A Forrester Total Economic Impact™ Study

Commissioned By

Veracode

Project Director:
Sean Owens

March 2015

The Total Economic Impact™ Of Veracode's Cloud-Based Application Security Service For Independent Software Vendors

Security Gains, Cost Savings, And Business Benefits Enabled By Veracode Application Security

FORRESTER®

Table Of Contents

Executive Summary 3

Disclosures 4

TEI Framework And Methodology 5

Analysis 6

Financial Summary 21

Veracode application security testing: Overview 22

Appendix A: Representative Organization Description 25

Appendix B: Total Economic Impact™ Overview 26

Appendix C: Glossary 27

Appendix D: Supplemental Material 28

Appendix E: Endnotes 28

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

© 2015, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to www.forrester.com.

FORRESTER®

Executive Summary

Veracode commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) independent software vendors (ISVs) may realize when leveraging Veracode's application security testing services. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Veracode on their organization.

> *"What Veracode can do in three or four days of scanning is at least a month of code review for our engineering team."*
>
> ~ Operations manager, midsize software vendor

To better understand the benefits, costs, and risks associated with the use of Veracode's cloud-based platform by software vendors interested in securing the products they sell, Forrester interviewed two current Veracode customers and collected completed survey responses from 21 others.

Prior to implementing Veracode for application security, independent software vendors used other methods for addressing security: Some used alternative software solutions; others had a homegrown mix of tools and processes. No matter their situation, software vendors reported spending too much time responding to questions about their development process, conducting too many expensive penetration tests on behalf of individual customers, remediating previously undetected product vulnerabilities, and digging into unplanned and unbudgeted security requests. These ISVs recognized they were spending too much on reactive application security on behalf of customers or prospects while not getting enough real security improvements incorporated into their products. By using Veracode for independent security audits of third-party applications, ISVs were able to improve application security metrics, and also their ability to respond to customers' questions about software security — all at a reasonable investment. Said one CISO, "Having a third-party assessment that we can share with our customers of the quality, security, and resiliency of our software is extremely valuable."

VERACODE REDUCED APPLICATION SECURITY TESTING COSTS AND SPED UP RESOLUTION

Interviews and survey responses from 23 existing Veracode customers and subsequent financial analysis found that a representative organization based on these interviewed organizations experienced the risk-adjusted ROI, benefits, and costs shown in Figure 1.[1] See Appendix A for a description of the representative organization.

The representative organization analysis points to benefits of $381,930 per year versus implementation costs of $52,800 and annual costs of $144,000, adding up to a net present value (NPV) of $538,896.

For the representative organization, this equals an average of nearly $3,800 per developer in benefits and cost savings over the three-year analysis period. The representative software vendor saw improvements such as a 68% reduction in application security vulnerabilities for its software, a 38% reduction in external compliance and remediation costs, and a 70% improvement in the time it takes to research and respond to its customers' application security questions and requests.

FIGURE 1
Financial Summary Showing Three-Year Risk-Adjusted Results

Source: Forrester Research, Inc.

› **Benefits.** The representative organization experienced the following risk-adjusted benefits that represent those experienced by the interviewed and surveyed companies:

- **Reduced application testing costs through improved software development habits that help avoid common software vulnerabilities, along with avoided additional penetration tests, totaling $301,537 per year.** Veracode's standard testing found many common errors that developers learned to avoid. This contributed to a 68% total reduction in application security vulnerabilities for its software, saving time in both development and application security testing processes. Additionally, software vendors can share the Veracode summary report with current or potential customers and avoid significant costs on customized and repetitive penetration testing.
- **Reduced audit and compliance costs with clear and easy-to-consume Veracode application security results and improved development and security processes, totaling $33,800 per year.** Software vendors reported a 50% improvement in preparing for application security audits or reports and a 33% reduction in external compliance fees per year (for a total cost reduction of 38%). More secure applications mean fewer security vulnerabilities, fewer potential compliance concerns, and easier preparation of audit and compliance reports.
- **Improved response to customer application security questions, leveraging a clear and presentable application security summary report from Veracode, adding up to $46,593 per year.** Many software vendors share their Veracode summary report with their customers, reducing the time it takes to find and prepare responses to customer application security questions, as well as reducing the overall number of questions asked. The representative organization experienced a 70% overall reduction in the time it takes to handle and answer customer questions about application security.

› **Costs.** The representative organization experienced the following risk-adjusted costs:

- **Implementation costs of $52,800.** This includes resource effort, training, and new or upgraded software and hardware.
- **Annual costs of $144,000 per year.** These costs include areas such as Veracode subscription fees, software, internal management resources, and other costs.

Disclosures

The reader should be aware of the following:

› The study is commissioned by Veracode and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

› Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the report to determine the appropriateness of an investment in Veracode's application security testing services.

› Veracode reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.

› Veracode provided the customer names for the interviews but did not participate in the interviews.

TEI Framework And Methodology

INTRODUCTION

From the information provided in the interviews, Forrester has constructed a Total Economic Impact (TEI) framework for those organizations considering implementing Veracode's application security testing. The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision, to help organizations understand how to take advantage of specific benefits, reduce costs, and improve the overall business goals of winning, serving, and retaining customers.

APPROACH AND METHODOLOGY

Forrester took a multistep approach to evaluate the impact that Veracode's application security testing can have on an organization (see Figure 2). Specifically, we:

- Interviewed Veracode marketing, sales, and/or consulting personnel, along with Forrester analysts, to gather data relative to application security testing and the marketplace for application security testing, particularly for ISVs.
- Interviewed two software vendors currently using Veracode's application security testing to obtain data with respect to costs, benefits, and risks.
- Surveyed 21 more organizations about their application testing time and resources before and since using Veracode.
- Designed a representative organization based on characteristics of the interviewed organizations (see Appendix A).
- Constructed a financial model representative of the interviews using the TEI methodology. The financial model is populated with the cost and benefit data as applied to the representative organization.
- Risk-adjusted the financial model based on issues and concerns the interviewed and surveyed organizations highlighted. Risk adjustment is a key part of the TEI methodology. While organizations provided cost and benefit estimates, some categories included a broad range of responses or had a number of outside forces that might have affected the results. For that reason, some cost and benefit totals have been risk-adjusted and are detailed in each relevant section.

Forrester employed four fundamental elements of TEI in modeling Veracode's service: benefits, costs, flexibility, and risks.

Given the increasing sophistication that enterprises have regarding ROI analyses related to IT investments, Forrester's TEI methodology serves to provide a complete picture of the total economic impact of purchase decisions. Please see Appendix B for additional information on the TEI methodology.

FIGURE 2

TEI Approach

Source: Forrester Research, Inc.

Analysis

> *"Having a third-party assessment that we can share with our customers of the quality, security, and resiliency of our software is extremely valuable."*
>
> ~ CISO, multinational software firm

REPRESENTATIVE ORGANIZATION

For this study, Forrester conducted a total of two interviews with representatives from the following independent software vendors, which are Veracode customers based in the US:

- A midsize independent software vendor that develops endpoint protection software and services.
- A multinational firm that develops and sells employee-benefit-related solutions to organizations.

Forrester also collected surveys from 21 more organizations that identified as ISVs, software development contractor or consultancy firms and other development organizations, focusing on the key processes and customer communication and sales that a software vendor would encounter. Interviewed and surveyed organizations ranged in size from fewer than 20 to nearly 100,000 employees. Based on the interviews, Forrester constructed a TEI framework, a composite company, and an associated ROI analysis that illustrates the areas financially affected. The representative organization synthesized by Forrester from these results represents an organization with the following characteristics:

- Is a US-based independent software vendor.
- Has 1,000 employees.
- Has 500 business customers that purchase or license developed software and services.
- Has 20 applications in the current portfolio and expects about 15 of those applications to be tested with Veracode each year for the next few years.
- Employs 250 software developers.

As a result of an increased frequency of customer questions about its application security and processes to ensure security — as well as a few customers who requested the software vendor specifically implement Veracode as the preferred application security testing provider — the representative organization reviewed internal and third-party application security options and selected Veracode as a respected leader in the space. The organization began deployment in the summer of 2013:

- Some application products were scanned immediately, but complete implementation, including full application security processes applied to new or upgraded applications, was completed in mid-2014.
- All software developers were trained in new software development and testing processes that leverage Veracode best practices, remediation guidance, and standardized testing guidelines to avoid common development mistakes and retesting.
- Most current and new applications produced and sold by the representative organization have been or will be tested with Veracode. The binary static analysis results are leveraged as artifacts of secure development to share with customers who ask about application security, so the representative organization can conveniently discuss its approach to product security with current or potential customers who ask.

- Some of the representative organization's software products have received the VerAfied seal from Veracode. This indicates that at the time of the assessment, the application had no "medium," "high," or "very high" severity vulnerabilities and no OWASP top 10 or CWE/SANS top 25 vulnerabilities were discovered. The representative organization can also leverage this seal to discuss the security of its products in marketing materials and on the company's website.

> *"We can provide our customers peace of mind by having our software scanned by an independent third party [Veracode]. We can provide [them] the Veracode test results and show that we are acting upon any potential vulnerabilities."*
>
> ~ Operations manager, midsize software vendor

INTERVIEW HIGHLIGHTS

These software vendors identified a number of issues with their previous solutions (or ad hoc processes) that were eliminated or reduced once they implemented Veracode.

Situation

Software vendors frequently faced questions from prospects and customers about the security of their software products during and after the buying cycle:

- Customer questions and requests for documentation were taking a lot of time when test results were not well organized and the organization required extra time to collect information for a customer.
- Application developers spent too much time on remediation of vulnerabilities without adequate training or coaching when using another application testing solution.
- With less secure software, organizations were at a higher risk to incur compliance and audit costs, in addition to the risk of a security event that could lead to lost customers.

Solution

The representative organization selected Veracode as an industry leader in application security that provides high-value application security expertise. After selecting Veracode, the organization kicked off a planning and pilot phase with a smaller development team to identify any processes that needed to be updated along with the implementation of the new solution. This planning, piloting, and gradual rollout phase lasted 45 weeks, at which point the organization standardized all development on incorporation of application testing through Veracode.

Results

The interviews revealed that:

- **Application testing and development is more efficient with Veracode.** Developers are learning how to avoid common development mistakes (like a SQL injection error) through Veracode training and advice. They don't spend extra time having to resolve the issue and rewrite the code. Applications pass Veracode testing more often on the first or early tries. And organizations that were investing significant costs for penetration

> *"We can respond to customer questions about application security virtually immediately."*
>
> ~ CISO, multinational software firm

testing can avoid all or a major portion of these testing costs with Veracode.

- **Organizations had improved documentation processes and clear application testing reports.** With this, compliance and audit resource times and third-party costs are greatly reduced.
- **Customer questions and requests for documentation are much quicker to resolve for a variety of reasons.** These include:
  - Veracode is a respected and recognized leader in application security, so just mentioning Veracode already answers many questions for customers.
  - Veracode testing results include scan results for detailed internal review, as well as a summary report that can be shared with customers.
  - Veracode's guidance covers not only processes related to increased application security but also customer response processes, advocating clear roles and responsibilities, good document management, and transparency when communicating processes and results to customers.

BENEFITS

The representative organization experienced a number of quantified benefits in this case study:

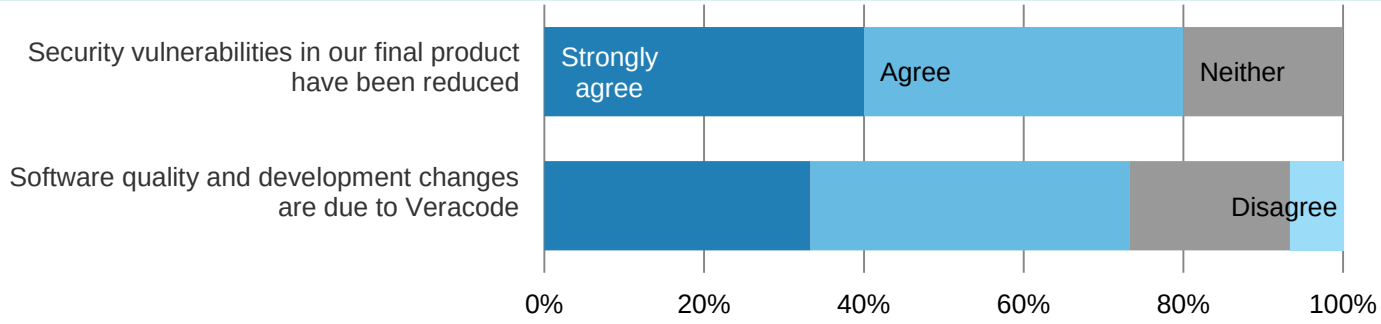
- Application development is more efficient, as developers learn to avoid common development mistakes.
- Compliance and audit costs are greatly reduced or avoided.
- Customer questions and requests for documentation are resolved more quickly.

> *"Veracode is an important part of our software development life cycle."*
>
> ~ Operations manager, midsize software vendor

More Efficient Application Testing And Development, Leading To Faster Time-To-Market

In addition to answering customer questions more quickly and at a higher quality, the application testing process is more efficient, and application development can be completed more quickly for a faster time-to-market. With Veracode, software vendors can test software efficiently and to a common standard. This means that early in their implementation of Veracode, many application flaws were identified and flagged for correction, and developers learned to avoid common mistakes like SQL injection vulnerabilities. As shown in Figure 3, organizations agreed that not only did application testing become more efficient and applications were completed sooner, but developers were more productive, as they were able to focus on completing new application development tasks rather than correcting past ones.

FIGURE 3
Application Testing Is More Efficient, And Developers Create Higher-Quality Software With Veracode



Base: 15 surveyed and interviewed organizations that use Veracode

Source: Forrester Research, Inc.

Fifteen interviewed and surveyed organizations highlighted more efficient application testing as a key benefit enabled with Veracode. These organizations reported:

- Before Veracode, 27% of applications would pass testing on the first try, and 60% would eventually pass after the first or later revision.
- With Veracode, those metrics improved to 62% passing on the first try and 75% passing after a later revision.

(Note that not every application needs to "pass" testing. None of the remaining vulnerabilities are "critical" or "high," so the software vendor or its customers may consider remaining vulnerabilities to be low priority, irrelevant, or tabled for a later release.)

TABLE 1
Reduced application security testing Costs

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
A1	Apps tested per year		15			
A2	Typical security vulnerabilities per app before Veracode		30			
A3	Worst-case security vulnerabilities per app before Veracode		8			
A4	Total security vulnerability reduction with Veracode		68%			
A5	Time to address typical security vulnerabilities before Veracode (hours)		12			
A6	Time to address worst-case security vulnerabilities before Veracode (hours)		18			
A7	Improvement in all security vulnerability resolution with Veracode		80%			
A8	Average developer hourly salary		$48			
A9	Penetration (pen) test requests from customers each year		8			
A10	Percentage of pen tests avoided with Veracode		75%			
A11	Cost per pen test		$20,000			
At	App development improvements	A1*(A2*A4*A5*A7+A3*A4*A6*A7)*A8+A9*A10*A11	$0	$317,407	$317,407	$317,407
	Risk adjustment	↓ 5%				
Atr	**App development improvements (risk-adjusted)**		**$0**	**$301,537**	**$301,537**	**$301,537**

Source: Forrester Research, Inc.

Before Veracode, organizations reported (as shown in Table 1):

- About 30 security vulnerabilities per application.
- Each took an average of 12 to 18 hours to review, correct, and test (longer for the security vulnerabilities considered “worst case”).

With Veracode, organizations reported a 68% reduction in security vulnerabilities and an 80% reduction in security vulnerability resolution time. They reported:

- About 10 security vulnerabilities per application.
- These security vulnerabilities take far less time to review and correct — now around only 2 to 4 hours.

The operations manager at a midsize software vendor said, "What Veracode can do in three or four days of scanning is at least a month of code review for our engineering team."

Developers can spend more time on their next application project, or the organization can invest in new projects. This developer time savings adds up to $197,407 per year, or a three-year NPV of $490,922 (or nearly $2,000 per developer).

For one interviewed software vendor, response improvements include a reduction in penetration testing time and costs. Current and potential customers would commonly ask for a penetration test ("pen test") of the product, often with their preferred testing platform. Past penetration tests were not of use, as customers often wanted their own report, or past reports included too much information from another customer. For one application, the organization would have had to conduct (at its expense, if it wanted to sell its software) multiple pen tests — often up to 10 and sometimes as many as 50 to 75. At $15,000 to $30,000 per pen test (for this illustration, as pen tests can cost much more), this adds up to significant costs. With Veracode, the organization can implement more scalable testing processes where it can conduct a single binary static analysis and replace virtually all but the occasional few pen tests. This could mean a savings of millions of dollars per year. This benefit has been included in the model; however, for the representative organization, the amount of avoided pen tests is lower, as most organizations conducted only a few, if any, pen tests for their applications. As shown in Table 1, six avoided pen tests per year (a 75% reduction of the original eight) at $20,000 per test adds up to $120,000 in annual avoided costs.

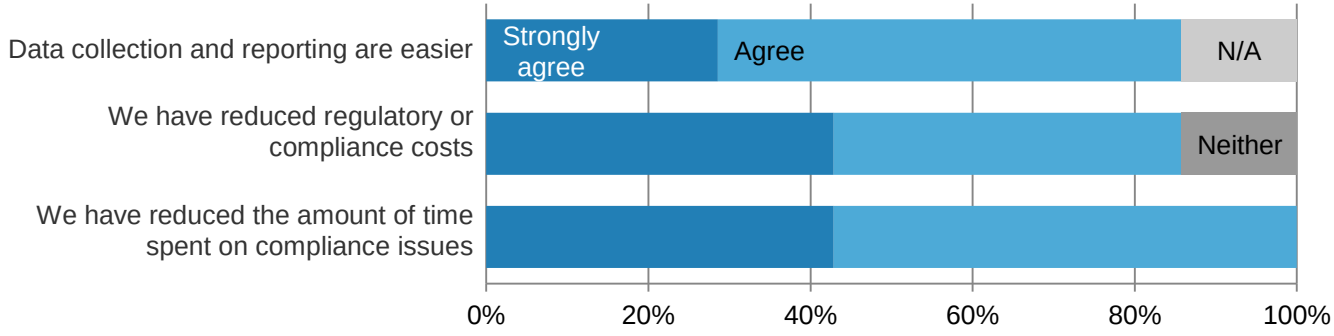
The avoided costs for developer application testing productivity and penetration testing add up to a savings of $317,407 per year, for a three-year NPV of $789,344. Since developer productivity may not be completely recovered (perhaps they take more breaks or there is a shortage of projects to assign), and penetration testing costs are varied, a 5% risk adjustment has been applied to this benefit. The risk-adjusted annual benefit is $301,537, for a risk-adjusted, three-year NPV of $749,877.

Also, while not included in the financial modeling, as there are other factors involved in application time-to-market, more efficient application testing can help make a difference. The representative organization measured a total of 2,742 hours saved per year, or nearly 35 days of 10 developers working 8 hours a day. With this time savings, software vendors could release a product earlier, potentially generating extra sales revenue. They could also use that time to develop another application for sale, which would also potentially generate new revenue.

Reduced Or Avoided Compliance And Audit Costs

As a result of improved application security processes and more secure applications, compliance and auditing issues related to application security are both less frequent and, for those issues that still occur, take less time to resolve. Seven interviewed and surveyed organizations identified this as a key benefit. Since implementing Veracode, they all reported time savings dealing with compliance issues; most identified time savings in audit report preparation, and most agreed they had experienced savings in compliance or regulatory costs (except one organization that neither agreed nor disagreed).

FIGURE 4
Application Testing With Veracode Improved Internal And External Compliance Efforts



Base: 7 surveyed and interviewed organizations that use Veracode
Source: Forrester Research, Inc.

While only three organizations reported external fees, they all reported a reduction in these fees since Veracode. As shown in Table 2, the representative organization had 24 application security audits or reports to prepare per year, based on the seven organizations that provided details about this benefit. Each report took about 20 hours to complete. The representative organization saw a 50% reduction in both metrics since implementing Veracode: Now it compiles about 12 audit or compliance reports per year, and they take only 10 hours to complete. With Veracode, the application security testing results answer a number of questions that would have otherwise required some data gathering and report preparation. With these testing results, along with updated reporting and application management processes, it is much easier for the organization to prepare the reports still needed. While this doesn't add up to be a very large benefit — 24 reports took 20 hours each before and were reduced to 12 reports at 10 hours now, which adds up to $4,080 per year — it is important to keep in mind that these improvements can have an impact on other parts of the business. Better reports can lead to better decision-making, and avoiding external compliance issues can help improve marketing and customer relations.

While many of these audits are for internal reporting processes, some end up in public forums. For example, the organization brought in third-party auditing services for an annual report, and a portion of these auditing efforts were related to application security. Also, the organization incurred some costs related to the security of its applications as reported by customers. Whether these customer-reported issues were real or perceived, without complete and clear auditing the organization considered it easier to pay the added costs rather than argue with a customer and probably damage the relationship. All told, the representative organization spent $110,000 on compliance and remediation costs before Veracode. With Veracode, external compliance costs were reduced by 33%, and external remediation costs were reduced by 50%, for a total reduction of $42,250 per year, or a total reduction in compliance and remediation costs of about 38%, as shown in Table 2.

TABLE 2
Reduced Or Avoided Compliance And Audit Costs

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
B1	Number of reports or audits per year before Veracode		24			
B2	Improvement with Veracode		50%			
B3	Hours to prepare for each security audit or review before Veracode		20			
B4	Improvement with Veracode		50%			
B5	External compliance costs before Veracode		$75,000			
B6	Improvement with Veracode		33%			
B7	External remediation costs before Veracode		$35,000			
B8	Improvement with Veracode		50%			
Bt	Compliance cost reduction	B5*B6+B7*B8		$42,250	$42,250	$42,250
	Risk adjustment	🡻 20%				
Btr	**Compliance cost reduction (risk-adjusted)**			**$33,800**	**$33,800**	**$33,800**

Source: Forrester Research, Inc.

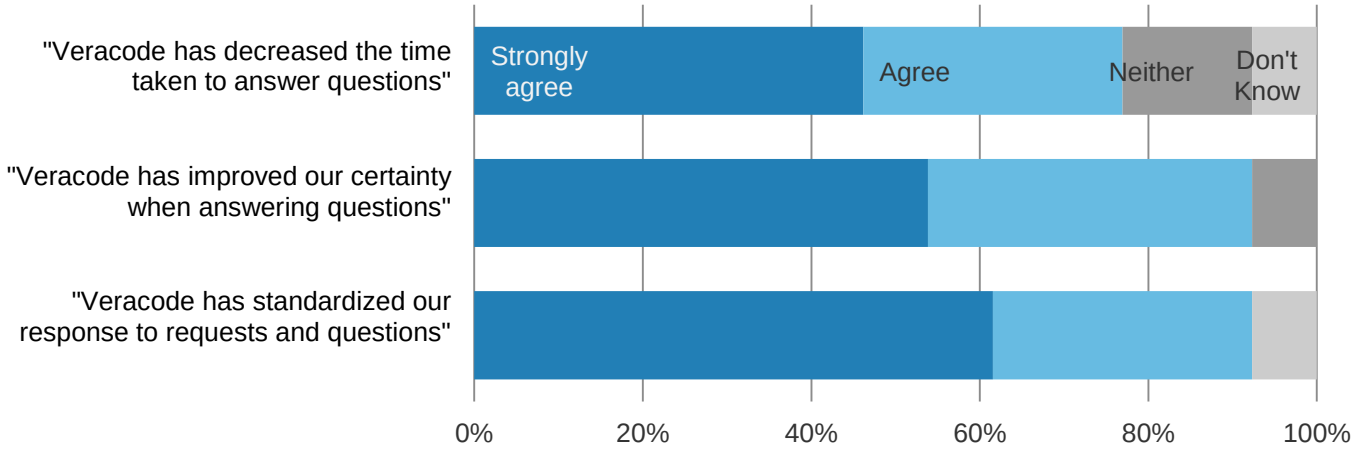
Resource and external costs together add up to $42,250 saved per year, or a three-year NPV of $105,069. This benefit has been risk-adjusted by the significant factor of 20%, since audit and compliance costs can vary greatly across organizations. The risk-adjusted annual benefit is $33,800, for a three-year, risk-adjusted NPV of $84,056.

Improved Quality And Speed Of Resolution To Customer Questions About Application Security

Security has become a larger concern for many organizations, and it will only continue to be a concern as more data is processed and more applications access that data. Organizations that collect and store data run a risk that data may be exposed or lost. Today, with improvements in networking and server security, applications are the most common way data is stolen or lost, according to multiple security reports.[2] Just a single lapse in an application might allow someone to take advantage with a SQL injection or cross-site scripting attack; it may also allow the wrong users (or any user) to mistakenly access secure data. Whether malicious or accidental, a data breach could mean thousands or even millions of dollars in remediation and recovery costs. It could lead to customer and sales losses and perhaps even spell the end of the business.

So, it's no surprise that customers buying software developed by an independent vendor want to know about the application's security and see results of security tests.

FIGURE 5
Responses To Customer Queries About Security Are More Efficient And Higher Quality With Veracode



Base: 13 surveyed and interviewed organizations that use Veracode
Source: Forrester Research, Inc.

For nearly all interviewed and surveyed organizations, Veracode helped independent software vendors resolve customer requests more quickly, and the organizations could share the Veracode summary report with their customers. All customers agreed with statements that Veracode has decreased the time to respond to requests, improved certainty of answers, and helped standardize responses. Because he or she can share results of Veracode scanning tests directly from the Veracode platform, the CISO of a multinational firm said, "We can respond to customer questions about application security virtually immediately."

Organizations were further asked about the frequency of customer questions, which were classified in two groups: typical and difficult (or "worst case"). They identified significant time savings for both types of questions. As shown in Table 3, before implementing Veracode the representative organization received a total of 300 questions each month: 270 typical and 30 difficult. Typical questions took an average of 30 minutes to resolve, and difficult ones took 47 minutes. With Veracode, the organization saw a 70% reduction in question resolution time, saving 21 to 33 minutes per request. Based on an average information worker salary (not developers, as these would be employees with groups such as customer support and sales representatives), this adds up to a total savings of $51,770 per year, for a three-year net present value (NPV) of $128,745. Given the variability in the number of requests, this benefit has been risk-adjusted down by 10%. The risk-adjusted annual benefit is $46,593, for a three-year NPV of $115,870.

TABLE 3
More Efficient Customer Response To Security Questions

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
C1	Total questions related to security per month		300			
C2	Percent of questions considered "worst case"		10%			
C3	Typical question response before Veracode (minutes)		30			
C4	Worst-case question response before Veracode (minutes)		47			
C5	Improvement to question response with Veracode		70%			
C6	Average information worker salary		$45			
Ct	Improved customer response	C1*(1-C2)*(C3/60*C5) *C6*12+C1*C2*C4/60*C5*C6		$51,770	$51,770	$51,770
	Risk adjustment	↓ 10%				
Ctr	**Improved customer response (risk-adjusted)**			**$46,593**	**$46,593**	**$46,593**

Source: Forrester Research, Inc.

Improved Sales

While not included in the model for the representative organization, three interviewed and surveyed organizations reported some sales improvement since implementing Veracode and using application security as a competitive differentiator. When asked about their agreement or disagreement with the statement, "Customers often select our product specifically because of our security," all three agreed or strongly agreed. However, the sales revenue and profit impact are widely variable. They can depend on whether the organization is taking a leadership role in its market with improved application security or catching up to its competitors. For this study, the representative organization does highlight successful Veracode application security testing in its sales discussions, but it does not have enough data at this time to estimate the impact on revenue. But as the operations manager at an interviewed software vendor said, "Veracode seals the deal."

Total Benefits

Table 4 shows the total of all benefits across the areas listed above, as well as present values (PVs) discounted at 10%. Over three years, the representative organization expects risk-adjusted total benefits to be a PV of nearly $950,000. The organization can also look at this in other ways: This equals an average of almost $3,800 per developer, or more than $63,000 on average per application tested.

TABLE 4
Total Benefits (Risk-Adjusted)

Ref.	Benefit Category	Initial	Year 1	Year 2	Year 3	Total	Present Value
Atr	App development improvements	$0	$301,537	$301,537	$301,537	$904,610	$749,877
Btr	Compliance cost reduction	$0	$33,800	$33,800	$33,800	$101,400	$84,056
Ctr	Improved customer response	$0	$46,593	$46,593	$46,593	$139,780	$115,870
	Total benefits (risk-adjusted)	**$0**	**$381,930**	**$381,930**	**$381,930**	**$1,145,790**	**$949,803**

Source: Forrester Research, Inc.

COSTS

The representative organization experienced a number of costs associated with Veracode:

- Implementation costs to implement Veracode, including resource effort, training, and new or upgraded software and hardware.
- Annual costs such as Veracode subscription fees, hardware and software, internal management resources, and other costs.

These represent the mix of internal and external costs experienced by the representative organization for initial planning, implementation, and ongoing fees and maintenance associated with the solution.

Implementation Costs

Veracode's security platform is a cloud-based service that makes implementation simple. A proper embedding of Veracode includes application development and testing process changes, which is reflected in the training costs and implementation time of nearly three-quarters of a year. This includes a quick deployment, then testing, piloting, and careful expansion through all development, test, and reporting teams and systems, as detailed in Table 5. Upfront costs do not include Veracode license fees, which are captured below as an annual subscription. However, interviewed and surveyed organizations reported some additional software and hardware costs. These are not related to Veracode's service but are for related systems that needed to be added or upgraded to fully integrate Veracode into a mature application development process. For example, organizations may need to purchase and/or deploy a new or expanded document management system to store and organize application testing results and other related materials, or a new integrated development environment (IDE) solution to support updated development processes.

TABLE 5
Implementation Costs

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
D1	Software and hardware		$10,000			
D2	Training		$2,000			
D3	Implementation weeks		45			
D4	FTE involved in implementation		0.5			
D5	FTE rate		$40			
Dt	Implementation costs	D1+D2+D3* D4*D5*40	$48,000	$0	$0	$0
	Risk adjustment	↑ 10%				
Dtr	**Implementation costs (risk-adjusted)**		**$52,800**	**$0**	**$0**	**$0**

Source: Forrester Research, Inc.

New Ongoing Costs

Annual costs include Veracode licensing fees, other related software and hardware maintenance costs, ongoing Veracode solution management resource costs, and other costs such as third-party consulting fees, as shown in Table 6. Note that the Veracode licensing costs are based on a broad estimate for the representative ISV and are provided for illustration purposes only; an individual's licensing costs will depend on a variety of factors.

TABLE 6
New Ongoing Costs

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
E1	Veracode license costs			$120,000		
E2	Hardware and software			$10,000		
E3	Other fees			$10,000		
E4	Labor costs			$4,000		
Etr	**New ongoing costs (risk-adjusted)**	E1+E2+E3+E4	**$0**	**$144,000**	**$144,000**	**$144,000**

Source: Forrester Research, Inc.

Total Costs

Table 7 shows the total of all benefits across the areas listed above, as well as present values (PVs) discounted at 10%. Over three years, the representative organization expects risk-adjusted total costs to be a present value of nearly $410,907. This adds up to less than $1,700 on average per developer, or about $27,500 per application tested.

TABLE 7
Total Costs (Risk-Adjusted)

Ref.	Cost Category	Initial	Year 1	Year 2	Year 3	Total	Present Value
Dtr	Implementation costs	$52,800	$0	$0	$0	$52,800	$52,800
Etr	New ongoing costs	$0	$144,000	$144,000	$144,000	$432,000	$358,107
	Total costs (risk-adjusted)	**$52,800**	**$144,000**	**$144,000**	**$144,000**	**$484,800**	**$410,907**

Source: Forrester Research, Inc.

FLEXIBILITY

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for some future additional investment. This provides an organization with the "right" or the ability to engage in future initiatives but not the obligation to do so. There are multiple scenarios in which a customer might choose to implement application security testing and later realize additional uses and business opportunities. Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix B).

As already described in the last section of the Benefits chapter, organizations can point to overall improvements in sales revenue by already including Veracode application security testing results in sales discussions, but we do not have enough data to quantify that benefit at this time.

However, organizations are not using their application security results for marketing at this time but plan to in the future. As explained in the Veracode application security testing: Overview section, Veracode's VerAfied and Scanned by Veracode programs can help customers promote their use of Veracode in their marketing and sales materials in order to leverage security as a competitive differentiator.

Software vendors can highlight the VerAfied or Scanned by Veracode seals on their website and in marketing materials, as a way to highlight:

- The software vendor's priority on application security and the high security of its applications.
- How it might differentiate it from other similar organizations as an application security leader.

RISKS

Forrester defines two types of risk associated with this analysis: "implementation risk" and "impact risk." Implementation risk is the risk that a proposed investment in application security testing may deviate from the original or expected requirements, resulting in higher costs than anticipated. Impact risk refers to the risk that the business or technology needs of the organization may not be met by the investment in Veracode, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for cost and benefit estimates.

TABLE 8
Benefit And Cost Risk Adjustments

Benefits	Adjustment
App development improvements	↓ 5%
Compliance cost reduction	↓ 20%
Improved customer response	↓ 10%

Costs	Adjustment
Implementation costs	↑ 10%
New ongoing costs	↑ 0%

Source: Forrester Research, Inc.

Quantitatively capturing implementation risk and impact risk by directly adjusting the financial estimates results provides more meaningful and accurate estimates and a more accurate projection of the ROI. In general, risks affect costs by raising

the original estimates, and they affect benefits by reducing the original estimates. The risk-adjusted numbers should be taken as "realistic" expectations since they represent the expected values considering risk.

The following impact risks that affect benefits are identified as part of the analysis:

- Organizational improvements in quality and response time to customer questions about application security can vary from company to company.
- Developer productivity may not be completely recovered for other application development work, and avoided penetration testing costs are varied.
- Compliance and auditing costs vary from organization to organization and can depend greatly on whether past issues have occurred.

The following implementation risks that affect costs are identified as part of this analysis:

- Both implementation and ongoing costs include broad assumptions that may vary from organization to organization.

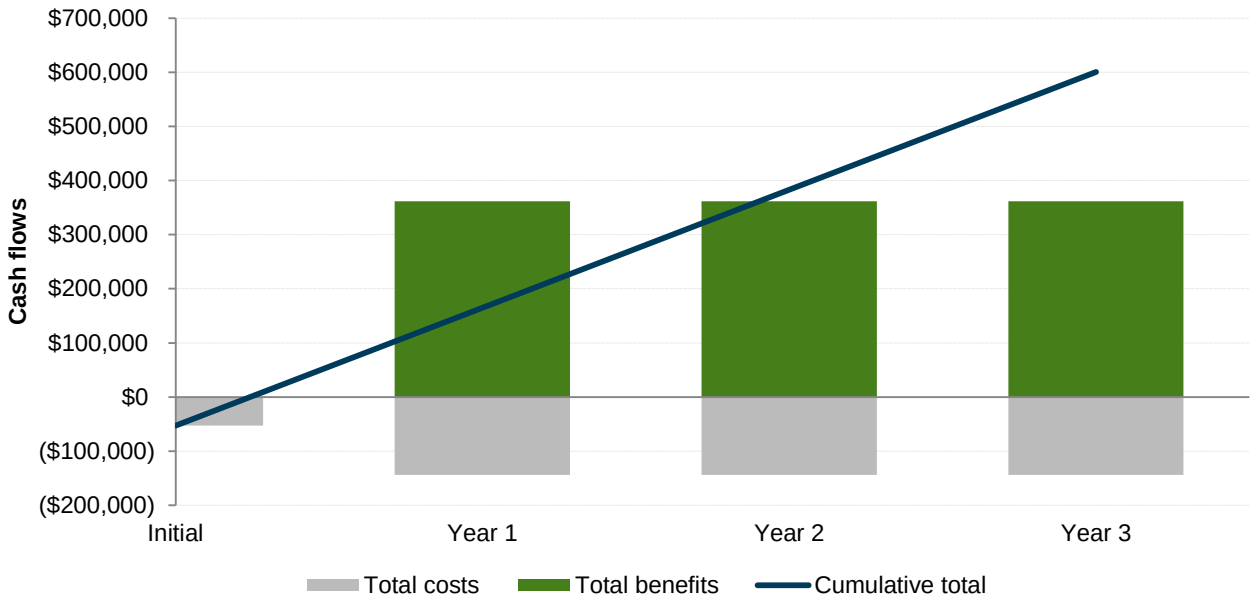
Table 8 shows the values used to adjust for risk and uncertainty in the cost and benefit estimates for the representative organization. Readers are urged to apply their own risk ranges based on their own degree of confidence in the cost and benefit estimates.

Financial Summary

The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the representative organization's investment in Veracode's application security testing services.

Table 9 below shows the risk-adjusted ROI, NPV, and payback period values. These values are determined by applying the risk-adjustment values from Table 8 in the Risks section to the unadjusted results in each relevant cost and benefit section.

FIGURE 6
Cash Flow Chart (Risk-Adjusted)



Source: Forrester Research, Inc.

TABLE 9
Cash Flow (Risk-Adjusted)

Summary	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($52,800)	($144,000)	($144,000)	($144,000)	($484,800)	($410,907)
Total benefits	$0	$381,930	$381,930	$381,930	$1,145,790	$949,803
Total	**($52,800)**	**$237,930**	**$237,930**	**$237,930**	**$660,990**	**$538,896**
ROI						**131%**
Payback period (months)						**2.7**

Source: Forrester Research, Inc.

Veracode application security testing: Overview

The following information is provided by Veracode. Forrester has not validated any claims and does not endorse Veracode or its offerings.

Veracode's cloud-based service and programmatic, policy-based approach deliver a simpler and more scalable solution for reducing global application-layer risk across web, mobile, and third-party applications. Recognized by leading analyst firms as an industry leader, Veracode secures hundreds of the world's largest global enterprises, including three of the top four banks in the Fortune 100 and more than 25 of the world's top 100 brands.

Veracode's key capabilities include:

- **A single cloud-based platform with multiple analysis techniques for optimum accuracy and coverage.** This includes SAST, DAST, behavioral analysis (for mobile applications), software composition analysis, and manual penetration testing. Veracode's centralized approach delivers a holistic view of application-layer threats across disparate business units and development teams — as well as across web, mobile, and third-party applications — using a single set of consistent policies, metrics, and reports.
- **Static application security testing (SAST).** Also known as "white-box" or "inside-out" testing, SAST finds common vulnerabilities by performing a deep analysis of your applications without actually executing them. Unique in the industry, Veracode's patented binary SAST technology analyzes all code — including third-party or open source components and libraries — without requiring access to source code. Binary static analysis works by analyzing binary code (rather than source code) to create a detailed model of the application's data and control paths. The model is then searched for all paths through the application that represent a potential weakness. For example, if a data path through the application originates from an HTTP request and flows through the application without validation or sanitization to reach a database query, then this would represent a SQL injection vulnerability.
- **Dynamic application security testing (DAST).** Also known as "black-box" or "outside-in" testing, DAST identifies architectural weaknesses and vulnerabilities in your running web applications before cybercriminals can find and exploit them. DAST uses the same approach used by attackers when probing the attack surface, such as deliberately supplying malicious input to web forms and shopping carts.
- **Behavioral analysis.** This dynamically analyzes a mobile application's real-time behavior, in a sandbox, to identify privacy and security violations such as data exfiltration to suspicious locations or access to sensitive data. This security intelligence is also integrated with mobile device management (MDM) solutions to enable enforcement of corporate bring-your-own-device (BYOD) policies. Veracode also provides a reputation service that publishes risk/security ratings for the most frequently downloaded apps from commercial app stores.
- **Web application discovery and monitoring.** Veracode's massively parallel, cloud-based discovery service provides visibility into all websites in your production infrastructure, including unknown sites you may not be aware of, such as external cloud-hosted sites, sites acquired via mergers and acquisitions, and temporary sites created by marketing agencies. It leverages an autoscaling cloud infrastructure to scan thousands of web applications simultaneously for the most exploitable vulnerabilities such as SQL injection and XSS. Unlike traditional network IP scanners, it uses a combination of advanced search techniques — such as DNS keyword searches, production-safe crawling, analysis of page redirects, and machine learning — to quickly identify unknown sites outside your normal corporate IP range. You can also feed security intelligence about specific vulnerabilities to your existing web application firewalls (WAFs) for rapid mitigation via virtual patching.
- **Enterprise policies that are based on the minimum acceptable levels of risk for applications according to their business criticality.** Risk is based on the severity of vulnerabilities identified in the application, using standards such as the OWASP top 10 (for web applications), the CWE/SANS top 25 (for nonweb applications), or compliance mandates such as PCI.

- **Analysis that is optimized for low false positives.** This analysis is prioritized based on severity so developers don't waste time on issues that don't matter.
- **Role-based access control (RBAC).** This provides granular, permission-based access to results and key performance indicators (KPIs) for all key stakeholders based on their roles — including development, security, and audit/compliance — for enhanced information sharing and continuous improvement across distributed organizations.
- **Support for Agile development processes.** Development teams are rapidly onboarded using proven and repeatable processes for tightly integrating security assessments — via rich application programming interfaces (APIs) — with Agile development processes and automated tools, including IDEs (Eclipse, Visual Studio, etc.), build processes (Jenkins, Ant, Maven, TFS, etc.), and issue tracking systems (JIRA, Bugzilla, Archer, etc.). In addition, the majority of assessments are completed in less than 4 hours, supporting overnight security assessments as an integral part of the daily build process.
- **Rapid remediation.** This is enabled by providing detailed and actionable information with line-of-code details to assist programmers in rapidly locating vulnerabilities in their source code and reproducing them, along with suggested corrective actions.
- **Compliance workflow automation.** Veracode's platform assesses applications for compliance with standard controls such as PCI, and policies can easily be customized to support specific corporate audit requirements as well as compliance requirements for SOX, HIPAA, NIST 800-53, MAS, and other mandates. Automated workflows reduce communication overhead as well as provide a secure audit trail of your approval processes, such as approvals for policy changes or mitigating controls (e.g., changes to WAF rules, operating system features, etc.) that temporarily remove the need to address vulnerabilities via code-level remediation.
- **Support of all widely used languages for desktop, web, and mobile applications**. This includes (note that this list is constantly being expanded):
  - Java and .NET.
  - C/C++: Windows, Linux, and Solaris.
  - Web platforms: J2EE, ASP.NET, Classic ASP, PHP, ColdFusion, and Ruby.
  - Mobile platforms: Objective-C for iOS, Java for Android, and J2ME for BlackBerry.
- **Vendor application security testing (VAST).** With VAST, enterprises are able to assess the security of vendor-supplied software without access to source code either through dynamic security testing (DAST) or through static binary analysis (SAST). Dynamic testing can be performed by the enterprises, while Veracode's binary static analysis technology, unique in the industry, allows independent software vendors to rapidly upload and test their compiled code without exposing their intellectual property and ultimately share the results of their security testing with their enterprise customers.
- **Mobile application reputation service.** This cloud-based directory and policy management service, accessible via APIs, provides detailed security intelligence about the most downloaded Android and iOS applications, including indicators related to exposing corporate intellectual property, data leakage of personally identifiable information (PII), transmitting data to suspicious geolocations, and hidden malware. This intelligence has also been integrated with widely used MDM solutions to enable enterprises to enforce corporate policies regarding applications downloaded to their employees' mobile devices.
- **Remediation coaching services.** These services help developers efficiently incorporate secure coding skills and practices into their existing development processes. Security experts are available on demand to respond to developer questions about assessment results, help prioritize remediation efforts, and provide guidance on code changes to quickly remediate vulnerabilities.

- **Security program management services.** These services enable the end-to-end success of global application security programs, in order to systematically reduce application-layer risk across the organization. Program managers leverage best practices to help you define the programs, policies, and KPIs focused on remediation so that actual improvements are made and organizational maturity increases, instead of simply encouraging check-box compliance; create appropriate engagement strategies for development teams and third-party vendors, encouraging key stakeholders to become supportive of the program; identify opportunities for process improvements, automation, and integration that can improve program effectiveness and scalability; and evaluate program health and revise program goals to remain aligned with enterprise strategy.
- **eLearning.** Veracode's eLearning service helps developers become proficient in secure coding practices. eLearning also helps organizations comply with PCI-DSS (Requirement 6.5) and industry standards such as ISO and the SANS Application Security Procurement Contract Language. Greater proficiency in secure coding skills means fewer security vulnerabilities in newly developed code and less time spent on remediation, enabling enterprises to securely innovate faster. Veracode gives enterprises a single cloud-based platform for developers to learn secure coding skills, test the code written with their new skills, and receive remediation coaching to reinforce those skills.
- **Manual penetration testing services.** These services add the benefit of specialized human expertise to automated binary static and dynamic analysis, using the same methodology cybercriminals use to exploit application weaknesses such as business logic vulnerabilities.
- **VerAfied and Scanned by Veracode:** Veracode enables software suppliers to communicate to their prospects and customers about the security of their products through VerAfied and Scanned by Veracode certifications. The VerAfied security mark signifies that a software provider has taken appropriate steps to remove vulnerabilities in its software or comply with respected industry standards such as the OWASP top 10 or the CWE/SANS top 25 most dangerous software errors. The Scanned by Veracode mark signifies that the software provider is leveraging Veracode in the development process of its software products.

Appendix A: Representative Organization Description

› For this TEI study, Forrester has created a representative organization to illustrate the quantifiable benefits and costs of implementing Veracode's application security testing services. The representative organization is based on characteristics of the interviewed customers and has the following characteristics:

- Is an independent software vendor.
- Has 1,000 employees, including 250 application developers.
- Has 500 business customers that buy its software.
- Has 20 applications in its current product portfolio, with 11 product updates made per year. About 15 are tested with Veracode each year.
- Has used Veracode for 10 months in full production.

› In purchasing Veracode, the representative organization had the following objectives:

- Reduce the time it takes to provide customers a quality response to application security questions.
- Reduce application security testing time and cost.
- Reduce compliance and auditing costs.
- Improve sales by highlighting application security as a competitive differentiator.

For the purpose of the analysis, Forrester assumes that benefits are captured linearly, so that unless otherwise highlighted, benefits across years 1, 2 and 3 are equal. Organizations that might need to consider a "ramp up" or "scale out" period should adjust benefits accordingly.

FRAMEWORK ASSUMPTIONS

Table 10 provides the model assumptions that Forrester used in this analysis. The discount rate used in the PV and NPV calculations is 10%, and the time horizon used for the financial modeling is three years. Organizations typically use discount rates between 8% and 16% based on their current environment. Readers are urged to consult with their respective company's finance department to determine the most appropriate discount rate to use within their own organizations.

TABLE 10
Model Assumptions

Ref.	Metric	Calculation	Value
F1	Hours per week, weeks per year, and hours per year (M-F, 9-5)	40*52	2,080
F2	Hours per year (24x7)		8,736
F3	IT admin fully burdened hourly rate	$82,500/2,080	$40
F4	Developer fully burdened hourly rate	$100,000/2,080	$48
F5	Information worker fully burdened hourly rate	$93,000/2,080	$45
F6	Discount rate (for NPV calculations)		10%

Source: Forrester Research, Inc.

Appendix B: Total Economic Impact™ Overview

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders. TEI assists technology vendors in winning, serving, and retaining customers.

The TEI methodology consists of four components to evaluate investment value: benefits, costs, flexibility, and risks.

BENEFITS

Benefits represent the value delivered to the user organization — IT and/or business units — by the proposed product or project. Often, product or project justification exercises focus just on IT cost and cost reduction, leaving little room to analyze the effect of the technology on the entire organization. The TEI methodology and the resulting financial model place equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization. Calculation of benefit estimates involves a clear dialogue with the user organization to understand the specific value that is created. In addition, Forrester also requires that there be a clear line of accountability established between the measurement and justification of benefit estimates after the project has been completed. This ensures that benefit estimates tie back directly to the bottom line.

COSTS

Costs represent the investment necessary to capture the value, or benefits, of the proposed project. IT or the business units may incur costs in the form of fully burdened labor, subcontractors, or materials. Costs consider all the investments and expenses necessary to deliver the proposed value. In addition, the cost category within TEI captures any incremental costs over the existing environment for ongoing costs associated with the solution. All costs must be tied to the benefits that are created.

FLEXIBILITY

Within the TEI methodology, direct benefits represent one part of the investment value. While direct benefits can typically be the primary way to justify a project, Forrester believes that organizations should be able to measure the strategic value of an investment. Flexibility represents the value that can be obtained for some future additional investment building on top of the initial investment already made. For instance, an investment in an enterprisewide upgrade of an office productivity suite can potentially increase standardization (to increase efficiency) and reduce licensing costs. However, an embedded collaboration feature may translate to greater worker productivity if activated. The collaboration can only be used with additional investment in training at some future point. However, having the ability to capture that benefit has a PV that can be estimated. The flexibility component of TEI captures that value.

RISKS

Risks measure the uncertainty of benefit and cost estimates contained within the investment. Uncertainty is measured in two ways: 1) the likelihood that the cost and benefit estimates will meet the original projections and 2) the likelihood that the estimates will be measured and tracked over time. TEI risk factors are based on a probability density function known as "triangular distribution" to the values entered. At a minimum, three values are calculated to estimate the risk factor around each cost and benefit.

Appendix C: Glossary

Independent software vendor (ISV): ISVs make and sell software products that run on one or more computer hardware or operating system platforms.

Discount rate: The interest rate used in cash flow analysis to take into account the time value of money. Companies set their own discount rate based on their business and investment environment. Forrester assumes a yearly discount rate of 10% for this analysis. Organizations typically use discount rates between 8% and 16% based on their current environment. Readers are urged to consult their respective organizations to determine the most appropriate discount rate to use in their own environment.

Net present value (NPV): The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made, unless other projects have higher NPVs.

Present value (PV): The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.

Payback period: The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

Return on investment (ROI): A measure of a project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits minus costs) by costs.

A NOTE ON CASH FLOW TABLES

The following is a note on the cash flow tables used in this study (see the example table below). The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1. Those costs are not discounted. All other cash flows in years 1 through 3 are discounted using the discount rate (shown in the Framework Assumptions section) at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations are not calculated until the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

TABLE [EXAMPLE]
Example Table

Ref.	Metric	Calculation	Year 1	Year 2	Year 3

Source: Forrester Research, Inc.

Appendix D: Supplemental Material

Related Forrester Research

"The Total Economic Impact™ Of Veracode's Cloud-Based Application Security Service," Forrester Consulting report prepared for Veracode, July 2014.

Appendix E: Endnotes

[1] Forrester risk-adjusts the summary financial metrics to take into account the potential uncertainty of the cost and benefit estimates. For more information, see the section on Risks.

[2] Verizon Data Breach Investigations Report (http://www.verizonenterprise.com/DBIR/).