A Forrester Total Economic Impact™ Study

Commissioned By

Veracode

Project Director:
Sean Owens

July 2014

The Total Economic Impact™ Of Veracode's Cloud-Based Application Security Service

Avoided Costs, Cost Savings, And Business Benefits Enabled By Veracode Application Security

FORRESTER®

Table Of Contents

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.

Executive Summary

Veracode commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Veracode's cloud-based application security service. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of the solution on their organizations, and to describe best practices for implementing enterprisewide governance programs for reducing application-layer risk.

> **"Veracode has helped us scale our program significantly, and it also helps us set our priorities correctly. We can focus on the optimal strategy, policies, and KPIs to systematically reduce enterprise risk."**
>
> **— Head of application security, financial services organization**

To better understand the benefits, costs, and risks associated with Veracode's application security service, Forrester interviewed a current customer — a Global 2000 financial services organization with multiple years of experience using the service to identify vulnerabilities in its code and measure the quality of its outsourced application development partners.

Prior to using Veracode's service, the firm had implemented a traditional on-premises scanning tool. Success was limited because the tool was complex and required specialized in-house expertise to configure it and interpret its results; in addition, scanning and remediation were performed in a more ad hoc manner rather than using a consistent process with standardized policies and metrics. As a result, the organization was only able to perform security assessments on a fraction of the applications it should be assessing for risk in its portfolio of several thousand applications. Extra costs were incurred when outsourcers delivered code with vulnerabilities that needed to be tracked, mitigated, and eventually remediated.

With Veracode's cloud-based service, combined with its remediation coaching and program management services, the organization was able to significantly scale its application security program. In particular, the program continuously assesses about 400 of the firm's business-critical applications and is finding vulnerabilities earlier in the software development life cycle (SDLC). This has significantly reduced enterprise risk and has avoided vulnerability management and remediation costs. The quality of its internal and outsourced code has also improved, as developers have benefited from the ongoing coaching and training in secure coding practices by Veracode security experts. The organization estimates it has also avoided costs by replacing manual testing of internally developed and legacy code with automated code assessments. The organization estimates that matching Veracode's application portfolio coverage would require significant expansion of its previous on-premises solution, as well as a number of additional people. "I don't think that we would have been able to expand the program [that we had before Veracode] to the point that we have now, due to the added complexity of our legacy application estate. We would have needed to add 15 FTEs to the team," said the head of application security at the organization.

VERACODE HELPS REDUCE APPLICATION-LAYER RISK WHILE REDUCING COSTS

Forrester's financial analysis, based on the organization interview and other research, estimates the risk-adjusted ROI and benefits, shown in Figure 1.[1] The analysis points to annual benefits of about $6.6 million to $7.6 million per year versus up-front costs of $1.6 million as part of a three-year present-value (PV) total cost of nearly $6 million. These add up to a three-year net present value (NPV) of nearly $12 million.

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

ROI:
192%

NPV:
$11,522,027

Application vulnerabilities:
↓ 60%

Source: Forrester Research, Inc.

- **Benefits.** The interviewed organization estimates the following risk-adjusted benefits:
  - **Avoided costs of $1.98 million per year in identifying, tracking, and mitigating vulnerabilities in applications developed by outsourced developers.** The organization and its outsourced developers can now identify vulnerabilities earlier in the SDLC and avoid the overhead and complexity of logging and tracking vulnerabilities for later remediation in the next application update (and mitigating them in the meantime where possible), thereby reducing retesting time and overhead costs. In addition, code quality has improved by around 60% (as measured by the number of vulnerabilities identified per megabyte of code).
  - **Avoided costs of $3 million per year in assessing internally developed and legacy applications.** The firm uses a number of legacy applications that are critical to the business and connect to sensitive data sources, but for which it is often impossible to obtain source code. Veracode's binary static analysis (SAST) assesses binaries without requiring access to source code. As a result, it is faster and 75% less expensive to identify vulnerabilities and remediate legacy applications earlier in the SDLC, compared with the manual testing approach that was previously used on applications after development had been completed.
  - **Improved development skill, speed, and best practices leading to reduced costs and improved margins totaling $976,200 to $1,952,400 per year.** Applications are now delivered to the business more quickly — without sacrificing security — which can lead to significant additional revenue and profit as applications are launched earlier.
  - **Avoided costs of $630,000 per year related to reduced application security risk.** Application-layer security vulnerabilities can lead to major breaches. Reducing the chance of application-related threats such as a successful cyberattack made possible by a SQL injection (SQLi) or a cross-site scripting (XSS)-related vulnerability — which can lead to theft of the firm's intellectual property or customer data — can mean significant avoided costs, risk reduction, and avoided lost revenue.
- **Costs.** The interviewed organization estimates the following risk-adjusted costs:
  - **Up-front costs of $1,624,000 and annual resource and software licensing and services fees of $840,000 to $2,154,000 per year.** This includes Veracode's subscription-based software, services, training, and support costs, as well as implementation and ongoing costs other than Veracode license costs, such as internal resource costs dedicated to the implementation and management of the Veracode service and associated processes.

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 service.
- 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 name for the interview but did not participate.

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 service. The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision.

APPROACH AND METHODOLOGY

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

- Interviewed Veracode consulting and other personnel, along with Forrester analysts, to gather data relative to the current state of application security and how enterprises are implementing global application security programs.

- Interviewed a Global 2000 organization currently using Veracode to obtain data with respect to costs, benefits, and risks.

- Constructed a financial model based on the interview using the TEI methodology. The financial model is populated with the cost and benefit data obtained from the interview.

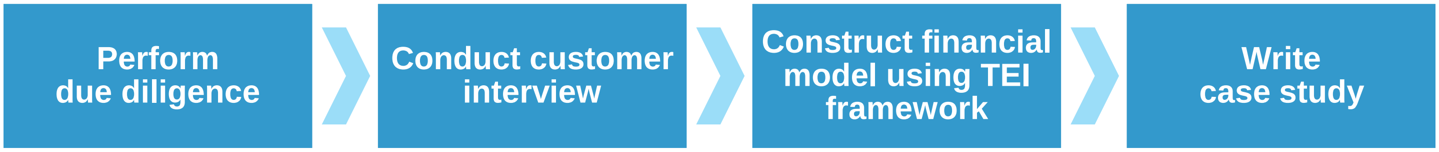
- Risk-adjusted the financial model based on issues and concerns the interviewed organization highlighted in the interview. Risk adjustment is a key part of the TEI methodology. While the interviewed organization provided cost and benefit estimates, some categories included a number of outside forces that might have affected the results. For that reason, some cost and benefit totals have been risk-adjusted for conservatism, as detailed in each relevant section.

Forrester employed four fundamental elements of TEI in modeling Veracode's application security 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 A for additional information on the TEI methodology.

FIGURE 2

TEI Approach


Perform due diligence
Conduct customer interview
Construct financial model using TEI framework
Write case study

Source: Forrester Research, Inc.

Analysis

ORGANIZATION

For this study, Forrester conducted an interview with representatives from a Veracode customer working in the financial services industry. The organization is based in Europe but doing business worldwide.

Based on this interview, Forrester constructed a TEI framework and an associated ROI analysis that illustrates the areas financially affected.

After careful consideration of alternate solutions, including a potential expansion of its existing on-premises scanning tool, the organization chose Veracode's cloud-based platform and program management service in 2010 and began implementation with both internal developers and outsourced development partners. The organization:

- Reviewed its application portfolio of more than 3,000 individual applications from a variety of sources (including vendor-developed commercial applications, internally developed custom applications, partner-developed custom applications, and open source applications) and prioritized the top 400 for immediate security assessment, as well as the next group to be covered as the program expanded. These applications included legacy applications from a variety of sources, as well as newer applications primarily developed by outsourcing partners.
- Used Veracode's binary SAST — also known as "white box" or "inside out" testing — to assess the most business-critical applications, and immediately uncovered (and fixed) a number of critical vulnerabilities such as SQLi and XSS issues that can be easily discovered and exploited by cyberattackers.
- Expanded testing to include dynamic analysis (DAST) — also known as "black box" or "outside in" testing — to identify vulnerabilities in public-facing web applications after they have been deployed in production, and also in preproduction quality assurance (QA). For better accuracy and coverage, Veracode provides both static and dynamic analysis on a single platform.
- Continues to assess new applications and frameworks for newly discovered vulnerabilities and threat vectors. Veracode's cloud-based platform is continuously learning as it performs new scans, and new assessment rules are constantly being added to the platform.
- Continues to work with internal and partner development resources to communicate and train development best practices, which helps improve application security and speed up future assessment and development processes.
- Continues to work with Veracode to evaluate its policies and key performance indicators (KPIs), benchmark its security posture against peers, and enhance its development processes.

INTERVIEW HIGHLIGHTS

The interviewed organization shared details about its use of Veracode's service, as well as some of the reasons it chose Veracode.

Situation

Before deployment, the organization faced a number of risk and cost challenges, but foremost was the realization that the firm did not have visibility into the security of all its top business-critical applications, thereby increasing enterprise risk.

> *"When you look over the last three years, the quality of code for each developer, including outsourced developers, has improved consistently and significantly."*
>
> ~ Head of application security, financial services organization

There were also cost issues. The firm was spending extra time and money, as it often took several weeks (or longer) to identify vulnerabilities in applications, usually after the software project was complete, which meant the vulnerability would have to be logged and tracked to be included in the next application update and often required significant extra costs to mitigate and then retest.

Solution

The organization selected Veracode's cloud-based service because it could scale to address all of the firm's business-critical applications — including applications from outsourcers — while providing on-demand developer coaching and training to continuously improve quality and embed security into the entire software development life cycle.

> *"Veracode has been essential in identifying and prioritizing the risks in our application portfolio."*
>
> ~Head of application security, financial services organization

Results

Since its initial Veracode implementation in 2010, the organization has seen significant improvements in its application security processes while also saving costs related to:

- **Tracking vulnerabilities in outsourced code.** Outsourcers are now responsible for assessing their applications themselves before delivering them to the organization. They are given direct access to Veracode's cloud-based service, along with clear requirements from the organization about minimum acceptable security standards (e.g., OWASP Top 10, CWE/SANS Top 25, etc.). This avoids the extra time and complexity the organization would otherwise incur to manage, track, and mitigate vulnerabilities in outsourced applications after they have been delivered. In addition, vulnerability counts are reduced as outsourced developers learn secure coding practices from Veracode experts.

- **Remediating vulnerabilities in internally developed applications and legacy code.** Identifying vulnerabilities earlier in the SDLC avoids significant remediation costs for both internally developed applications and for legacy code that is often integrated with internally developed applications. Also, Veracode's patented, binary SAST technology assesses binaries rather than source code, which is especially helpful when source code is no longer available for legacy code. Vulnerabilities are then remediated by developers (if available), mitigated with a web application firewall or other external security control, or the code is decommissioned entirely.

- **Improved development skill, speed, and best practices.** Automated assessments and cleaner code mean secure applications are delivered to the business more quickly, leading to additional revenue or cost savings for the business. In addition to the cloud-based training provided by Veracode, developers work directly with Veracode experts to learn best practices and improve their skills on the job. In particular, they regularly leverage in-depth "remediation guidance calls" with Veracode experts to better understand their assessment results and optimize remediation and mitigation efforts.

- **Reduced risk from application-layer breaches.** By producing more secure applications, the firm is reducing the risk and hence the potential costs of an application-layer breach. If sensitive company or customer data is involved, the brand impact and costs of a breach can be extremely significant. Veracode's cloud-based service and best practices help identify vulnerabilities early so they can be fixed or distanced from sensitive data.

BENEFITS

The organization has estimated and continues to expect a number of quantified benefits in this case study:

- Avoided costs from identifying, tracking, and mitigating vulnerabilities in applications produced by outsourced developers (and avoiding the long wait and time spent on possible mitigation tasks between identification of vulnerabilities and development of the next application version). This also helps incent outsourcers to reduce the number of vulnerabilities in their code. To increase code quality, the organization provided developers with cloud-based access to Veracode's automated assessment and remediation coaching services.

- Avoided costs from identifying and remediating vulnerabilities in internally developed and legacy applications, achieved by replacing manual testing with automated assessments that now occur earlier in the SDLC rather than at the end of each development cycle.

- Improvements in development best practices leading to faster delivery of critical applications to the business (without sacrificing security).

- Costs avoided by reducing the risk of a major application-layer breach.

> *"We gave our outsourced developers a set of security requirements plus direct access to Veracode's automated service. As a result, they now have the right people and processes integrated into their development cycles to make sure their code is clean when they present it for delivery."*
>
> ~Head of application security, financial services organization

⊕ Reduction In Vulnerability Management Costs For Applications Developed By Outsourced Developers

The organization contracts the development of custom applications, either as standalone web applications or as integration layers or add-ons to third-party software applications. The organization develops approximately one-third of its own applications with an internal development and testing team of 250 full-time equivalents (FTEs); the remaining majority are outsourced to a handful of global outsourced development partners.

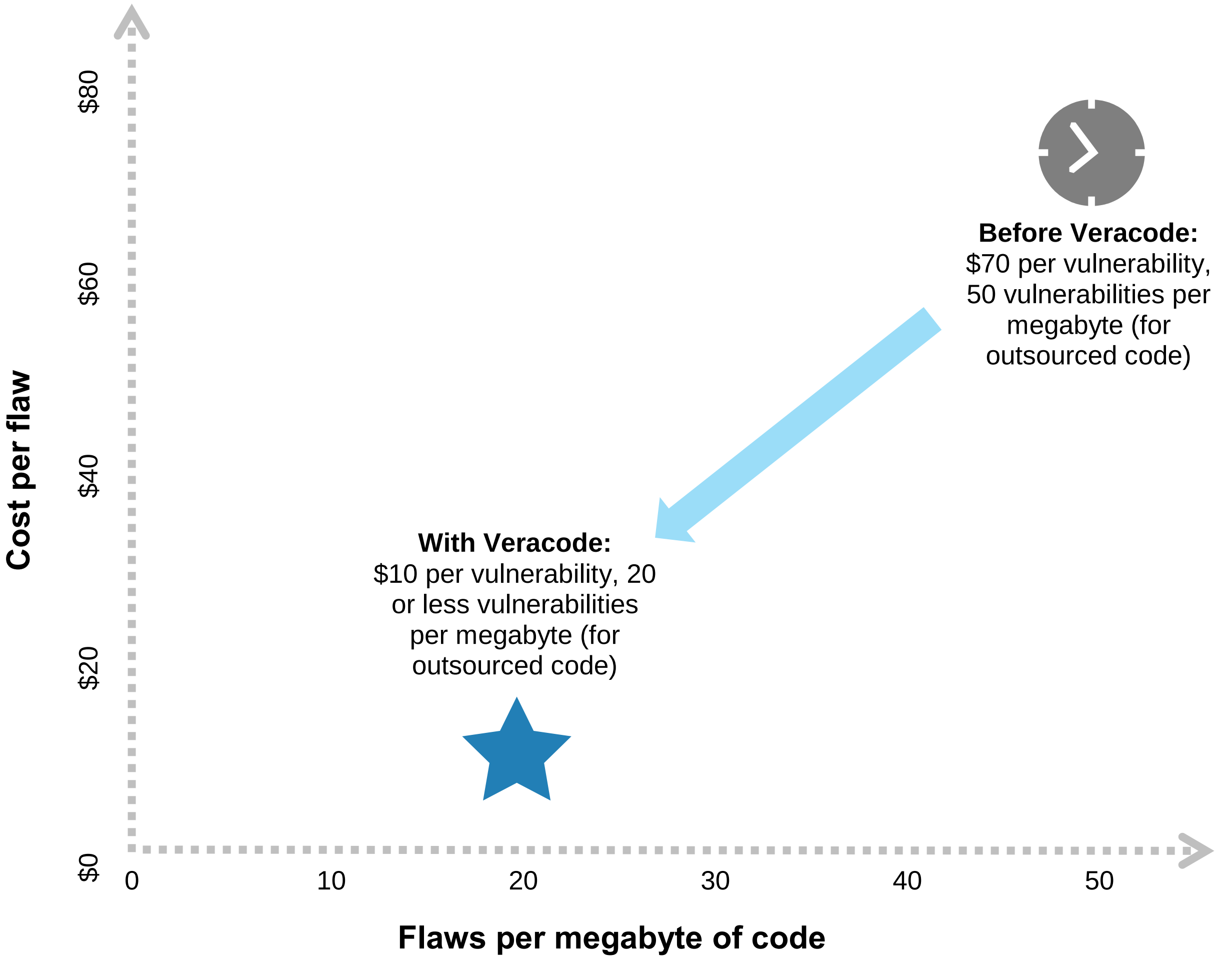
In the past, the organization would initiate a project to develop a new or upgraded application. The organization found that its internal assessment processes were just too slow and that unnecessary costs were piling up. When a vendor delivered an application to the organization, the application would typically be accepted after minimal security testing — but if a vulnerability was discovered after the code warranty period (either by chance or by later application testing processes), remediation changes would have to wait until the next application update. That meant vulnerabilities needed to be identified, logged, tracked, and then once remediated, reassessed — adding complexity and overhead. Time was also often required to set up mitigating controls to work around more severe vulnerabilities until the application was fixed.

For externally developed applications, if outsourcers can check their code themselves for easily exploitable security vulnerabilities — before delivering the application to the organization — they can deliver code that has already been independently assessed to meet the organization's minimum security standards, thereby avoiding the added costs of catching vulnerabilities later in the SDLC. The outsourcers also benefit — they are better off making sure they focus on meeting client requirements for delivered code, avoid the extra cost around remediation in the next release, and spend more time on more profitable core development tasks.

Veracode helped reduce the overhead of managing vulnerabilities, while also helping reduce the total number of vulnerabilities, as detailed for outsourced-developed code in Figure 3. The organization estimates that before implementing Veracode, outsourced applications contained about 100 vulnerabilities per 2 megabytes (MB) of code (the average size of an application). Each vulnerability cost the organization around $70 (on average) in internal resource time to manage, mitigate, and track (as detailed above).

Since implementing Veracode, the cost per vulnerability to the organization is much lower, because outsourced developers now have direct access to Veracode's cloud-based platform to perform automated assessments of their code, while the platform itself tracks risk-related KPIs and the status of all vulnerabilities in outsourced code (e.g., remediated, mitigated, or open). The organization's internal security team has full and immediate visibility into these KPIs and status information via the platform.

FIGURE 3
Application Security Improvements



Before Veracode: $70 per vulnerability, 50 vulnerabilities per megabyte (for outsourced code)

With Veracode: $10 per vulnerability, 20 or less vulnerabilities per megabyte (for outsourced code)

Source: Forrester Research, Inc.

In addition, vulnerability counts have been reduced to only 40 per 2 MB of outsourced code, because developers can now leverage actionable line-of-code-level results from the platform to quickly locate and prioritize fixes. Outsourcers also use Veracode's on-demand coaching services for assistance in remediating vulnerabilities before delivering their code (and while not shown in Table 1, vulnerability counts are expected to reduce further as developers continue learning secure coding practices).

Also, as a result of the organization's detailed acceptance criteria and Veracode's automated tracking of vulnerability metrics, the outsourcer is now incentivized to focus on application security and drive up its quality metrics. As part of its service, Veracode provides a program manager who helps the organization define clear, policy-based requirements for developers, based on best practices for implementing enterprisewide governance programs. These requirements are easy to follow and learn from, incenting developers to assess their code often and avoid past mistakes in order to complete projects more quickly and with fewer vulnerabilities.

The organization estimates it contracts the development of about 200 new or updated applications from its development outsourcers. It expects it could avoid around $2.6 million per year in vulnerability management, tracking, and mitigation costs. Since there are a number of assumptions and external influences included in these estimates (such as the partner's performance and new types of application security issues that might be discovered and exploited in the future), these benefits have been risk-adjusted by 25%. The risk-adjusted benefit is about $2 million per year, as shown in Table 1. See the Risks section for more details on risk adjustment as part of the TEI methodology.

TABLE 1

Avoided Overhead Costs And Reduced Number Of Vulnerabilities For Outsourced Application Development

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
A1	Number of nonlegacy, business-critical applications developed by outsourcers that are assessed	Estimate	200		
A2	Average MB of code per application	Estimate	2		
A3	Number of vulnerabilities per MB of code from outsourcers (on average) before Veracode	Assumption	100		
A4	Number of vulnerabilities per MB of code from outsourcers (on average) since Veracode	Estimate	40		
A5	Cost per vulnerability before Veracode, to log, manage, track, and mitigate (as needed)	Assume about 1.5 hours	$70		
A6	Cost per vulnerability with Veracode	Assume about 10 to 15 minutes	$10		
At	Avoided overhead costs and reduced number of vulnerabilities for outsourced application development	A1*A2*(A3*A5-A4*A6)	$2,640,000	$2,640,000	$2,640,000
	Risk adjustment	↓ 25%			
Atr	**Avoided overhead costs and reduced number of vulnerabilities for outsourced application development (risk-adjusted)**		**$1,980,000**	**$1,980,000**	**$1,980,000**

Source: Forrester Research, Inc.

⊕ Avoided Costs From Assessing And Remediating Internally Developed And Legacy Applications

The organization also supports a number of legacy applications, many of which are critical to the business and access sensitive data sources. Of the 3,000 applications in the organization's portfolio, many are internally developed and/or legacy applications. A large number will be retired soon, but about 200 applications are considered business-critical and were prioritized for security assessments.

For internally developed applications, developers can produce code and quickly assess that it meets minimum security standards, thereby avoiding the added costs of catching vulnerabilities later in the SDLC.

With legacy applications, it is not always possible to review source code (or in some cases even ask the developer for help) to find and remediate vulnerabilities. With Veracode's patented binary static analysis technology, organizations can assess the security of legacy applications without having access to source code (they can also assess third-party software such as commercial off-the-shelf applications and third-party libraries). If product support is available, the vendor might help by developing a patch, though in many cases static analysis will identify insecure applications that should be decommissioned, replaced, or protected via compensating controls. For example, the organization has set up web application firewalls (WAFs) around legacy applications to help secure these applications when it no longer has access to source code.

The organization previously assessed and remediated internally developed applications and legacy code via manual tests performed by users at the end of each development cycle. The organization estimates that using this approach to identify vulnerabilities and then remediate applications later in the SDLC could cost as much as $40,000 per application. With Veracode's automated assessments occurring earlier in the SDLC, those same tasks could cost $10,000 or less per application per year. As shown in Table 2, this adds up to annual avoided costs of about $6 million per year. There are a number of other factors that can affect these estimates, so a 50% risk adjustment has been applied; the risk-adjusted avoided costs are about $3 million per year. See Table 2 for more detail, and the Risks section for more information on risk adjustment as part of the TEI methodology.

TABLE 2

Avoided Costs For Assessing And Remediating Vulnerabilities In Internally Developed And Legacy Applications

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
B1	Cost to manually assess and remediate an application at the end of each development cycle (before Veracode)	Estimate	$40,000		
B2	Cost to perform automated assessments and remediate an application early in the SDLC (with Veracode)	Estimate	$10,000		
B3	Internal and legacy applications to be assessed in a given year	Estimate	200		
Bt	Avoided costs for assessing and remediating internally developed and legacy applications	B3*(B1-B2)	$6,000,000	$6,000,000	$6,000,000
	Risk adjustment	↓ 50%			
Btr	**Avoided costs for assessing and remediating internally developed and legacy applications (risk-adjusted)**		$3,000,000	$3,000,000	$3,000,000

Source: Forrester Research, Inc.

✪ Improvements In Development Best Practices

In addition to lowering costs by helping reduce vulnerabilities, Veracode helps developers learn how to deliver secure applications more quickly. Veracode provides training and support by security experts, including on-demand remediation guidance calls that help developers understand their assessment results, prioritize remediation activities, develop strategies for rapid remediation, and complete projects more quickly.

The Veracode platform pinpoints vulnerabilities to specific lines of code, which can then be viewed within the developer's native integrated development environment (IDE) and provides actionable, in-context explanations about vulnerabilities found, explaining, for example, "What is a SQL injection vulnerability?" and "What is the best way to remediate it?" Once remediated, applications can quickly be reassessed to validate fixes. Veracode also provides a dedicated program manager to help the organization establish consistent policies, metrics, and reporting across global development teams, thereby leading to continuous improvement in code quality.

All these improvements help the organization gain small (but important) improvements in delivering secure applications to the business more quickly. If the quicker time-to-market of customer- or sales-facing applications could influence a small percentage (even just 1%) of incremental profit, then delivering those applications even a couple of weeks ahead of schedule could add up significantly. Incremental profit would be realized from direct revenue-generating web applications or applications that help influence revenue increases (such as a sales tool that provides new or improved cross- and up-sales recommendations). The organization expects to achieve about $1.6 million in improved time-to-market profit in the first year, growing to more than $3.2 million as development skills and time-to-market improve.

Given that these improvements, especially revenue- and profit-related benefits, are influenced by far more than just how Veracode is used in the organization, a risk adjustment of 40% has been applied. The risk-adjusted annual benefits range from about $975,000 to $2 million per year, as detailed in Table 3. See the Risks section for more information on risk adjustment as part of the TEI methodology.

TABLE 3
Development Improvements Leading To Increased Revenue And Profit

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
C1	Improved time-to-market benefit (profit)	Estimate of 2 to 4 weeks of profit	$1,627,000	$2,440,000	$3,254,000
Ct	Development improvements for delivering applications to the business faster and more securely	C1	$1,627,000	$2,440,000	$3,254,000
	Risk adjustment	↓ 40%			
Ctr	**Development improvements for delivering applications to the business faster and more securely (risk-adjusted)**		**$976,200**	**$1,464,000**	**$1,952,400**

Source: Forrester Research, Inc.

✪ Avoided Costs From Reduced Risk

As a global enterprise working in the financial sector, the organization thinks about risk and considers it an important factor in most business decisions. While the avoided costs detailed above were important drivers behind choosing Veracode, reducing the organization’s risk exposure — and associated potential costs — was the key factor in choosing and implementing Veracode.

The risk avoidance analysis focuses on major potential issues where data could be exposed because of an application-layer breach. These are significant and costly events that could lead to the loss of sensitive customer data or corporate intellectual property information; broad, lasting outages that interrupt ongoing operations; or other events that can have a severe impact on revenue, costs, and customer satisfaction.

(It’s important to note that next-generation firewalls and intrusion detection and/or intrusion prevention (IDS/IPS) systems are typically unable to prevent application-layer breaches because public-facing web applications are specifically designed to allow access from the outside world to corporate and customer data.)

It’s assumed that the organization has relatively mature security policies with modern firewalls and IDS/IPS systems; maintains up-to-date malware protection across all servers and user devices; keeps software up-to-date and refreshes hardware regularly; has documented data management processes for sensitive data; and uses Veracode to assess critical applications that access sensitive data. So for a company of this size and overall security maturity, research conducted by several organizations has estimated that the cost of a single lost or exposed sensitive data record is about $200, that a data breach could affect as many as 100,000 records, and that the chance of a major breach happening in any given year is about 10%.[2] (In other words, using these assumptions, a major data breach would be expected to happen about once every 10 years and could result in $20 million in remediation, cleanup costs, cost to brand image, lost customers, and loss in shareholder value.) Over the long run, the average potential cost of a data breach caused by an application-layer vulnerability can be estimated by multiplying the likelihood of a breach occurring by the cost per exposed record by the total number of exposed records. This would further be segmented by the probability that a data breach was the result of an application-layer vulnerability (which, for a financial services firm with many customer-facing transactional applications and strong security controls at the network layer and other layers, is very high).

The organization expects that this risk can be significantly reduced with Veracode. The expected annual cost avoidance is about $700,000 per year as shown in Table 4. Given the variability of these estimates, a 10% risk reduction has been applied. The risk-adjusted annual cost avoidance is more than $630,000 per year.

TABLE 4
Avoided Costs From Reduced Risk

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
D1	Cost of a major data security issue	External research	$20,000,000	$20,000,000	$20,000,000
D2	Estimated share of data breaches caused by application security issues	External research	50%	50%	50%
D3	Chances of a major security issue in a given year	External research	10.0%	10.0%	10.0%
D4	Application security risk reduction with Veracode	Assumption	70%	70%	70%
Dt	Risk cost avoidance	D1*D2*D3*D4	$700,000	$700,000	$700,000
	Risk adjustment	↓ 10%			
Dtr	**Risk cost avoidance (risk-adjusted)**		**$630,000**	**$630,000**	**$630,000**

Source: Forrester Research, Inc.

TOTAL BENEFITS

Table 5 shows the total of all benefits across the five areas listed above, as well as present values (PVs) discounted at 10%. Over three years, the organization expects total risk-adjusted benefits to represent a PV of more than $17 million.

TABLE 5
Total Benefits (Risk-Adjusted)

Ref.	Benefit	Year 1	Year 2	Year 3	Total	Present Value
Atr	Avoided overhead costs and reduced number of vulnerabilities for outsourced application development	$1,980,000	$1,980,000	$1,980,000	$5,940,000	$4,923,967
Btr	Avoided costs for assessing and remediating internally developed and legacy applications	$3,000,000	$3,000,000	$3,000,000	$9,000,000	$7,460,556
Ctr	Development improvements for delivering applications to the business faster and more securely	$976,200	$1,464,000	$1,952,400	$4,392,600	$3,564,239
Dtr	Risk cost avoidance	$630,000	$630,000	$630,000	$1,890,000	$1,566,717
	Total benefits (risk-adjusted)	**$6,586,200**	**$7,074,000**	**$7,562,400**	**$21,222,600**	**$17,515,479**

Source: Forrester Research, Inc.

COSTS

The organization experienced the following costs associated with Veracode's application security service:

- Veracode license, training, and support costs.
- Implementation costs
- Ongoing management resource costs.

These represent the costs experienced by the organization for initial planning, implementation, licensing, and ongoing management associated with Veracode.

$ Veracode Implementation, Annual Resource, Licensing, Training, and Support Costs

The organization estimates its Veracode deployment took about two months to complete and required some FTEs from the application security team.

The organization licenses Veracode's cloud-based service based on the total number of applications to be assessed. Veracode's model allows for an unlimited number of assessments for each application, so that developers are encouraged to assess their code as often as possible, such as whenever remediation changes or other changes are implemented.

There is an additional annual fee for a dedicated program manager, whose role is to help the organization implement enterprisewide governance programs with consistent policies, metrics, and reporting in order to continuously reduce application-layer risk across its development teams (including outsourcing partners). Program managers also help the organization track its use of Veracode services and its progress over time in achieving continuous improvement.

Technical support is also charged separately. Veracode provides on-demand remediation guidance calls (also called "readout calls") to help developers understand assessment results and optimize remediation efforts. The organization also takes advantage of Veracode eLearning offerings, also priced separately, to provide partners with online training.

License and resource costs dependent on the organization size, licensing scope, and other factors, and in particular resource costs can vary as salaries change and higher-than-expected turnover may require more training costs. To include these risks in the assessment, a 20% risk factor has been added. Table 6 shows the total of all costs as well as associated present values, discounted at 10%. Over three years, the organization expects risk-adjusted total costs to total a net present value of nearly $6 million. See the Risks section for more information on risk adjustment as part of the TEI methodology.

TABLE 6
Total Costs (Risk-Adjusted)

Cost	Initial	Year 1	Year 2	Year 3	Total	Present Value
Veracode implementation and annual costs (risk-adjusted)	**($1,624,000)**	**($2,154,000)**	**($2,154,000)**	**($840,000)**	**($6,772,000)**	**($5,993,452)**

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 Veracode's application security service 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 A).

Implementing VAST

Another key area of future benefits is the Vendor Application Security Testing (VAST) program that Veracode provides for reducing risk from commercial off-the-shelf (COTS) applications. With this program, Veracode works with the organization to set policies, metrics, and reporting processes that third-party commercial vendors must meet to do business with the enterprise. Veracode then works directly with each of the organization's third-party vendors — on an outsourced basis — to assess their code, remediate it, and enhance their development and testing processes, including providing training in secure coding practices to these vendors.

> *"VAST is another way we can work with our application providers to align our security and commercial objectives. VAST will be critical to scale our assurance program and lower the risk from packaged applications."*
>
> ~ Head of application security, financial services organization

This organization has just started its VAST program with Veracode and expects to see a significant reduction in third-party software risk in the future.

Avoiding Costs By Not Expanding Previous On-Premises Scanning Tool

A third area the organization identified is the costs avoided by not having to expand its previous on-premises scanning tool (from a major IT vendor), to achieve the same level of scale as it has obtained from Veracode's cloud-based service.

This savings was excluded from the cost/benefit analysis above because that would have double-counted both the cost avoidance gained by not expanding the previous solution *and* the benefits gained from replacing it with Veracode's cloud-based service.

The organization estimated that expanding its on-premises solution to match Veracode's scale would require doubling its existing software and hardware implementation — as well as require hiring 15 additional resources, including five consultants, to manage the program.

The total cost avoidance, including hardware, software, and maintenance costs for an expanded installation, plus additional people resources, amounts to an NPV of more than $5 million over three years. If included above, these totals would have been risk-adjusted, but the total cost avoidance would still be more than $4 million per year.

> *"I don't think that we would have been able to expand the program [that we had before Veracode] to the point that we have now, due to the added complexity of our legacy application estate. We would have needed to add 15 FTEs to the team."*
>
> ~Head of application security, financial services organization

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 Veracode application security service 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.

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:

- Cost reductions from identifying and remediating vulnerabilities in outsourced applications, internally developed applications, and legacy code can be attributed to more than just Veracode; while a major driver of benefits and process changes, some process changes could have been implemented without Veracode.
- Enhancements in development best practices, particularly additional revenue and profit gained by faster delivery of applications to the business, are variable and very hard to estimate.
- Risk avoidance is, obviously, a very volatile metric based on a number of externalities (as well as individual organization needs).

The following implementation risk that affects costs is identified as part of this analysis:

- Resource, licensing, training and support costs are often variable and hard to estimate several years in advance.

Table 7 shows the values used to adjust for risk and uncertainty in the cost and benefit estimates. Readers are urged to apply their own risk ranges based on their own degree of confidence in the cost and benefit estimates.

TABLE 7
Benefit And Cost Risk Adjustments

Benefits	Adjustment
Avoided costs for internal and outsourced application development resources	↓ 25%
Cost avoidance for legacy and internally developed applications	↓ 50%
Development best practices	↓ 40%
Avoided costs from reduced risk	↓ 10%

Costs	Adjustment
Implementation and annual costs, including resources, ongoing licenses, training and support costs	↑ 20%

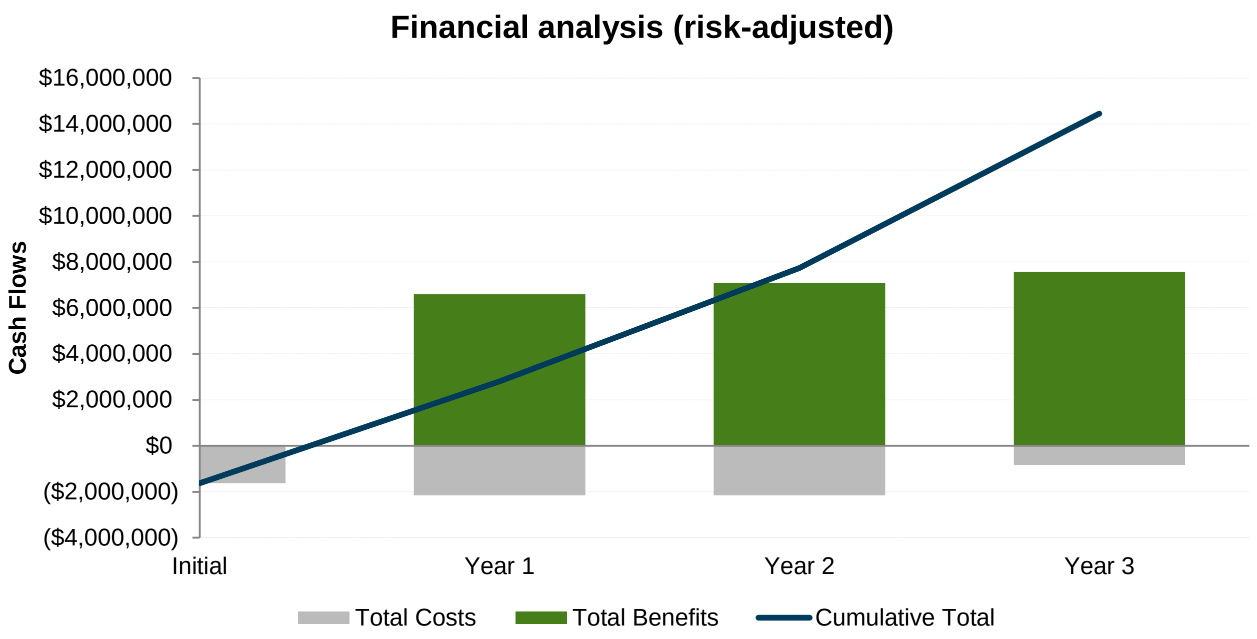
Source: Forrester Research, Inc.

Financial Summary

The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and cash flow for the organization's investment in Application Security.

Table 8 and Figure 4 show the risk-adjusted ROI, NPV, and cash flow values. These values are determined by applying the risk-adjustment values from Table 7 in the Risks section to the unadjusted results in each relevant cost and benefit section.

FIGURE 4
Cash Flow Chart (Risk-Adjusted)



Source: Forrester Research, Inc.

TABLE 8
Cash Flow (Risk-Adjusted)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Costs	($1,624,000)	($2,154,000)	($2,154,000)	($840,000)	($6,772,000)	($5,993,452)
Benefits	$0	$6,586,200	$7,074,000	$7,562,400	$21,222,600	$17,515,479
Net benefits	($1,624,000)	$4,432,200	$4,920,000	$6,722,400	$14,450,600	$11,522,027
ROI						192%

Source: Forrester Research, Inc.

Veracode’s Cloud-Based Application Security Service

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, including 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 – 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 – identifies architectural weaknesses and vulnerabilities in your running web applications before cyber-criminals 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** 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 MDM solutions to enable enforcement of corporate 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, analyzing 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 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** and prioritized based on severity so developers don’t waste time on issues that don’t matter.

- **Role-based access control (RBAC)** that provides granular, permission-based access to results and 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 that 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, including (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, Veracode helps ensure all of your vendor-supplied code is up to your minimum internal standards for acceptable risk. Veracode works directly with your software vendors to assess and remediate their code — including commercial and outsourced applications, software-as-a-service (SaaS) applications, and open source components — and helps you implement an enterprisewide governance process for reducing risk from third-party software, based on industry best practices. Veracode's binary static analysis technology, unique in the industry, allows independent software vendors (ISVs) to rapidly upload and test their compiled code without exposing their intellectual property in the form of source code.

- **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 mobile device management (MDM) solutions to enable enterprises to enforce corporate policies regarding applications downloaded to their employees' mobile devices.

- **Remediation coaching services** to 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.

- **Program management services** that 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 program, 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** that 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.

Appendix A: 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.

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 B: Glossary

Discount rate: The interest rate used in cash flow analysis to take into account the time value of money. Companies set their own a 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 C: 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] Cost per record, the amount of records, and likelihood of occurrence data all collected from research conducted by the Ponemon Institute for Symantec. Source: Netskope (http://www.netskope.com/reports-infographics/ponemon-2014-data-breach-cloud-multiplier-effect/) and databreachcalculator.com (https://databreachcalculator.com/).