A Forrester Total Economic Impact™ Study

Commissioned By

IBM

Project Director:
Sarah Musto
Jon Erickson

July 2016

The Total Economic Impact™ Of IBM Security AppScan Source

Cost Savings And Business Benefits Enabled By AppScan Source

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.

FORRESTER®

Executive Summary

IBM commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying IBM AppScan Source. The purpose of this study is to provide readers with a framework for evaluating the potential financial impact of AppScan Source on their own organizations.

AppScan Source helps organizations lower costs and reduce risk exposure by identifying web-based and mobile application source code vulnerabilities early in the software development life cycle so that they can be fixed before deployment. Although we did not review IBM Security AppScan Enterprise, IBM Security AppScan Standard, IBM Application Security on Cloud, or Arxan Application Protection for IBM Solutions, organizations can also consider these solutions, which provide web and mobile application security.

To better understand the benefits, costs, and risks associated with this implementation, Forrester interviewed a large organization with a global infrastructure deployment and multiple years of experience using AppScan Source. Before deploying AppScan Source, this organization was using several smaller tools and had a decentralized, inconsistent process for reviewing code across all of its development teams. This led to a number of challenges, including costly code fixes late in the development life cycle, the need to use a third party to document code reviews for compliance purposes, and substantial security team time spent on code review. Additionally, the organization had no visibility into the coding practices of developers or the level of vulnerability for its applications, making it very difficult to assess what vulnerabilities they faced and how to best protect the organization's applications. Given these challenges, and the volume of sensitive customer and employee data it manages, the organization decided to improve its security practices to further its record of protecting customer data and to drive customer growth and loyalty.

With AppScan results and better security education, developers remediate code issues faster and earlier in the development cycle, creating significant cost savings. The organization's security team also saves time on code reviews, and the organization can reduce the use of professional services to prove compliance. Increased visibility into vulnerabilities allows the organization to understand what needs to be fixed and to proactively prevent security issues. This improved focus on security positions the organization to better protect customer data and support business growth.

APPSCAN SOURCE ENABLES COST-EFFECTIVE CODE REVIEW AND COMPLIANCE, AS WELL AS SECURITY TEAM TIME SAVINGS

Our interview and subsequent financial analysis found that the interviewed organization experienced the risk-adjusted ROI and benefits shown in Figure 1. The analysis points to benefits of $6.4 million over three years versus costs of $1.8 million, adding up to a net present value (NPV) of $4,588,322.

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

ROI: 253%	NPV: $4,588,322	Payback: 6 months	Cost savings to remediate early in cycle: 90%

Source: Forrester Research, Inc.

Disclosures

The reader should be aware of the following:

- The study is commissioned by IBM 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 IBM AppScan Source.
- IBM 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.
- IBM provided the customer name for the interview but did not participate in the interview or follow-up discussions.

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 IBM AppScan Source. 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

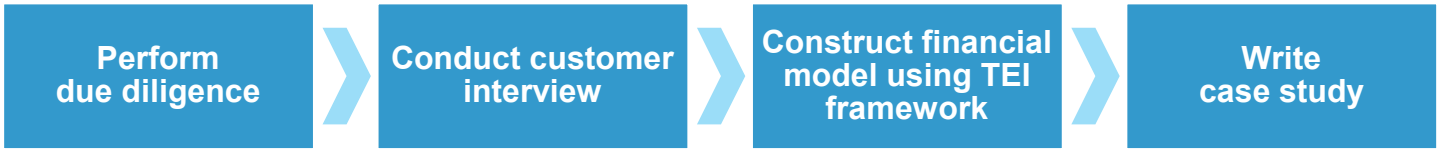
Forrester took a multistep approach to evaluate the impact that AppScan Source can have on an organization (see Figure 2). Specifically, we:

- Interviewed IBM marketing, sales, and/or consulting personnel, along with Forrester analysts, to gather data relative to AppScan Source and the marketplace for AppScan Source.
- Interviewed one organization currently using AppScan Source to obtain data with respect to costs, benefits, and risks.
- Constructed a financial model representative of the interviewed organization 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. Risk adjustment is a key part of the TEI methodology. While the interviewed organization 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 AppScan Source's impact: 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



Source: Forrester Research, Inc.

Analysis

INTERVIEWED ORGANIZATION

For this study, Forrester interviewed a representative from a large enterprise with a global infrastructure deployment.

INTERVIEW HIGHLIGHTS

Situation

The organization needed to improve its code review processes in order to create efficiencies and to improve the security of its applications. Before using AppScan Source:

- The organization had been increasing its focus on security in recent years, but there hadn't always been a strong focus on securing the environment and protecting sensitive data.
- The review of code was decentralized. Reviewing code was done on a team-by-team basis, with each team having different policies and using several smaller tools.
- Because the organization had a decentralized approach to code review, it lacked visibility into how vulnerable its applications were. The security team had no visibility into others' coding practices.
- The lack of visibility and consistency in security practices was troubling because the organization handles a large volume of customer and employee data. Its customers place their trust in the organization to keep their data secure, and a security breach that compromises that data or an application's availability could damage the organization's reputation. This is particularly significant in that the organization considers itself to be a target for threats and attacks based on its size.

Solution

The interviewed organization selected AppScan Source because:

- AppScan Source supports Java and .NET.
- AppScan Source's features found the most vulnerabilities compared with other solutions considered.
- The IBM brand represents quality solutions and productive business partnerships.

Results

The interview revealed that:

- **AppScan Source enables better security practices and more cost-effective code review by developers.** With the use of AppScan Source and training on better security practices, the organization has been able to create standard, consistent, and more cost-effective security processes. Developers now review code prior to testing processes, which has resulted in a 90% cost savings compared to remediating findings later in testing. Additionally, developers can use AppScan Source to find the best place in the flow to fix code, considerably reducing the amount of time needed to remediate findings. The overall effect is faster, more-thorough, and more cost-effective development processes.
- **Better security practices and increased visibility into vulnerabilities create more secure applications.** Prior to using AppScan, the organization had a decentralized process for reviewing code that resulted in low visibility into coding practices and the vulnerabilities of applications. With AppScan Source, the organization can create better, more consistent coding practices that result in more thorough code reviews and more secure applications. Now the developers and security

team have a better understanding of security vulnerabilities and can take the right steps to ensure improved application security.

- **The organization can use AppScan Source to expand its security focus and ensure continued security to support business objectives.** This expansion in focus, combined with the improved security practices and visibility achieved with AppScan Source, will further improve the security of the organization's applications. Given the volume of customer and employee data that the organization manages, and the security threat level from its large footprint, the improved ability to protect data and systems from outside threats will help the organization maintain and improve its brand image.

BENEFITS

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

Cost Savings From Remediating Findings Earlier In The Development Life Cycle

The organization's developers were focused on developing applications with good functionality, but prior to AppScan Source, many applications would be stopped late in the development life cycle due to code that needed to be fixed. The organization wanted developers to use security coding practices earlier in the development process in order to reduce the time and cost to put applications in production.

When application development was halted late in the development cycle, changes to the application would require an additional full testing cycle before the application could be put in production. Depending on the complexity of the application, the cost for these late changes could be very high. Remediating these issues late in the development cycle required, on average, four FTEs for one month and one developer for two weeks, or 720 total hours. Finding and remediating these issues prior to testing required one developer for just two weeks, or 80 total hours. Remediating issues early in the development cycle is 10% of the cost of remediating the issues later on, a significant savings. The organization estimates that 95 of its applications are affected by this new process. With time savings benefits, Forrester applies a productivity capture to conservatively estimate the amount of time saved that is repurposed for additional work.

The interviewed organization provided average estimates for time required for remediation prior to and with AppScan Source. These estimates are subject to variability. Additionally, developer adoption of AppScan Source and proactive remediation of scan results can affect the ability to realize this benefit. To compensate, we risk-adjusted and reduced this benefit by 10%. The risk-adjusted total benefit resulting from earlier remediation over the three years was almost $4.4 million. See the section on Risks for more detail.

TABLE 1
Cost Savings From Remediating Findings Earlier In The Development Life Cycle

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
A1	Applications per year where code issues were remediated late in the development life cycle		95	95	95
A2	Total hours to remediate findings later in the development life cycle, per application		720	720	720
A3	Total hours to remediate findings early in the development life cycle, per application		80	80	80
A4	Hours saved per application with AppScan Source	A2-A3	640	640	640
A5	Average hourly fully loaded compensation		$65	$65	$65
A6	Productivity capture		50%	50%	50%
At	Cost savings from remediating findings earlier	A1*A4*A5*A6	$1,976,000	$1,976,000	$1,976,000
	Risk adjustment	↓10%			
Atr	**Cost savings from remediating findings earlier (risk-adjusted)**		**$1,778,400**	**$1,778,400**	**$1,778,400**

Source: Forrester Research, Inc.

Cost Savings From Faster Remediation With AppScan Source

AppScan Source identifies sources of significant application vulnerabilities so that they can be remediated in large groups rather than individually. Prior to using AppScan, an average application would require 20 hours to remediate all findings, but with AppScan Source, those same findings can be addressed in only 30 minutes. The organization estimates that 95 applications are relevant to this process, and findings are remediated approximately once per quarter.

The interviewed organization provided average estimates for time required for remediation prior to and with AppScan Source. These estimates are subject to variability. Additionally, developer adoption of AppScan Source and the presence of false positives in AppScan results can affect the ability to realize this benefit. To compensate, we risk-adjusted and reduced this benefit by 10%. The risk-adjusted total benefit resulting from faster remediation over the three years was $539,000. See the section on Risks for more detail.

TABLE 2
Cost Savings From Faster Remediation With AppScan Source

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
B1	Number of relevant applications		95	95	95
B2	Number of times application is reviewed each year		4	4	4
B3	Total hours to remediate findings prior to AppScan Source		20	20	20
B4	Total hours to remediate findings with AppScan Source		0.5	0.5	0.5
B5	Average hourly fully loaded compensation		$65	$65	$65
B6	Productivity capture		50%	50%	50%
Bt	Cost savings from faster remediation	B1*B2*(B3-B4)*B5*B6	$240,825	$240,825	$240,825
	Risk adjustment	↓10%			
Btr	**Cost savings from faster remediation (risk-adjusted)**		**$216,743**	**$216,743**	**$216,743**

Source: Forrester Research, Inc.

Reduction In Security Team Time Spent On Code Reviews

Prior to using AppScan Source, the security team was primarily responsible for reviewing code for vulnerabilities. Given the large number of projects, code reviews were time consuming. With AppScan Source, the organization can provide scan results to developers so that developers can see all known issues for their applications and remediate findings. By taking these steps, the security team is able to save one FTE worth of time spent on code reviews which can then be redirected to other types of work.

Time savings estimates are average approximations but are subject to variability. To compensate, we risk-adjusted and reduced this benefit by 5%. The risk-adjusted total benefit resulting from reduced security team time on code reviews over the three years was $319,000. See the section on Risks for more detail.

TABLE 3
Reduction In Security Team Time Spent On Code Reviews

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
C1	Number of security team FTEs repurposed for additional work		1	1	1
C2	Average fully loaded compensation		$135,000	$135,000	$135,000
Ct	Reduction in security team time	C1*C2	$135,000	$135,000	$135,000
	Risk adjustment	↓5%			
Ctr	**Reduction in security team time (risk-adjusted)**		**$128,250**	**$128,250**	**$128,250**

Source: Forrester Research, Inc.

Reduction In Professional Services For Compliance

Prior to using AppScan Source, the organization relied on third-party professional services to review code and provide evidence of scans to allow the organization to remain PCI-compliant. The organization has to show evidence that it is scanning for certain types of vulnerabilities in order to be compliant. Now, the organization is able to use AppScan Source for source code scanning, and developers can provide the chain of evidence necessary so that the organization's own compliance department can manage that process internally.

The organization estimates that it spent approximately $500,000 per year on these compliance services that it no longer spends, but this estimate could be variable. To compensate, we risk-adjusted and reduced this benefit by 10%. The risk-adjusted total benefit resulting from reduced professional services over the three years was just over $1.1 million. See the section on Risks for more detail.

TABLE 4
Reduction In Professional Services For Compliance

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
Dt	Compliance cost savings due to reduced professional services		$500,000	$500,000	$500,000
	Risk adjustment	↓10%			
Dtr	**Compliance cost savings (risk-adjusted)**		**$450,000**	**$450,000**	**$450,000**

Source: Forrester Research, Inc.

Nonfinancial Benefits

The organization mentioned two additional benefits related to the use of AppScan Source, although they could not be quantified. The first benefit is the ability to eliminate tools previously used to review code, thereby eliminating costs associated with those tools. The second benefit is improved time-to-market for applications due to faster remediation of code issues with AppScan Source, although the organization could not accurately

estimate the attribution to AppScan Source of that improved time to market considering other changes to tools and processes that could also contribute to that benefit.

Total Benefits

Table 5 shows the total of all benefits across the four areas listed above, as well as present values (PVs) discounted at 10%. Over three years, the organization expects risk-adjusted total benefits to be a PV of about $6.4 million.

TABLE 5
Total Benefits (Risk-Adjusted)

Ref.	Benefit Category	Year 1	Year 2	Year 3	Total	Present Value
Atr	Cost savings from remediating findings earlier in the development life cycle	$1,778,400	$1,778,400	$1,778,400	$5,335,200	$4,422,618
Btr	Cost savings from faster remediation with AppScan Source	$216,743	$216,743	$216,743	$650,228	$539,007
Ctr	Reduction in security team time spent on code reviews	$128,250	$128,250	$128,250	$384,750	$318,939
Dtr	Reduction in professional services for compliance	$450,000	$450,000	$450,000	$1,350,000	$1,119,083
	Total benefits (risk-adjusted)	**$2,573,393**	**$2,573,393**	**$2,573,393**	**$7,720,178**	**$6,399,646**

Source: Forrester Research, Inc.

COSTS

The interviewed organization experienced a number of costs associated with the use of AppScan Source. These represent the mix of internal and external costs experienced by the interviewed organization for implementation, ongoing maintenance associated with the solution, and ongoing use of AppScan Source.

IBM AppScan Source License Costs

The estimated upfront license cost for a large enterprise, based on the number of developers and industry average AppScan use, is $500,000, with $125,000 per year in subscription and support (S&S). This license cost represents average discounts for large organizations purchasing AppScan Source through an enterprise license agreement and includes two versions of AppScan. S&S includes the costs of support, fixes, and new versions, so there are no additional costs for the organization for a version upgrade in Year 1. These costs reflect a large deployment by a large organization. Smaller deployments will result in lower AppScan costs.

Software license costs can vary based on differences in product usage, different licensing agreements, other products that may be licensed from the same vendor, and other discounts. The license cost presented here is an approximation based on the number of developers. To compensate for this variability, we risk-adjusted this cost up by 5%. The risk-adjusted cost of AppScan Source licenses over the three years was $851,000. See the section on Risks for more detail.

TABLE 6
IBM AppScan Source License Costs

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
Et	AppScan Source license costs		$500,000	$125,000	$125,000	$125,000
	Risk adjustment	↑5%				
Etr	**AppScan Source license costs (risk-adjusted)**		**$525,000**	**$131,250**	**$131,250**	**$131,250**

Source: Forrester Research, Inc.

Additional Hardware And Administration Costs

The organization had to purchase additional hardware to support AppScan Source. For the initial implementation, the organization procured an application server in two instances, one to support each instance of AppScan running in its environment. The organization also procured a database server and database space for each instance. For the initial implementation, the organization estimates it spent $62,500 for the hardware, configuration, networking, and maintenance for the total life cycle. Assuming a five-year average life cycle, the upfront cost was $31,250 with $6,250 in ongoing costs each year.

When the organization upgraded one of its AppScan versions in Year 1, the organization had to procure additional hardware. The organization expects the lifetime cost for the additional hardware investment to total $31,250, which includes $15,625 in Year 1 and $3,125 per year in maintenance over a five-year life cycle.

The organization has a large environment and more complex deployment of AppScan Source. The figures provided are estimates of the total cost for the hardware procurement, installation, and maintenance over an average life cycle, but these costs can vary based on a number of internal and external factors. To compensate,

we risk-adjusted this cost up by 5%. The risk-adjusted cost of additional hardware and administration over the three years was just under $70,000. See the section on Risks for more detail.

TABLE 7
Additional Hardware And Administration Costs

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
F1	Initial hardware purchase and administration		$31,250	$6,250	$6,250	$6,250
F2	Additional hardware and administration for AppScan Source upgrade			$15,625	$3,125	$3,125
Ft	Additional hardware and administration costs	F1+F2	$31,250	$21,875	$9,375	$9,375
	Risk adjustment	↑5%				
Ftr	**Additional hardware and administration costs (risk-adjusted)**		**$32,813**	**$22,969**	**$9,844**	**$9,844**

Source: Forrester Research, Inc.

Installation And Deployment

The organization spent a total of four months on deployment. The installation of AppScan Source was fairly quick, requiring approximately 8 hours. Most of the time spent over those four months was on the integrations with existing tools and rolling out AppScan Source to its developers. A total of 300 hours of a single FTE's time was spent on integrating AppScan Source into its environment. The organization noted that some of these integrations were not provided out of the box and required the organization to write the integration code themselves, taking longer than expected. The organization also had two FTEs spend three months distributing a plug-in to allow developers to use their IDEs to scan code. The organization decided to upgrade in Year 1 to a newer version of AppScan Source to support newer versions of other tools in its environment. The effort to upgrade to the new version required a month of engineering time and three months to distribute the new version to all developers.

The installation and deployment process was complex due to the organization's large developer population and heterogeneous environment with multiple versions of AppScan Source. The organization noted that this heterogeneous environment was maintained due to compatibility issues with versions of AppScan and other tools in the environment. Additionally, some of the integrations and implementation steps took longer than expected. To compensate, we risk-adjusted this cost up by 15%. The risk-adjusted cost of installation and deployment over the three years was $145,000. See the section on Risks for more detail.

TABLE 8
Installation And Deployment

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
G1	Hours spent on installation		8			
G2	Hours spent on deployment of plug-in		1,040			
G3	Hour spent on integrations with development systems		300			
G4	Hours spent on AppScan upgrade			650		
G5	Average hourly fully loaded compensation		$65	$65		
Gt	Installation and deployment	(G1+G2+G3+G4)*G5	$87,620	$42,250	$0	$0
	Risk adjustment	↑15%				
Gtr	**Installation and deployment (risk-adjusted)**		**$100,763**	**$48,588**	**$0**	**$0**

Source: Forrester Research, Inc.

Ongoing Use Of AppScan

FTEs on the security team and team leads use AppScan Source on an ongoing basis. On the security team, two FTEs use AppScan as part of a process where they review code for other teams. Each of the two analysts creates seven reports a year, requiring 25% of their overall time. The organization noted that each scan produces a large number of false positives in addition to true vulnerabilities, which requires time from each team lead to sort through. The organization also notes that there is no net additional time required for developers to use AppScan compared with the prior environment, and there is no time spent on AppScan administration.

FTE time spent on the ongoing use of AppScan is based on an estimate of the average usage across the security team and team leads. To compensate, we risk-adjusted this cost up by 5%. The risk-adjusted cost of the ongoing time spent on AppScan over the three years was $219,000. See the section on Risks for more detail.

TABLE 9
Ongoing Use Of AppScan

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
H1	FTEs on security team using AppScan			2	2	2
H2	Hours per year per FTE spent on AppScan			520	520	520
H3	Team leads using AppScan			50	50	50
H4	Hours per year per team lead spent on AppScan			5	5	5
H5	Average hourly fully loaded compensation			$65	$65	$65
Ht	Ongoing use of AppScan	((H1*H2)+(H3*H4))*H5	$0	$83,850	$83,850	$83,850
	Risk adjustment	↑5%				
Htr	**Ongoing use of AppScan (risk-adjusted)**		**$0**	**$88,043**	**$88,043**	**$88,043**

Source: Forrester Research, Inc.

Training Costs

The organization required developers to participate in training sessions on OWASP top 10 vulnerabilities. During these courses, the developers would learn about secure coding. All developers participated in a 4-hour training session. The organization also created training videos on security best practices, which cost approximately $5,000. Overall, the initial training effort cost $395,000 for the creation of the training videos and the time spent by developers. AppScan training was provided by video.

With the upgrade in Year 1 to the newest version of AppScan, the organization used an online training tool to educate developers on new features. The online training course for the developers takes 90 minutes to complete. The additional training cost in Year 1 is $145,000 in developer time. If additional upgrades are required in years 2 and 3, additional training time may be required.

TABLE 10
Training Costs

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
I1	Creation of professional training videos		$5,000			
I2	Cost of developer time spent on training		$390,000	$145,000		
It	Training costs	I1+I2	$395,000	$145,000	$0	$0

Source: Forrester Research, Inc.

Total Costs

Table 11 shows the total of all costs as well as associated present values (PVs), discounted at 10%. Over three years, the organization expects risk-adjusted total costs to be a PV of almost $1.8 million.

TABLE 11
Total Costs (Risk-Adjusted)

Ref.	Cost Category	Initial	Year 1	Year 2	Year 3	Total	Present Value
Etr	IBM AppScan Source license costs	($525,000)	($131,250)	($131,250)	($131,250)	($918,750)	($851,399)
Ftr	Additional hardware and administration costs	($32,813)	($22,969)	($9,844)	($9,844)	($75,469)	($69,224)
Gtr	Installation and deployment	($100,763)	($48,588)	$0	$0	($149,351)	($144,933)
Htr	Ongoing use of AppScan	$0	($88,043)	($88,043)	($88,043)	($264,128)	($218,949)
Itr	Training costs	($395,000)	($145,000)	$0	$0	($540,000)	($526,818)
	Total costs (risk-adjusted)	**($1,053,576)**	**($435,849)**	**($229,136)**	**($229,136)**	**($1,947,697)**	**($1,811,324)**

Source: Forrester Research, Inc.

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 AppScan Source 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 AppScan Source, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for cost and benefit estimates.

TABLE 12
Benefit And Cost Risk Adjustments

Benefits	Adjustment
Cost savings from remediating findings earlier in the development life cycle	↓ 10%
Cost savings from faster remediation with AppScan	↓ 10%
Reduction in security team time spent on code reviews	↓ 5%
Reduction in professional services for compliance	↓ 10%

Costs	Adjustment
IBM AppScan Source license costs	↑ 5%
Additional hardware and administration costs	↑ 5%
Installation and deployment	↑ 15%
Ongoing use of AppScan	↑ 5%

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:

- The interviewed organization provided average estimates for time required for remediation prior to and with AppScan. These estimates are subject to variability. Additionally, developer adoption of AppScan and proactive remediation of scan results can affect the ability to realize this benefit. Developers can use their discretion to decide which issues to remediate and when to remediate them. Additionally, false positives from scan results not caught by team leads can slow remediation time.
- Time savings estimates are average approximations but are subject to variability. Accurately measuring time saved on specific processes can be challenging, so to make the estimate more conservative, we risk-adjusted this benefit.
- The interviewed organization estimates that it spent on average $500,000 per year on professional services related to source code scanning for compliance, but this estimate could be variable. In order to make this estimate more conservative to account for inaccuracies in the estimation, we risk-adjusted this benefit.

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

- Software license costs can vary based on differences in product usage, different licensing agreements, what other products may be licensed from the same vendor, and other discounts. The license cost presented in this study is an approximation based on the number of developers and industry average use of AppScan but does not represent actual costs paid by the interviewed organization.

- The organization noted that its heterogeneous environment, with two versions of AppScan Source, was maintained due to compatibility issues with versions of AppScan and other tools in the environment. Compatibility issues mean more time on installation and integrations with each upgrade.
- The organization has a large environment and more complex deployment of AppScan Source. The figures provided are estimates of the total cost for the hardware procurement, installation, and maintenance over an average life cycle, but these costs can vary based on a number of internal and external factors.
- The installation and deployment process was complex due to the organization's large developer population and heterogeneous environment with multiple versions of AppScan. Additionally, some of the integrations and implementation steps took longer than expected. This is because some integrations were not provided out of the box and the organization had to write them themselves. Additionally, some issues required the organization to request workarounds from IBM.
- FTE time spent on the ongoing use of AppScan is based on an estimate of the average usage across the security team and team leads. We added a risk adjustment to make the estimate of time more conservative, considering the large number of false positives displayed in the AppScan results that team leads have to spend time removing from the code quality platform.

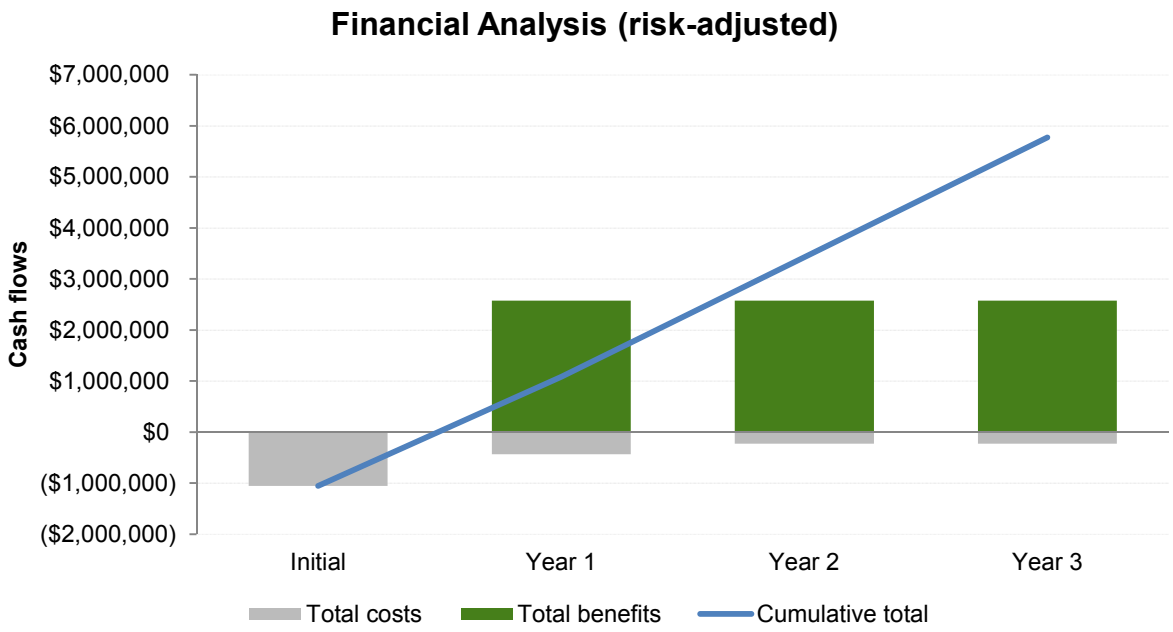
Table 12 shows the values used to adjust for risk and uncertainty in the cost and benefit estimates for the interviewed organization. Readers are urged to apply their own risk ranges based on their own degree of confidence in the cost and benefit estimates.

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 interviewed organization's investment in AppScan Source.

Table 13 below shows the risk-adjusted ROI, NPV, and payback period values. These values are determined by applying the risk-adjustment values from Table 12 in the Risk section to the unadjusted results in each relevant cost and benefit section.

FIGURE 3
Cash Flow Chart (Risk-Adjusted)



Source: Forrester Research, Inc.

TABLE 13
Cash Flow (Risk-Adjusted)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Costs	($1,053,576)	($435,849)	($229,136)	($229,136)	($1,947,697)	($1,811,324)
Benefits	$0	$2,573,393	$2,573,393	$2,573,393	$7,720,178	$6,399,646
Net benefits	**($1,053,576)**	**$2,137,544**	**$2,344,256**	**$2,344,256**	**$5,772,481**	**$4,588,322**
ROI						**253%**
Payback period						**6 months**

Source: Forrester Research, Inc.

IBM Security AppScan Source: Overview

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

IBM Security AppScan enhances web application security and mobile application security, improves application security program management, and strengthens regulatory compliance. By scanning your web and mobile applications prior to deployment, AppScan enables you to effectively identify security vulnerabilities and generate reports and fix recommendations.

You are already familiar with IBM Security AppScan Source, which was utilized by this study's identified IBM customer to lower costs and reduce risk exposure by identifying vulnerabilities early in the development life cycle.

IBM's Application Security Testing portfolio also includes the following:

IBM Security AppScan Enterprise: Mitigates application security risk, strengthens program management, and helps you to achieve regulatory compliance.

IBM Security AppScan Standard: Reduces the likelihood of web application attacks and data breaches by automating application vulnerability testing.

IBM Application Security on Cloud: Helps secure web, mobile, and desktop applications by detecting a wide range of pervasive and published security vulnerabilities.

Arxan Application Protection for IBM Solutions: Expands mobile security with application hardening and cryptographic key protection.

For additional information, please visit ***http://www-03.ibm.com/software/products/en/appscan*** or contact your IBM representative.

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. 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.

FRAMEWORK ASSUMPTIONS

Table 14 provides the model assumptions that Forrester used in this analysis.

The discount rate used in the PV and NPV calculations is 10% and 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 14
Model Assumptions

Ref.	Metric	Calculation	Value
X1	Hours per week		40
X2	Weeks per year		52
X3	Hours per year (M-F, 9-5)		2,080
X4	Hours per year (24x7)		8,736
X5	Average fully loaded compensation		$135,000
X6	Hourly fully loaded compensation	(X5/X3)	$65

Source: Forrester Research, Inc.

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 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.