A Forrester Total Economic Impact™ Study

Commissioned By

IBM

Project Director:
Henry Huang

May, 2017

The Total Economic Impact™ Of IBM BigFix Patch And BigFix Compliance

Cost Savings, Business Benefits, And Better Sleep At Night, Made Possible With BigFix

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.

© 2017, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to www.forrester.com.

FORRESTER®

Executive Summary

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 BigFix Patch and BigFix Compliance. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of taking a more proactive patching and compliance stance with BigFix.

To better understand the benefits, costs, and risks associated with a BigFix implementation, Forrester interviewed several customers with multiple years of experience using BigFix for application patch and compliance management — two imperatives that are constantly top priorities for organizations. Over 75% of external breaches use publicly known application vulnerabilities that can been patched.[1] BigFix directly identifies and addresses this exposure at the endpoint level with a patch automation toolset that is efficient, scalable, and cost effective.

IBM BigFix Patch and IBM BigFix Compliance are two modules of the BigFix toolset that help automate endpoint management to decrease security risk surfaces, manage configurational drift, and maintain continuous compliance.

"BigFix has become the eyes and ears of our environment."
~ Security solution architect

The financial assessment of a composite organization of 10,000 endpoints, based on a series of customer interviews, concludes:

- **Costs of usage: $1,931,693.**
- **Hard benefits: $7,245,379.**
- **Three-year net present value: $5,095,911.**

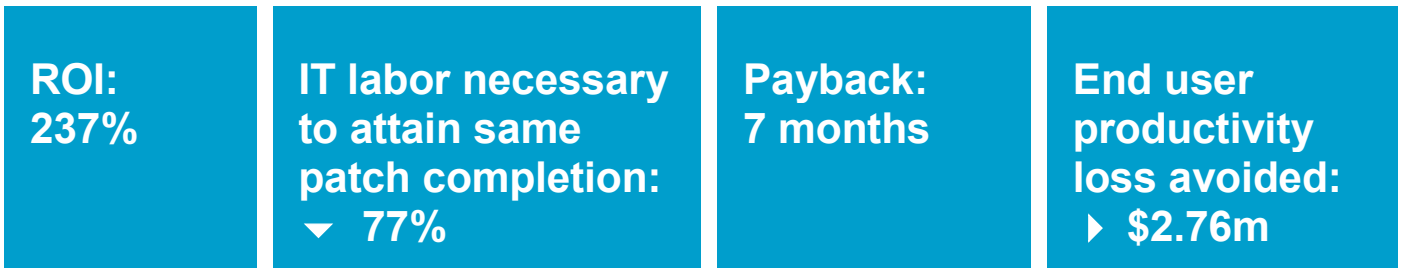
Prior to BigFix, customers had implemented various patch management systems, ranging from the occasional spreadsheet documentation to more complex centralized patch deployment solutions. The lack of patching cadence was a glaring issue for some, while poor patch performance from legacy patch and compliance solutions was simply too cumbersome to be effective at larger organizations with more complex networks. An assortment of unidentified compliance issues, end user difficulties, and a porous security surface led to costly breaches in some organizations and sleepless nights for the leaders of others. With BigFix, customers were able to assess endpoints in near real-time, automate patch processes, and rapidly respond to compliance issues across their enterprise. Endpoint assessments were reduced from days to hours, while patch completion rates improved from 80% to 97%.

ASSESS, PATCH, AND ENFORCE FASTER WITH BIGFIX

Our interviews with four existing customers and subsequent financial analysis found that a composite organization based on these interviewed organizations experienced the risk-adjusted ROI benefits and costs shown in Figure 1.[2]

The composite organization analysis points to benefits of $2.4 million per year versus average annual costs of approximately $0.6 million, adding up to a three-year net present value (NPV) of over $5 million. And while these hard benefits were significant, the composite most importantly reduced risk exposure that could have potentially led to issues with business continuity and viability.

FIGURE 1
Financial Results Reflecting Three-Year Risk-Adjusted Results



Source: Forrester Research, Inc.

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

- **Patching more effectively with BigFix resulted in business end users losing fewer productivity minutes. The productivity retained is equivalent to nearly $1 million annually.** Prior to BigFix Patch and BigFix Compliance, the composite organization had an 80% success rate with patches. With 10,000 endpoints in the organization, numerous end users suffered incomplete patches, resulting in inoperable or poorly performing applications that required remediation. The organization's end users lost an average of 15 minutes per incident to call helpdesk resolution and an additional 40 minutes for manual patching. Accounting for risk adjustments (see the Risk section for details), the benefit recognized by the organization was $2.8 million after three years.
- **Systems engineers saved over 29,000 hours per year through improved patch automation.** BigFix Patch was successful on 97% of patch deployments, which were released on a biweekly interval at the composite organization. With a dramatically improved automated patch assessment and completion rate, the team of five systems engineers performed dramatically fewer manual endpoint patches. In its previous state, the composite organization would have needed to hire 17 additional engineers to fully deploy patches with the same frequency and success rate as it does with BigFix Patch. This benefit amounted to over $4.3 million over three years.
- **Network assessments and endpoint audit compliance improved with better tracking and a quicker return of information on BigFix.** The efficiency of the BigFix solutions in providing assessments resulted in reporting within hours, sometimes minutes, rather than days with the legacy endpoint management solution. Reporting gains amounted to a total of $96,604 over three years at the composite organization.
- **Avoided PCI DSS noncompliance fines of $66,860 over three years.** In the prior state before BigFix, the composite organization had a high level of variability with patching success. Failed patches were fixed manually but left some periods of noncompliance with PCI DSS and at times resulted in fines. Repeat offenses of noncompliance increase fine amounts with each occurrence.

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

- The combined license and support fees of BigFix Patch and BigFix Compliance amounted to more than $1.9 million over three years. Perpetual licenses mainly encompass initial costs, while annual support fees are recurring charges to cover 10,000 endpoints initially to 10,500 by the second year and 11,000 by the third.
- **Training costs for the initial ramp-up period and advanced further education to fully leverage the BigFix solutions add to $217,775.** The composite organization recognized an initial ramp-up period of two months prior to realizing full benefit from the product. Additionally, a one-time professional services fee of $80,000 was paid to IBM for the initial implementation period. Users frequently cited the powerful capabilities of BigFix but also noted that to fully exploit the capabilities, further advanced training was necessary.

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 BigFix.

› 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.

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 BigFix Patch and BigFix Compliance. 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 IBM BigFix 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 BigFix and the marketplace for BigFix.
- Interviewed four organizations currently using IBM BigFix to obtain data with respect to costs, benefits, and risks.
- Designed a composite organization based on characteristics of the interviewed organizations.
- Constructed a financial model representative of the interviews using the TEI methodology. The financial model is populated with the cost and benefit data obtained from the interviews as applied to the composite organization.
- Risk-adjusted the financial model based on issues and concerns the interviewed organizations highlighted in interviews. Risk adjustment is a key part of the TEI methodology. While interviewed organizations provided cost and benefit estimates, some categories included a broad range of responses or had a number of outside forces that might have affected the results. For that reason, some cost and benefit totals have been risk-adjusted and are detailed in each relevant section.

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

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

FIGURE 2

TEI Approach

Source: Forrester Research, Inc.

Analysis

INTERVIEWED ORGANIZATIONS

For this study, Forrester conducted a total of four interviews with representatives from the following companies, which are global IBM customers:

- A major US university with over 10,000 staff and approximately 70,000 BigFix managed endpoints. The endpoints are split primarily between two major operating systems, both of which are supported by BigFix. Prior to introducing BigFix, the organization was hit by an attack that affected thousands of machines and cost $1.5 million in clean-up over three months. Since patching had been left to the IT resources within individual departments, the attack served as a wake-up call that a central patch management solution was required.
- A biotech company, employing over 400 full-time employees. Their network is 100% virtualized, and patching had been far from consistent. Owning significant intellectual property and being faced with various regulatory and compliance measures, the organization found BigFix to be the solution that it needed. The sheer number of audits standard in this specific vertical were simplified and made easier with BigFix providing rapid reporting.
- A major payment processor with tens of data centers based globally serving millions of merchants. Their network is heavily virtualized, running mostly desktop and laptop hardware. As an acquirer, it is subject to Federal Financial Institutions Examination Council (FFIEC) related fines up to $500,000 per customer for regulatory noncompliance. PCI noncompliance was also a major concern; it can lead to both fines and blacklisting from banks. IT resource strain became a compounding issue as compliance audits increased in more recent years. While network segmentation had been implemented to contain the spread of malicious elements inside the network, patching with regularity was the key for this organization to stay compliant in the regulatory minefield.
- A multi-billion-dollar US-based data and telecom equipment company, employing 15,000 employees in 100 offices across 50 countries. Their internal private cloud serves the vast majority of their end user computing requirements. They are subject to both SOX and PCI compliance, with BigFix shortening the audit process for both considerably. BigFix was initially brought in for its ability to consolidate and centralize incident response, but soon the patch and compliance capabilities proved invaluable as well.

> ***"In the days prior to BigFix, we used a spreadsheet to track our patching and it was hardly ever accurate. There was no cadence to our patching. That just doesn't seem right in this day and age, does it?"***
>
> ~ Manager of governance technology, payment processor

> ***"Being out of compliance can result in fines of $100,000 to $500,000 with the FFIEC. But if PCI compliance isn't passed, our business can come to a full stop with many banks."***
>
> ~ Manager of governance technology, payment processor

In addition to the data points and insights presented by the firms' representatives in their current roles, many of the representatives from these organizations presented insight on their experience with patching, staying compliant, and BigFix usage from their roles with prior employers. We applied a combined analysis of results to the financial model analysis presented here.

THE COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an associated ROI analysis that illustrates the areas financially affected. The composite organization that Forrester synthesized from these results represents an organization with the following characteristics:

> *"If you don't have a solution like BigFix, you're not doing compliance. You're lying to yourself if you're saying otherwise."*
>
> ~ Director of IT, US biotech company

- A large eCommerce retailer organization operating across North America and Europe facing regulatory measures, some of which are region-specific and some region-agnostic.
- This organization processes a significant number of payments and thus is regulated by the PCI council in addition to governmental regulations.
- It manages well over 10,000 endpoints on a complex network consisting of some virtualization and on-premises infrastructure. It is an ongoing initiative to further virtualize the environment and retire legacy systems as a top-down business initiative.
- It has 8,000 employees, the majority of whom are business users who have varying configurations on their Windows-based machines for relevancy to their jobs.
- IT staffing resources are shared among the enterprise business units, with a dedicated team of five engineers whose sole task is to maintain security compliance.
- It had previously suffered a data breach, setting back branding efforts and resulting in PCI fines.
- It believes that endpoint security is best managed through proactive measures by keeping security holes to a minimum through endpoint patching and, in turn, reducing the likelihood of breaches. This helps to attain compliance, protects employees and customers, and avoids costly incident clean-up costs.

SITUATION

Like many organizations, the composite organization feared the threat of cyberattack and data breach — an increasing problem requiring constant vigilance from already strapped IT resources. Regulatory measures and financial compliance governance bodies too were increasingly ramping up audits to protect the interests of consumers. After a previous breach resulting in lost customer loyalty and reduced revenues, executives decided to formalize an internal security compliance team of engineers to avoid a repeated situation. While the dedicated task force had made notable strides in patching of technology resources and taken a direction toward improving security compliance, the existing endpoint management solution lacked the speed to be truly effective at patching. More recently, an initiative had been made to source a newer centralized solution capable of improving endpoint management efficiency and automation. In doing so, it hoped to be able to scale a growing, digitally focused business without adding significant headcount

The second but still important part of the composite organization's initiative was to avoid the noncompliance fines and related legal fees that had become an unsustainable portion of the budget. If the organization were able to patch endpoints with accuracy and speed, it could maintain such constant vigilance that PCI audits would go more smoothly and result in zero fines. Protracted audit and legal processes needed to be shortened and perhaps removed altogether.

After it reviewed its current security mitigation and response efforts, the organization considered broader implications that had not previously been considered part of the problem. For example, its review included lost employee productivity as a result of system downtime due to incomplete or incompatible patches, forcing IT to take users offline. Perhaps even more important, it considered whether an endpoint management service could be used to augment its IT operations with greater ITSM and ITAM capability. It even considered the cost of turnover following a breach, knowing recruitment of new staff — especially after a high-profile breach — may take longer and cost more. With all the potential costs and benefits in mind, the organization sought the following in an endpoint monitoring solution:

- A centralized patch alerting and delivery mechanism to set a cadence for patching of both OS and third-party applications.
- Continuous security compliance across all endpoints on the corporate network that reduced the cost and complexity of IT management.
- A solution with powerful out-of-the-box capabilities not only of patch and compliance management today but with room for customization as the environment changes.
- Scalability without minimal performance loss that protects any and all additional endpoints automatically.

After a business case process evaluating multiple vendors, the composite organization chose IBM and began deployment of BigFix Compliance and BigFix Patch. Primary and secondary factors that factored into the decision-making process was the ability to attain near constant compliance with the rapidity of endpoint monitoring and patching, as well as comprehensive ability for BigFix to manage endpoints of multiple OS and device types.

> ***"Going from our old patching system, that took two or more days to pull reports, to BigFix and its ability to rapidly respond, was quite a stark contrast."***
>
> ~ CISO, global telecom equipment company

- The organization performed a pilot of BigFix, which soon resulted in full visibility over the initial segment of managed endpoints and its associated compliance risk.
- A corporatewide implementation followed with integration to the existing endpoint antivirus/antimalware detection solution. Soon after deployment of the BigFix Patch and BigFix Compliance, the organization could enforce policies in near real-time and detect anomalies across the network. The organization was enabled to self-enforce daily audits for regulatory compliance — an insurmountable task prior to adoption on BigFix.
- Initial feedback from administrators indicated that the platform was highly capable of providing on-the-fly reporting, given that the BigFix application agents were actively analyzing information at the endpoint upon deployment.
- Following the successful rollout, the IT organization was able to track quantifiable year-over-year savings to the business in avoided costs such as IT labor, compliance fines, and external audit fees. Other crucial, yet less quantifiable, savings included loss in brand confidence or decreased customer lifetime value from potential breaches.
- Given the importance of brand value, the organization viewed attaining continuous compliance and minimizing breachable points of entry through regular patching as paramount to ongoing business success.

Ultimately, by choosing the BigFix Patch and Compliance toolset, the composite organization gained stronger network security; avoided lost business user productivity, IT labor, and compliance costs, and increased its efficiency in remediation. These are hard benefits that are easily translatable to other adopters of the solution.

BENEFITS

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

- Business user productivity loss avoidance.
- Network engineer productivity time savings.
- Audit and assessment efficiency gains.
- Cost avoidance of PCI DSS noncompliance fines.

Beyond the quantified benefits, the most powerful driver for implementing the BigFix solution is the threat of a breach and the possibility of associated heavy losses. Because the cost of a breach varies greatly between organizations, depending on such factors as the scale and duration of the breach and motivations and operators behind it, we have included the decreased risk of breach from the use of BigFix as an important but unquantified benefit.

Readers should consider the following two major factors of this benefit category:

- No organization is immune to breaches. The size of an organization cannot determine the likelihood of attack or the accompanying potential damage, nor can any particular industry preclude an organization, as motivations behind breaches have evolved.[3] Information can be of significant value to one entity but might be of little worth to another. Visibility as an organization is also of limited relevance. If your data is valuable to someone, they will come get it. We cannot say with precision the percentage of organizations that are breached, as some organizations that have been breached have yet to even identify or wish to externally indicate that they have been breached. We can say, however, that the proper question is not "if" but "when."
- Breaches can financially affect organizations in a number of different ways such as:
  - Lost revenues. This can derive from loss of customer loyalty, loss of customer confidence, or an attack preventing the access of customer-facing channels. Revenue losses can be extenuating, based upon the impact of the breach.
  - Legal settlements. A loss of highly confidential information can increase the likelihood and the severity of the legal case. Stakeholders are not limited to the parties contained within the breached data but can also include entities a number of degrees of connection beyond.
  - Regulatory fines. Highly regulated data such as healthcare information can trigger fines from governmental entities such as HIPAA and FTC.
  - Cost of new security infrastructure and implementations to resolve the existing security gaps.

There are additional considerations for the financial impact of a breach, and readers should measure the potential impact of breaches against their specific environment. With that in mind, security risk reduction should be considered as more than just an unquantified benefit, but also as a crucial element of business operations in the digital world. Maintaining application patches up to date and managing compliance are key prevention steps and the first steps that should be taken toward reducing the risk of a breach.

Business User Productivity Loss Avoidance

Prior to adopting BigFix, the composite organization suffered from poor application performance and uptime, resulting in lost productivity from business end users. A poorly executed patching plan to shore up security following an initial breach saw systems engineers implementing patches without accurate cataloguing and assessments of the endpoints prior to deployment. Lacking critical information, systems engineers were unable

to improve upon the endpoint situation effectively with a legacy solution. Further exacerbating the issue was a lack of patch execution status following deployment. The need for security drove business leaders to demand better security compliance, faster patch delivery, and a better security posture. Regulatory scrutiny increased invariably, too, following the breach incident. Ultimately, end users suffered technical issues, with incomplete patches and technology unavailability driving them to call IT helpdesk, followed by a manual patch update by systems engineers.

Following the implementation of BigFix, the composite organization saw quicker patch delivery cycles without performance degradation or, what would be even worse, technology unavailability. Whereas the legacy solution was slow and applied patches with an 80% success rate, the BigFix Patch solution applied patches in minutes, and typically with a success rate of 97%. The patch failure difference between the legacy and BigFix solution equated to an improvement of 1,700 more successfully deployed patches per cycle in the first year. Business end users gained approximately 4 hours per year in productivity that would otherwise have been lost to failed patch automation. Over three years, avoided business end user productivity loss across multiple lines of business at a fully loaded hourly rate of $37.50 per hour equated to an organizational PV benefit of $3,955,398.

Readers should be aware that some organizations may experience differences in the capture rate of productivity time recovered from the use of BigFix Patch. While end users undoubtedly were met with less interruption, our findings indicate that some users do not call helpdesk as they do not experience immediate effects of incomplete patches. In other instances, we noted that end users were able to move to unutilized workstations to continue work. To reflect the ability for some end users to continue contributing productively, this benefit category has been risk-adjusted and reduced by 30% as a conservative measure. The risk-adjusted PV benefit of end user productivity loss avoidance over three years was $2,768,778. See the section on Risks for more detail.

TABLE 1
Business User Productivity Loss Avoidance

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
A1	Technical support for non-standard application behavior related to posture or patch, in minutes per incident			15	15	15
A2	Manual patch, policy, and compliance correction time, making the end user system unavailable, in minutes per year			40	40	40
A3	Cost of business user of endpoint, hourly, fully loaded	$60,000*1.2X / 1920 hours		$37.50	$37.50	$37.50
A4	Total endpoints			10,000	10,500	11,000
A5	Delta in endpoints fully patched by BigFix vs. the prior solution	A4*17%		1,700	1,785	1,870
A6	Frequency of patches			26	26	26

At	Business user productivity loss avoidance	(A1+A2)/60*A3*A5*A6	$0	$1,519,375	$1,595,344	$1,671,313
	Risk adjustment	↓30%				
Atr	**Business user productivity loss avoidance (risk-adjusted)**		**$0**	**$1,063,563**	**$1,116,741**	**$1,169,919**

Source: Forrester Research, Inc.

Systems Engineer Productivity Time Savings

In addition to business end user productivity gains, the composite organization experienced a productivity time savings to its systems engineers responsible for manual patching sessions. Automated patching success rates improved 17%, as indicated in the previous benefit, and saved 40 minutes per manual patch action avoided. Notably, the composite organization completed patch cycles more consistently and without the need to hire additional systems engineers. For the organization to achieve the same level of engineer productivity and pace of patch deployment with the legacy solution, 17 additional engineers would have been necessary. At a significantly higher cost per engineer resource than business end users, the savings realized from improved patching automation saved the organization a three-year PV $4,317,137.

TABLE 2
Systems Engineer Productivity Time Savings

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
B1	BigFix Patch endpoint completion rate			97%	97%	97%
B2	Existing solution endpoint patch completion rate			80%	80%	80%
B3	Patch completion delta	17% * total endpoints		1,700	1,785	1,870
B4	Frequency of patches per year			26	26	26
B5	Hours necessary per manual endpoint patch session unsuccessfully completed, excluding the time-to-know			0.67	0.67	0.67
B6	Hourly cost of network engineer, fully loaded	$90,000 * 1.2X / 1920 hours		$56.25	$56.25	$56.25
Bt	Systems engineer productivity time savings	B3*B4*B5*B6	$0	$1,658,329	$1,741,245	$1,824,162
	Risk adjustment	0%				
Btr	**Systems engineer productivity time savings (risk-adjusted)**		**$0**	**$1,658,329**	**$1,741,245**	**$1,824,162**

Source: Forrester Research, Inc.

Audit And Assessment Efficiency Gains

The composite organization indicated an improvement in the time to assess and audit endpoints for status. Systems engineers require information to keep them aware of patch status across the enterprise, as do compliance auditors. With BigFix Compliance, information delivery was seamless and was delivered significantly quicker than with the legacy solution. The legacy solution delivered some endpoint data as smaller segment batch chunks rather than a single large delivery batch for the entire network, freeing engineers to carry forward with alternate tasks while awaiting assessments. Due to this compromise, only 50% of the actual time savings for the actual time saved has been reflected as productivity captured.

Over three years, the organization saved a PV of $92,604 in assessment efficiency gains.

TABLE 3
Audit And Assessment Efficiency Gains

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
C1	PCI DSS audit savings in hours, per year	16 hours/quarter * 4 quarters		64	64	64
C2	Internal IT audit, time-to-know reduction for each endpoint posture, compliance, and patch assessment, in hours			46	46	46
C3	Patch deployments per year			26	26	26
C4	Hourly cost of IT auditor, fully loaded	$90,000 * 1.2x / 1920 hours		$56.25	$56.25	$56.25
C5	Productivity capture			50%	50%	50%
Ct	Audit and assessment efficiency gains	(C1*C4)+(C2*C3*C4*C5)	$0	$37,238	$37,238	$37,238
	Risk adjustment	0%				
Ctr	**Audit and assessment efficiency gains (risk-adjusted)**		**$0**	**$37,238**	**$37,238**	**$37,238**

Source: Forrester Research, Inc.

Cost Avoidance Of PCI DSS Noncompliance Fines

As an eCommerce organization conducting millions of payment transactions, the composite organization was held to strict PCI DSS regulations. On the BigFix Patch and BigFix Compliance platforms, the organization exhibited significant improvement in consistency of patching and provided substantiating audits and reports quickly in compliance with PCI requirements. Whereas the organization was fined almost yearly in its former state for noncompliance, the equivalent PV fees of $66,860 were avoided while operating BigFix.

TABLE 4
Cost Avoidance Of PCI DSS Noncompliance

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
D1	PCI DSS noncompliance avoidance			$20,000	$40,000	
D2	Labor costs avoided for investigation and remediation of PCI noncompliance			$9,000	$9,000	
Dt	Cost avoidance of PCI DSS noncompliance	D1+D2	$0	$29,000	$49,000	$0
	Risk adjustment	0%				
Dtr	**Cost avoidance of PCI DSS noncompliance (risk-adjusted)**		**$0**	**$29,000**	**$49,000**	**$0**

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 composite organization expects risk-adjusted total benefits to be a PV of more than $7.2 million.

TABLE 5
Total Benefits (Risk-Adjusted)

Ref.	Benefit Category	Initial	Year 1	Year 2	Year 3	Total	Present Value
Atr	Business user productivity loss avoidance	$0	$1,063,563	$1,116,741	$1,169,919	$3,350,222	$2,768,778
Btr	Systems engineer productivity time savings	$0	$1,658,329	$1,741,245	$1,824,162	$5,223,736	$4,317,137
Ctr	Audit and assessment efficiency gains	$0	$37,238	$37,238	$37,238	$111,713	$92,604
Dtr	Cost avoidance of PCI DSS noncompliance	$0	$29,000	$49,000	$0	$78,000	$66,860
	Total benefits (risk-adjusted)	**$0**	**$2,788,129**	**$2,944,223**	**$3,031,318**	**$8,763,670**	**$7,245,379**

Source: Forrester Research, Inc.

COSTS

The composite organization experienced a number of costs associated with the BigFix solution:

- Software license and support costs.
- Implementation, baseline, and additive training costs.

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

Software License And Support Costs

Perpetual software license costs for the BigFix Patch and BigFix Compliance solutions are incurred as one-time costs, paid to IBM based on the number of endpoints managed. A small cost for four perpetual server licenses (to account for redundancy) was also assumed. It should be noted that an investment in BigFix Compliance typically includes BigFix Patch functionality. Our analysis of prior current customers is comprised of customers who used Compliance and Patch at times separately, hence individual pricing has been presented in the table below. In practice, organizations purchase either BigFix Compliance or Patch, but do not have to pay for each independently. Ongoing software support costs of 20% have also been incorporated to the base license costs and incorporated over the study time frame. Over three years, a total PV of $1,931,691 in software licensing and support fees, or about $193.17 per endpoint, was tallied.

TABLE 6
Software License And Support Costs

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
E1	Endpoints across entity		10,000	10,000	10,500	11,000
E2	Patch client licenses, with support and service	E1*License fee *1.2 + virtual server licenses + aggregate support costs	$54,000		$14,040	$14,580
E3	Compliance client license, with support and service	E1 * Perpetual license fee *1.2 + aggregate support costs	$1,236,000		$278,100	$288,400
E4	PCI add-on license		$160,000	$0	$8,000	$8,000
Et	Software license and support costs	E2+E3+E4	$1,450,000	$0	$300,140	$310,980
	Risk adjustment	0%				
Etr	**Software license and support costs (risk-adjusted)**		**$1,450,000**	**$0**	**$300,140**	**$310,980**

Source: Forrester Research, Inc.

Implementation, Baseline, And Additive Training Costs

The composite organization incurred a majority portion of training costs during the initial implementation phase for the purposes of ramping up the security compliance team. A smaller ongoing training program to add to BigFix Patch capabilities and to account for network engineer resource turnover was also implemented, adding marginally incremental costs. Initial professional services amounting to $80,000 were provided from IBM and were leveraged to accelerate platform proficiency. Following three months of a ramp-up period, the composite organization was able to fully realize the core capabilities of the platform and effectively patch and monitor for compliance. The total PV cost of training over three years, inclusive of professional services, was $197,977.

Training costs vary between organizations with differing endpoint management maturity and engineer capabilities. To account for complications in transitioning, some organizations may allocate additional hours for engineer training for the BigFix platform. This cost was risk-adjusted up by 10% to compensate for possible disparity. The risk-adjusted PV cost of training and professional services over the three years was $217,775. See the section on Risks for more detail.

TABLE 7
Implementation, Baseline, And Additive Training Costs

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
F1	Implementation and ramp-up training, hours per engineer		320			
F2	Total patching and compliance related engineers		5	5	5	5
F3	Cost of network operations engineer, fully loaded, annually		$108,000	$108,000	$108,000	$108,000
F4	Cost of network operations engineer, fully loaded, hourly	F2/1920	$56.25	$56.25	$56.25	$56.25
F5	Advanced training, to leverage BigFix beyond patching, in hours			40	40	40
F6	Professional services		$80,000			
Ft	Implementation, baseline, and additive training costs	F1*F2*F4+F5*F2*F4+F6	$170,000	$11,250	$11,250	$11,250
	Risk adjustment	↑10%				
Ftr	**Implementation, baseline, and additive training costs (risk-adjusted)**		**$187,000**	**$12,375**	**$12,375**	**$12,375**

Source: Forrester Research, Inc.

Total Costs

Table 8 shows the total of all costs as well as associated present values (PVs), discounted at 10%. Over three years, the composite organization expects total costs to be a PV of slightly more than $2.1 million.

TABLE 8
Total Costs (Risk-Adjusted)

Ref.	Cost Category	Initial	Year 1	Year 2	Year 3	Total	Present Value
Etr	Software license and support costs	($1,450,000)	$0	($300,140)	($310,980)	($2,061,120)	($1,931,693)
Ftr	Implementation, baseline, and additive training costs	($187,000)	($12,375)	($12,375)	($12,375)	($224,125)	($217,775)
	Total costs (risk-adjusted)	**($1,637,000)**	**($12,375)**	**($312,515)**	**($323,355)**	**($2,285,245)**	**($2,149,468)**

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 BigFix 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).

Our research indicates two principal benefits:

- Some users of the BigFix Patch and Compliance solutions cited the additive benefit of the BigFix agent being flexible enough to run tasks beyond patching. The BigFix agent is extensible and incurs no added license costs to deliver additional endpoint customization. One interviewee in particular presented several differentiated use cases of BigFix, including the use of BigFix to deliver net-new software, remove applications, and change authentication methods.
- Integration with Carbon Black for endpoint threat detection in real time provides a single pane of glass for operations and security. Zero day threats, advanced persistent threats data, and other types of malicious activity are consolidated so that organizations can respond more quickly, limiting breaches as they occur.

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

TABLE 9
Benefit And Cost Risk Adjustments

Benefits	Adjustment
Business user productivity loss avoidance	↓ 30%
Costs	**Adjustment**
Initial and continued training costs	↑ 10%

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 risk that affects benefits is identified as part of the analysis:

› Business end users sometimes do not resort to technical assistance, as patching failure is not always made obvious in the form of application crashes. Due to this, technical support time savings may not have the same impact as pre-risk-adjusted numbers indicate. Some organizations also have a surplus of endpoint workstations as a buffer for capacity and thus, the end users of those organizations may experience a lower impact of mandatory manual patching. A significant downward risk-adjustment of 30% has been made to this benefit impact.

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

› Training in general is a concern for implementation. Customer users of BigFix Patch suggested inexperienced systems engineers may have a difficult initial learning period on BigFix. Other organizations indicated the desire to further leverage the framework for additional endpoint tasks, which may require additional training following the initial ramp-up phase.

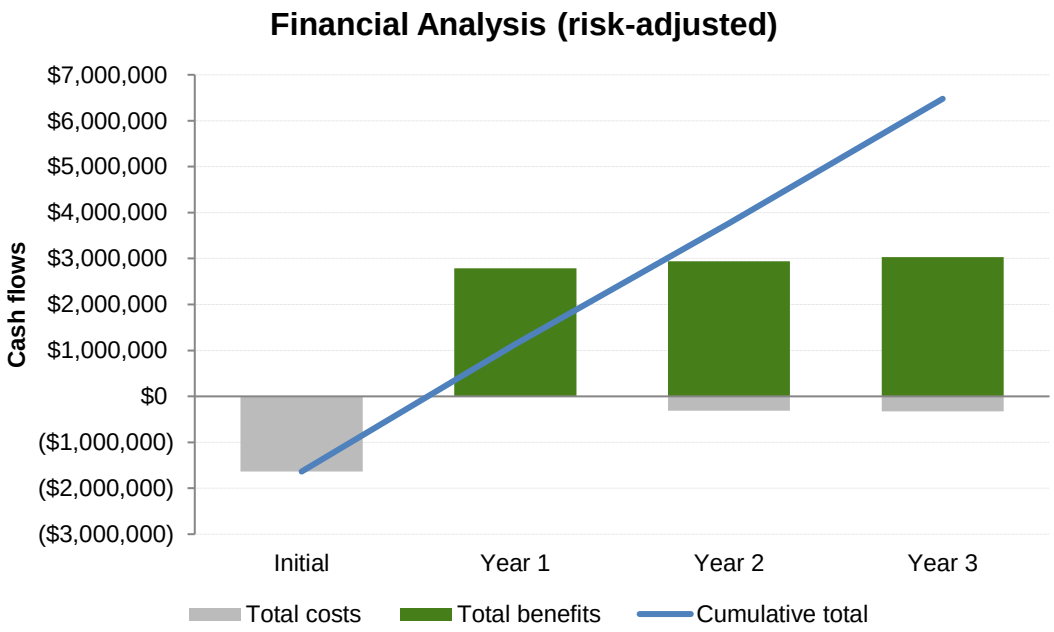
Table 9 shows the values used to adjust for risk and uncertainty in the cost and benefit estimates for the composite organization. Readers are urged to apply their own risk ranges based on their own degree of confidence in the cost and benefit estimates.

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 composite organization's investment in BigFix.

Table 10 below shows the risk-adjusted ROI, NPV, and payback period values. These values are determined by applying the risk-adjustment values from Table 9 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 10
Cash Flow (Risk-Adjusted)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Costs	($1,637,000)	($12,375)	($312,515)	($323,355)	($2,285,245)	($2,149,468)
Benefits	$0	$2,788,129	$2,944,223	$3,031,318	$8,763,670	$7,245,379
Net benefits	**($1,637,000)**	**$2,775,754**	**$2,631,708**	**$2,707,963**	**$6,478,425**	**$5,095,911**
ROI						**237%**
Payback period						**7 months**

Source: Forrester Research, Inc.

IBM BigFix: Overview

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

IBM BigFix is an endpoint management and security platform for IT infrastructure and security professionals. BigFix manages and secures the diversity of endpoints — from laptops and servers, to ATMs and POS terminals — that are commonplace in today's highly distributed work environments. BigFix enables clients to continuously monitor and enforce compliance policies with tens of thousands of out-of-the-box security and compliance checks, and includes multiplatform patching that delivers a 98%+ first-pass patch success rate. And, it does all this through a single shared platform that provides complete visibility and control into the status of all endpoints regardless of connectivity. The IBM BigFix platform includes BigFix Compliance, BigFix Inventory, BigFix Lifecycle, and BigFix Patch. Each module is rapidly enabled by switching on a license key.

With BigFix, security and operations teams can reduce endpoint attack surface while minimizing the cost, time and effort required to **discover**, **manage** and **secure** endpoints across the extended enterprise.

- **Discover** *quickly*: First identifies then provides accurate, real-time information about your endpoints regardless of operating system, location or connectivity.
- **Manage** *easily*: Automatically deploys and patches operating systems and 3rd party software, assesses application usage, monitors compliance, and inventories endpoints across multiple operating systems to simplify endpoint management.
- **Secure** *continuously*: Provides continuous monitoring, patching and compliance enforcement across endpoints.

IBM BigFix secures over 100 million endpoints worldwide across all major industries. The platform features the industry's most extensive plug-and-play remediation kit, the broadest industry compliance (PCI, DISA-STIG, and much more), in addition to meeting full US federal standards for cybersecurity. Using IBM BigFix, organizations will cut operational costs, compress endpoint management cycles and enforce compliance with unmatched ability to discover, manage and secure endpoints – in real time – regardless of operating system, location and connectivity.

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.

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.

Appendix C: Supplemental Material

Related Forrester Research

"Calculate The Business Impact And Cost Of A Breach," Forrester Research, Inc., November 17, 2016

Online Resources

More information about PCI DSS is available directly from the PCI Security Standards Council at: https://www.pcisecuritystandards.org

Appendix D: Endnotes

[1] "Raising The Bar For Cybersecurity," Center For Strategic & International Studies, February 12, 2013

[2] 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.

[3] "Understanding the Business Impact And Cost Of A Breach," Forrester Research Inc., January 15, 2015