise?

## Consider independent third-party evaluation

- You need third party evaluation when
  - » Internal expertise is lacking
  - » Independent opinion sought as additional verification
- Two forms of third-party evaluation
  - » Third-party code reviews
  - » Penetration testing
- Evaluation must comply with today's enterprise, distributed development environment

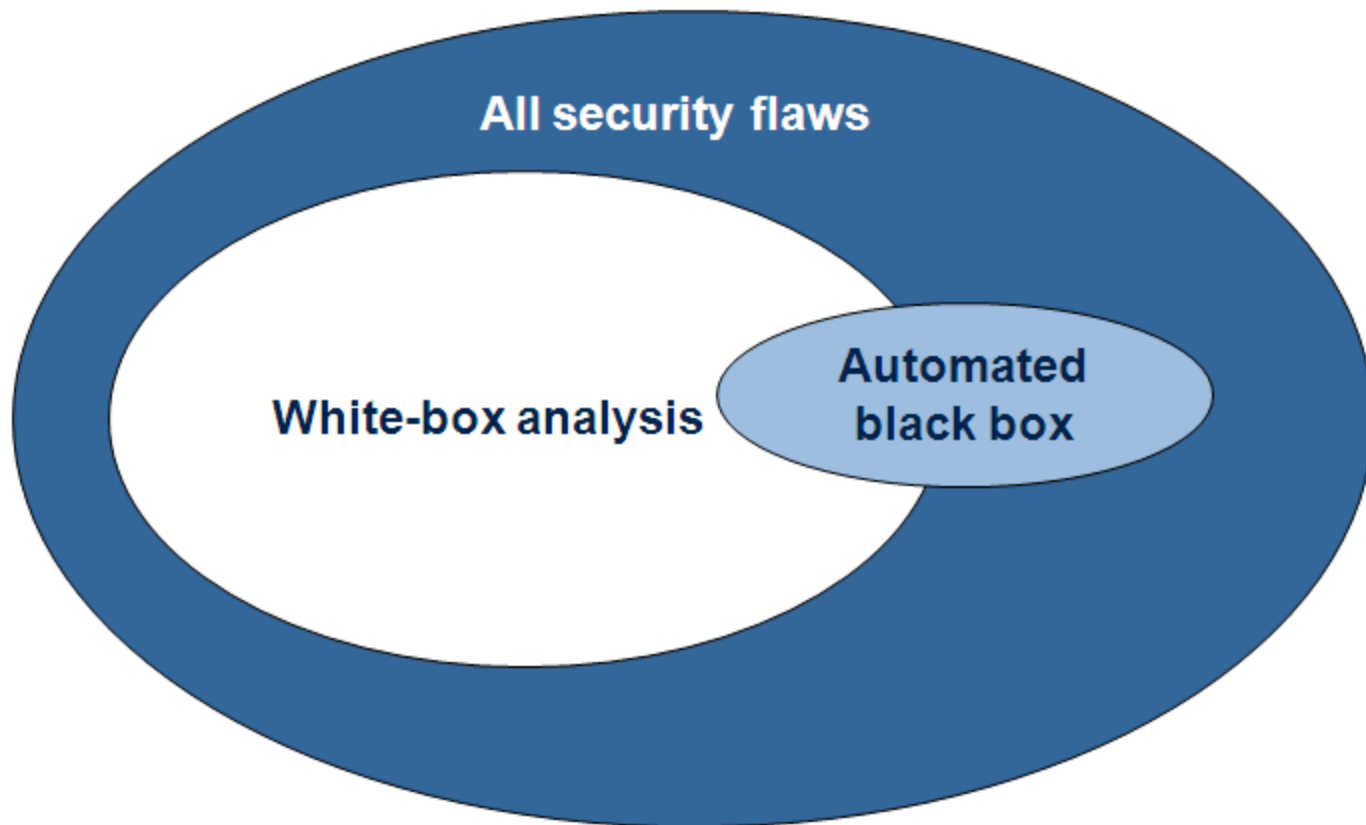
## A note about independent opinions

- Evaluator and the software producer can't be the same entity
  - » Conflict of interest
  - » Maker-checker principle
  
- Why not consider in-house evaluator?
  - » Often defeats the purpose of outsourcing
  - » Visibility is severely limited for packaged apps

## Third-party alternatives

- White-box code reviews
  - » Source code review: time consuming and source code availability is always a problem
  - » Binary scanning: a viable and effective alternative preserving much of the white-box advantages
  
- Black-box penetration testing
  - » Complementary to white-box
  - » Requires staging or production environment

## A note about white-box and black-box



# Application Security Maturity Model

Phase I



Phase II



Phase III

- Predominately reactive measures: fix vulnerabilities if exploited
- Ad hoc application scanning and penetration testing
- Isolated web application firewall deployment

- Proactive app security measures
- Established process for systematic application scanning and penetration testing
- Utilize secure coding tools in the development phase
- Systematic tracking of vulnerability databases

- Mature, end-to-end secure coding lifecycle
- Integrated white-box, black-box, and deployment tools
- Clearly defined success metric
- Corporate wide application security awareness

## Best practices summary

- You need a way to validate and ascertain how secure your outsourced software is
  - » Without necessarily build up the security expertise of your organization
  - » Without relying solely on internal expertise
- Third-party audit and evaluation is a must

# **Implementing Best Practices:**

## **5 Actionable Strategies to Secure COTS Software or Outsourced Development**

# Step 1: Software Risk Analysis

## Assigning Application Assurance Levels

Assurance Level	Description
Very High	Mission critical for business/safety of life and limb on the line
High	Exploitation causes serious brand damage and financial loss with long term business impact
Medium	Applications connected to the internet that process financial or private customer information
Low	Typically internal applications with non-critical business impact
Very Low	Applications with no material business impact

U.S. Govt. OMB Memorandum M-04-04; NIST FIPS Pub. 199

## Step 2: Create SLAs & Metrics

- Independent ratings based on industry standards enables better decision-making (CWE, CVSS, NIST)
- Eliminate the headaches associated with normalizing output from multiple testing techniques and vendors
- A common language to compare internally and externally developed code
- Ratings benefit both the Enterprise and the Provider

CVSS

NIST

CWE

APPLICATIONS'  
BUSINESS CRITICALITY

## Step 3: 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, code review, dynamic testing, penetration testing)
  - » Specific tools that should be used for testing
  - » Acceptance thresholds for testing
  - » Vulnerability correction rules



## Step 4: Conduct Independent Assessments

- Work collaboratively with outsourced provider or COTS vendor
- Trusted 3<sup>rd</sup> party provides transparency and unbiased analysis
- Independent Verification & Validation (IV&V)
  - » Meets auditing standards
  - » Segregation of Duties
  - » Strong proof of a security control
- Costs
  - » Forrester recommends budgeting at least 1% on of contract value for security and privacy monitoring (potential to pass on all or part of the cost to supplier)



**Moody's Investors Service**



**Underwriters  
Laboratories**

**Consumer  
Reports**

*“Rather than trying to change processes within both the bank and our vendors, Veracode's software-as-a-service model gave us rapid execution and results with minimal resources.”*

*– Rhonda MacLean, CISO of Barclays*

## Step 5: Set acceptance testing thresholds & remediation rules

- What security rating is acceptable?
- If rating not met, what is remediation roadmap to meet requirements?

Vendor SecurityReview®  
Summary Report for Company

Vendor: Open Source  
Application: Apache HTTP Server

Application Rating: D



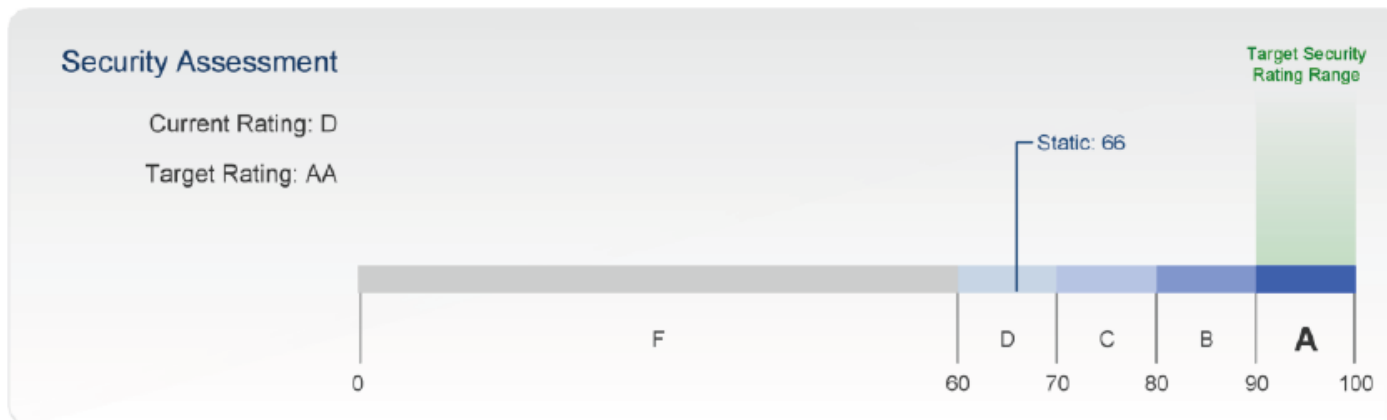
Rated: Sep 7, 2007

Top Risks

Top security flaws detected in the application included:

Flaw Category	Severity	Count
Buffer Overflow	Very High	4
Dangerous Functions	Very High	3
Numeric Errors	Medium	16
Authentication Issues	Medium	8
Error Handling	High	1

Total Flaws detected in application: 37

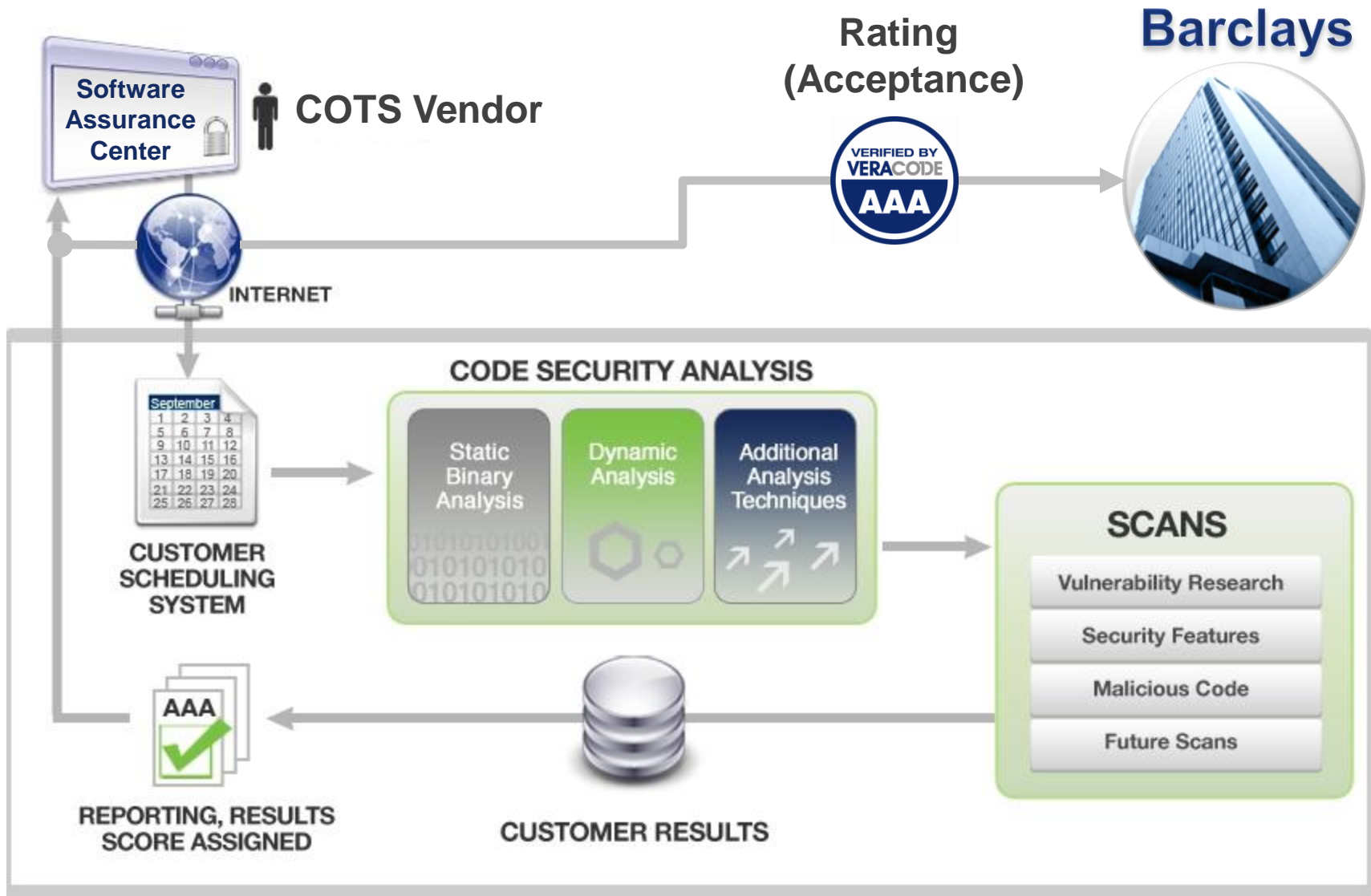


## Case Study: Automating COTS Security Testing

- Profile: One of the largest global financial services institutions
- Challenges:
  - » Multiple high assurance COTS software vendors
  - » Heavily regulated industry
  - » Transacts sensitive personal and financial data
  - » Large investment in application testing
  - » IP Issues inhibit testing (access to source code)
- Veracode COTS SecurityReview
  - » Automate security assessments
  - » Handle high volumes of applications with consistent ratings
  - » Identify issues and focus penetration testing efforts



# Case Study: Automating Security Acceptance Testing



# Sample Veracode COTS SecurityReview Report

## Vendor SecurityReview® Summary Report for Company

Application Rating: D



Rated: Sep 7, 2007

Vendor: Example Company  
Application: Project Management System

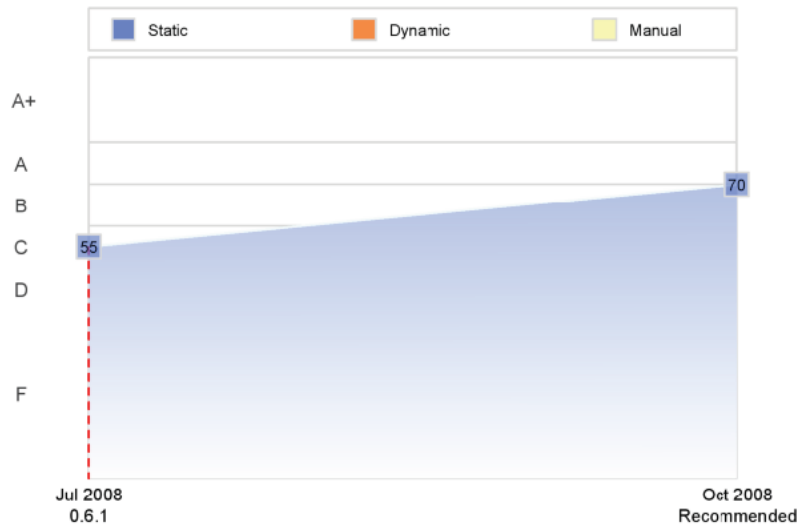
### Top Risks

Top security flaws detected in the application included:

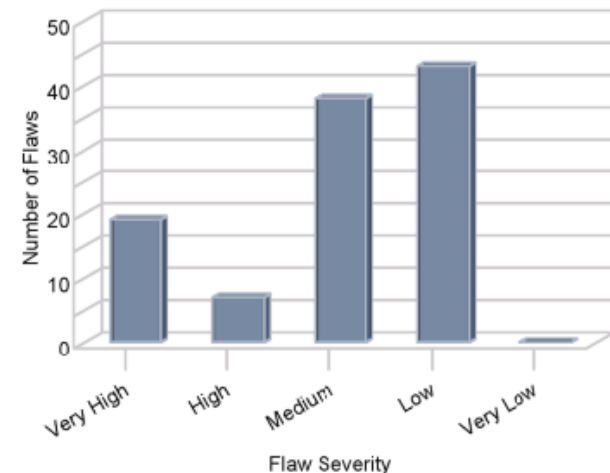
Flaw Category	Severity	Count
Buffer Overflow	Very High	4
Dangerous Functions	Very High	3
Numeric Errors	Medium	16
Authentication Issues	Medium	8
Error Handling	High	1

Total Flaws detected in application: 37

### Application Ratings Trend



### Security Flaws by Severity



## Case Study: Benefits

- Customer
  - » Security of sensitive data
  - » Instills confidence in enterprise
- Barclays
  - » Improves security posture
  - » Lowers costs & risks
  - » Covers large application portfolio
  - » Enables vendor management
  - » Meets regulatory requirements
- COTS Vendor
  - » Forms deep & lasting relationship
  - » Provides higher security quality code
  - » Trickle down security training
  - » Security becomes a competitive differentiator



*“Veracode’s rating system and remediation roadmaps provide extremely meaningful data that help our software suppliers to fix not just the obvious defects, but also the root cause of problems. The net result for Barclays is a rapid cycle of improvement in the security of applications, which is a clear benefit to our customers”*

**Rhonda MacLean, Global Security Officer for Barclays Global Retail and Commercial Bank**

## Summary

- The security of outsourced or COTS applications poses a serious threat to enterprises
- The liability of software vulnerabilities has rested mainly on the enterprise
- Enterprises can take actionable steps today to improve their security posture
- Independent testing provides transparency, while maintaining the intellectual property rights of vendors and preserves the benefit for enterprises to outsource or use COTS software

# Q&A

[contact@veracode.com](mailto:contact@veracode.com)  
781-425-6040

**VERACODE**

**FORRESTER®**