A Forrester Total Economic Impact™
Study Commissioned By IBM
October 2017

The Total Economic Impact™ Of IBM Resilient

Cost Savings And Business Benefits Enabled By The Resilient Incident Response Platform

FORRESTER®

Table Of Contents

Project Director:
Henry Huang

Executive Summary

IBM provides a security incident response (IR) solution called Resilient that helps its customers address security incidents quickly in an automated and orchestrated manner. 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 Resilient. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of the Resilient platform on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed a Resilient customer with several years of experience using the solution. Forrester found that, as an incident response platform, the solution provides significant benefits by shortening the response time for security incidents through the enablement of automation and orchestration to security professionals — effectively shortening the time-to-contain security incidents. Security tools and devices across the enterprise are more frequently put into play sooner with dynamic playbooks that cut analysis and triage times required by incident responders.

Prior to using Resilient, the interviewed customer leveraged a ticketing system that provided little in the way of automation. This system yielded limited success, leaving the customer with little intelligence due to a lack of integration to the security tool stack. These limitations led to the need for a significant army of security professionals who needed to be specialized in a wide variety of security areas to be able to identify and contain threats.

Key Findings

Quantified benefits. The interviewed organization experienced the following risk-adjusted present value (PV) quantified benefits:

- **Orchestration and automation saved 25 minutes per security analyst and over an hour in total per security incident.** With over 350 cybersecurity incidents per week, the interviewed organization was saving nearly 22,750 hours of security analyst man-hours in the first year. Accounting for the rise in cybersecurity incidents over the years and the relative high cost of security analysts, this translated to a three-year savings worth $4.5 million in labor costs. The reduction in effort by the security analysts to handle incidents resulted in increased time for them to perform advanced analysis of threats and develop new countermeasures to further improve the organization's security posture.
- **End users benefited from quicker incident response and improved uptime.** While the Resilient platform did not offer direct improvement on the detection of incidents, it did allow incident responders to contain threats much more quickly after the initial detection. On a per incident basis, business users saved half an hour due to the reduction in time-to-contain as they no longer needed to wait as long for security analysts to investigate and perform remediation steps. Additionally, the quicker time-to-contain led to avoided image restores and wider scale remediation action on the endpoints. In all, the organization saved between 11,830 and 15,645 hours per year with the Resilient platform.

Key Benefits

Orchestration and automation savings for incident response:
$4,502,964

End user productivity recapture improvement:
$1,346,720

Existing security asset value realization improvement:
$1,760,331

ROI
104%

Benefits PV
$7.6 million

NPV
$3.9 million

Payback
9 months

- **Resilient, as the incident response platform, brought visibility to the efficacy of existing security tools, enabling security professionals to realize the full potential of the organization's library of tools.** With Resilient acting as the central dashboard orchestrating the response to security incidents, security professionals were able to centrally collect data and determine points in the security architecture that were less responsive. With the insight, security professionals could identify the exact point of failure and choose to either reconfigure the tool or substitute the tool with a more effective replacement. Security tools are expensive investments, and Resilient helps professionals reaffirm that these investments are working as advertised.

Unquantified benefits. The interviewed organization experienced the following benefits, which are not quantified for this study:

- **Resilient provides instant dashboarding to help expedite the audit process and reduce scrutiny from regulatory bodies.** Most enterprises are audited on the security front numerous times a year and provide management reporting on security incidents at an even higher frequency. By being able to centralize security response data in the Resilient platform, the interviewed organization can provide internal and external auditors with data that reduces security professional effort and auditor effort.

- **The organization saw continual security posture improvement from newly free time to security analysts.** Whereas the interviewed organization was once constantly fighting fires, it is now doing deep analysis into threats to continually improve its processes and defenses. The value of this has not been calculated, but it certainly helps the organization's security individuals sleep better at night knowing that they are better postured to prevent massive fallout from situations like recent, widely publicized security breaches.

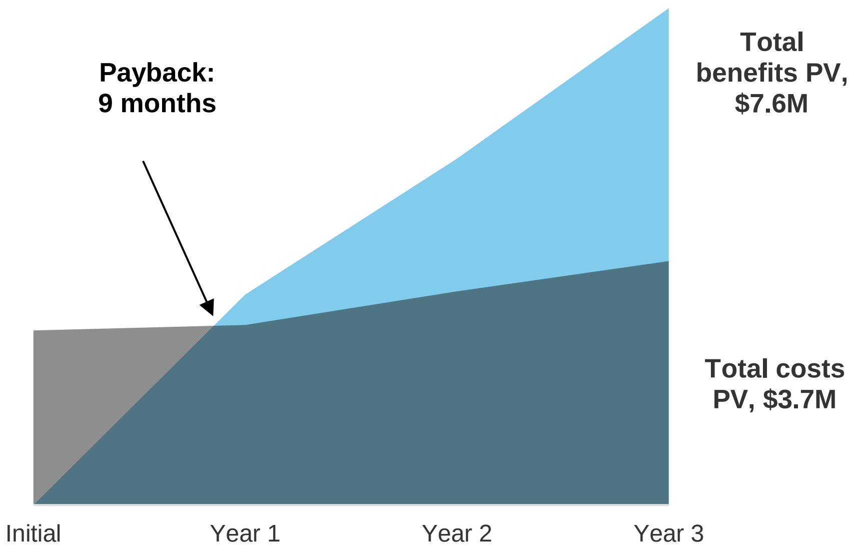
Costs. The interviewed organization experienced the following risk-adjusted costs:

- **License and support costs amounted to $3,469,440 over three years.** The license costs are comprised of both user licenses for the incident responders as well as the primary software licenses for production and development environments. Standard support and service has also been accounted for in this category.

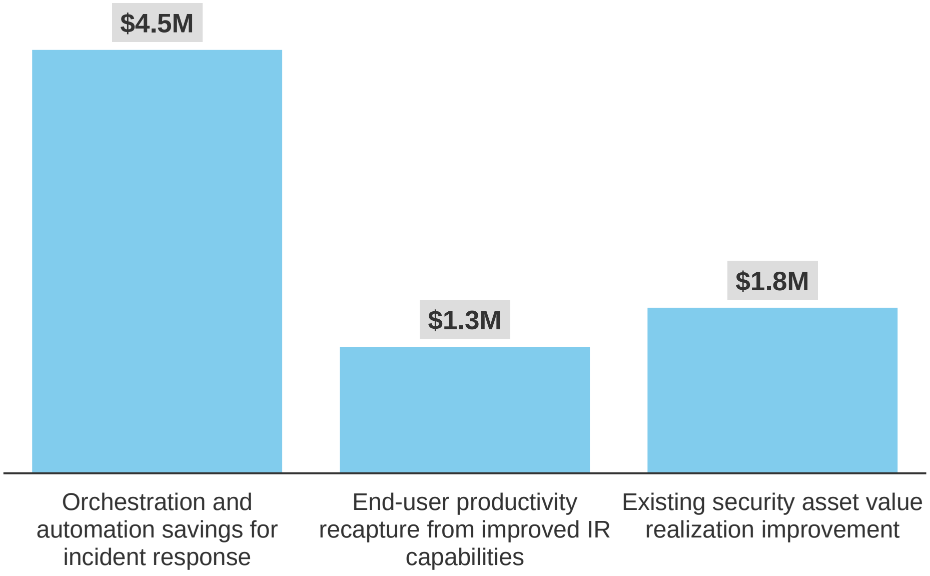
- **Software integration and process buildouts are a low but ongoing cost.** This cost category is inclusive of deployment, orchestration buildouts, and integration buildouts with existing security tools. Some APIs are included, but as the interviewed organization's security architecture was complex and tools are numerous, the custom buildout of these integrations was necessary and cost $266,745 over three years.

Forrester's interview with an existing customer and subsequent financial analysis found that the interviewed organization experienced PV benefits of $7,610,015 over three years versus PV costs of $3,736,185, adding up to a net present value (NPV) of $3,873,830 and an ROI of 104%.

Financial Summary



Benefits (Three-Year)



TEI Framework And Methodology

From the information provided in the interview, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering implementing IBM Resilient.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that IBM Resilient can have on an organization:

The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

DUE DILIGENCE
Interviewed IBM stakeholders and Forrester analysts to gather data relative to Resilient.

CUSTOMER INTERVIEW
Interviewed one organization using Resilient to obtain data with respect to costs, benefits, and risks.

FINANCIAL MODEL FRAMEWORK
Constructed a financial model representative of the interview using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewed organization.

CASE STUDY
Employed four fundamental elements of TEI in modeling IBM Resilient’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.

DISCLOSURES

Readers should be aware of the following:

This 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 Resilient.

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 names for the interviews but did not participate in the interviews.

The Resilient Customer Journey

BEFORE AND AFTER THE RESILIENT INVESTMENT

Interviewed Organization

For this study, Forrester interviewed an IBM Resilient customer with multiple years of experience using the platform:

- This is a financial services organization with a worldwide footprint.
- It employs more than 15,000 full-time equivalents (FTEs) and has revenues in the tens of billions.
- It has a cyber defense team of approximately 150 security professionals.
- This is an organization that is held accountable to multiple regulatory bodies; effective security posture and processes are instrumental to meeting the standards.

Key Challenges

Coming from an existing state of using a homebrew incident response plan that incorporated the use of an IT ticketing system, the security team at the organization felt that its needs were largely unmet. There was a clear lack of visibility and integration into various security tools, providing for weak documentation and a complete absence of automation*. “We had a clear desire for so much more to improve our efficiency*, *and when we realized that the existing solution failed at 99% of our wants, it was time to move on*,” said the VP of cyber defense. Further, “The messaging from the top was that we had these solutions already — but our own analysis suggested it [the old solution] was clearly incapable of doing what we needed to be effective.”

> ““Before we had automation and the things we’re doing with Resilient today, our incident responders were in constant firefighter mode. They were dealing with incident after incident without break. It was a constant struggle.”
>
> *VP of cyber defense, financial services organization*

- **There was a lack of integration with various security tools.** Lacking integration with the security stack resulted in very little documentation and metrics for consumption. Further still, the effort required to triage and actually drive to the root cause of the incidents was largely manual and time-consuming. The old system served as a way to mark issues but aided very little in actually feeding information to security professionals so that they could take proper action on containment.
- **A lack of playbooks meant that every situation was assessed manually when it could have been automated.** Incidents arose in a variety of forms and attack vectors. Incident responders would manually go through the analysis process, pulling information from various tools to determine the proper course of action. Said simply, the security analysts needed to enact different containment processes on every incident. The result was that different analysts performed containment and remediation in different ways, piling up on the inefficiencies.

- **There was a clear disconnect on automation and orchestration.** Without integration, there was no automation. No single centralized point of control was dictating the hundreds of remedial actions that had previously been seen. Again, these actions took manual labor, and remediation was left to the wildly varying methods between the incident responders.
- **Security professionals were a scarce commodity.** Being in a constant firefight mode required a large force of incident responders who were each versed in a wide variety of security elements. As the need for these professionals grew, it was more and more costly to add to this cyber defense group. Intelligent automation was a clear solution to reduce the laborious effort of analysis and containment.

> “Beyond just automation, what really appealed to us was [Resilient’s] dynamics playbooks. With it, we’re able to handle evolving and multistage incidents. An incident could start with a phishing attack, then lead to a malware attack and data infiltration. Each of these pieces in the attack series requires a different response.”
>
> *VP of cyber defense, financial services organization*

Decision To Use Resilient

After an extensive request for proposal (RFP) and business case process evaluating multiple vendors, the interviewed organization chose Resilient and began deployment:

- The organization chose Resilient because of its dynamic playbooks — the ability to follow the path of incidents and act dynamically through the stages of breach from initial identification to internal network proliferation and widespread data corruption.
- By the end of the bake-off proof of concept (POC), the organization had built simple integration that translated into significant automation savings for all incident responders.
- The Resilient solution was running and integrated with many of the organization’s mission-critical security tools within two weeks.

Key Results

The interview revealed that key results from the Resilient investment include:

- **Integration with existing security toolsets allowed for a dramatic automation improvement.** By integrating with existing tools, Resilient took initiative to present the relevant data on issues to security analysts and then completed the required actions through the tools once approved by analysts. In short, orchestration and automation eliminated a large portion of investigative work from the detect, analyze, contain, and eradicate workflow.
- **Like security practitioners, business end users found greater productivity.** As the time-to-contain shortened from automation, business users enjoyed higher levels of uptime at their workstations, directly feeding value back to the organization in productive output. Disruptions were reduced in scale; even IT help desk effort was reduced as reimage sessions or virtual machine (VM) recomposes were minimized by fast action to resolve incidents.

> ““We’ve done heavy integrations with our security tools into Resilient and have been able to find significant automation savings as a result.”
>
> *VP of cyber defense, financial services organization*

- **Having a capable incident response platform was the final piece of the security puzzle to tackle increasingly complex attacks.** While detection and remediation were still largely left to the existing tools in the security group, the time to take action and contain threats had dramatically improved. Being without an IR platform capable of orchestration was like having the tools but having to wait to decide when and where to use which specific tool for the task.

> "That ability to close down incidents that much quicker brings our organization a lot of value. Even though we're talking about minutes at times — minutes can make the difference between containment or a major breach."
>
> *VP of cyber defense, financial services organization*

Financial Analysis

QUANTIFIED BENEFIT AND COST DATA

Total Benefits

REF.	BENEFIT	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Atr	Orchestration and automation savings for incident response	$1,426,425	$1,804,428	$2,282,601	$5,513,454	$4,502,964
Btr	End user productivity recapture from improved IR capabilities	$472,017	$542,820	$624,242	$1,639,079	$1,346,720
Ctr	Existing security asset value realization improvement	$1,650,000	$165,000	$165,000	$1,980,000	$1,760,331
	Total benefits (risk-adjusted)	**$3,548,442**	**$2,512,247**	**$3,071,843**	**$9,132,533**	**$7,610,015**

The table above shows the total of all benefits across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the interviewed organization expects risk-adjusted total benefits to be a PV of more than $7.6 million.

Orchestration And Automation Savings For Incident Response

Following the deployment of IBM Resilient, the interviewed organization realized a significant gain in the automation and, in turn, a reduction of security analyst effort. Whereas the existing solution offered very limited or no data from the relevant security pieces, Resilient, once integrated with the security stack, was able to provide vivid detail on security incidents and enact on containment and remediation actions with minimal input from security personnel. From the interview, Forrester determined:

- Security experts can see from a centralized command center the initial point of detection and any further exploitation caused by the incident. Using dynamic playbooks, the Resilient platform visibly displays the actions required and can execute with a single click from the incident responders.
- In the previous state where incidents morphed and affected multiple points across the network, incident responders would rely on multiple analysts to determine and contain these threats. With Resilient, the organization can identify these threats and reduce the number of actual personnel necessary to mitigate the issues.
- The interviewee stated that the longest part of the incident response workflow was the analysis and triage on the incidents. Resilient effectively reduced the effort involved by over 80%. Accounting for three analysts who may have been involved in these incidents, their individual effort was reduced by nearly 25 minutes for analysis, resulting in a total of 1.25 hours saved per incident.
- At an average rate of 350 incidents occurring on a weekly basis, we estimate that 22,750 hours were saved in the initial year by the security responders and analysts.

Calculations have been adjusted for an increase in efficiency through optimization of orchestrations and an increase in incidents that will occur

Security analysts can recoup 25 minutes per incident with automation. In many cases where there is more than one analyst involved, the time saved is even greater.

over the ensuing years. Forrester estimates security incidents to increase by nearly 15% at financial services organizations on a year-over-year basis.

- Incidents will grow in frequency by 15% year over year.
- Tuning and optimization of the orchestration through further integration with security tools will increase the time saved by security professionals by 10% year over year.
- At a rate of $110,000 per year, accounting for benefits, security professionals earn the equivalent of $66/hour.

With the time saved, the security analysts were not necessarily relinquished — especially as they are highly sought after. Instead, the interviewed organization allocated these analysts to spend the newly found time saved from automation to perform deep level analysis — such as determining the advanced behavior of malware or optimizing rule sets and orchestration so that incidents are handled even faster in the future.

While Forrester believes the value of automation and orchestration to be undeniable, readers should be aware of the potential impact risk of exacting the benefits if an established IR plan is already in place. Consideration of this risk should be for organizations that may already be very mature in incident response and security posture — factors that may diminish the value cited in this category.

To account for this risk, Forrester adjusted this benefit downward by 5%, yielding a three-year risk-adjusted total PV of $4,502,964

.

Impact risk is the risk that the business or technology needs of the organization may not be met by the investment, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for benefit estimates.

Orchestration And Automation Savings For Incident Response: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
A1	Cybersecurity incidents annually	350 incidents per week in Year 1, growing at 15% yearly	18,200	20,930	24,070
A2	Triage and incident analysis effort reduced with automation and orchestration, in hours per incident	Assumption of three analysts allocated per incident (rounded to nearest hundredth)	1.25	1.38	1.51
A3	Hours saved annually by security analysts with Resilient orchestration and automation	A1*A2	22,750	28,779	36,405
A4	Cybersecurity analyst hourly compensation, fully burdened	$110,000*1.2x benefits multiplier/2,000 hours	$66	$66	$66
At	Orchestration and automation savings for incident response	A3*A4	$1,501,500	$1,899,398	$2,402,738
	Risk adjustment	↓5%			
Atr	**Orchestration and automation savings for incident response (risk-adjusted)**		**$1,426,425**	**$1,804,428**	**$2,282,601**

End User Productivity Recapture From Improved IR Capabilities

IBM Resilient does not enable quicker detection of malicious activity — this is a function of the existing security infrastructure. Likewise, Resilient does not perform the remediation. Instead, the Resilient solution accelerates the incident response workflow once an incident has been detected, leading to a significantly reduced time to enact the remediation and containment procedures — otherwise explained as the period of time between mean-time-to-detect (MTTD) and mean-time-to-contain (MTTC).

Incident responders previously required between 20 and 30 minutes to analyze and determine a proper containment approach, which has largely been eliminated due to Resilient's automation and orchestration to carry out containment measures. End users who operate on the enterprise network would often find that their machines were locked out upon detection, resulting in a period of downtime until the endpoint was contained and remediated. With the reduction in the period between MTTD and MTTC, the end users are able to recover this time to be spent productively.

Additionally, a number of incidents often cause deeper and collateral damage as time passes. A hastened action to respond to the incident often reduces the need for deeper-level remediation/recovery techniques, such as a complete reimage.

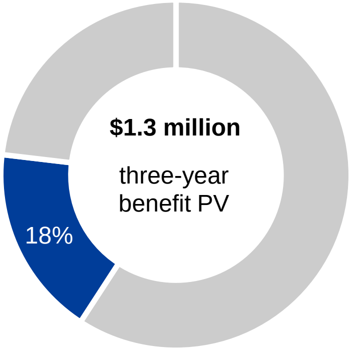
For the interviewed organization, Forrester found that:

- For each of the incidents occurring across the enterprise, end users are saving a minimum of 30 minutes per incident. They are repurposing those 30 minutes into productive output.
- The percentage of incidents that ultimate may have necessitated full restores or VM recompose without a hastened response is 10%.
- The average time for reimage, recompose, or full remediation is estimated at 1.5 hours — time that would have been taken away from user productivity.

The reduction in productivity recaptured can vary depending on:

- The number of applications installed on the endpoint stations.
- The time needed to reimage/recompose.
- The detection efficacy of security measures already in place.

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year risk-adjusted total PV of $1,346,720.



End user productivity recapture: **18%** of total benefits

End user productivity lost to security incidents is a metric that many organizations overlook.

Organizations that generate greater revenue per FTE will reap higher levels of benefit in their instances.

End User Productivity Recapture From Improved IR Capabilities: Calculation Table

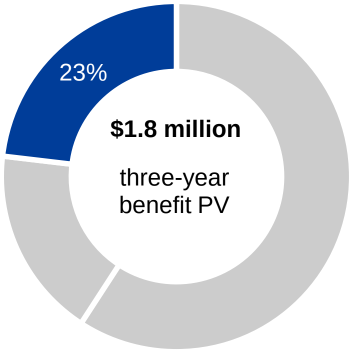
REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
B1	End user uptime improvement from automation and orchestration of containment, in hours per incident		0.5	0.5	0.5
B2	Hours saved annually by end users	A1*B1	9,100	10,465	12,035
B3	End user hourly compensation, fully burdened	$70,000*1.2x benefits multiplier/ 2,000 hours	$42	$42	$42
B4	Reimage/full scale remediation situations avoided, measured in hours	A1*10% of incidents*1.5 hours per incident	2,730	3,139.5	3,610.5
Bt	End user productivity recapture from improved IR capabilities	B2*B3+B3*B4	$496,860	$571,389	$657,097
	Risk adjustment	↓5%			
Btr	**End user productivity recapture from improved IR capabilities (risk-adjusted)**		**$472,017**	**$542,820**	**$624,242**

Existing Security Asset Value Realization Improvement

Enterprises today are rightfully concerned about their security posture and allocate increasing amounts to security budgets — especially given the number of high-profile breaches that frequent the news. With an assortment of tools, how do organizations determine the efficacy of these individual tools following POC and deployment? Forrester's interview with the customer organization revealed that while POCs and bake-offs can be useful for a first impression, sometimes the solutions are not quite as effective as originally expected. With Resilient as a central point of orchestration and data collection, the interviewed organization gained visibility into its collective security stack and was better able to evaluate its existing investments.

- Upon integration with Resilient, the security team was able to collect information as to which defense mechanisms were more effective, if effective at all, on detection or containment of malicious activity.
- The interviewed organization was able to clearly delineate whether its browser sandboxing and database access management were working, as results were all reported back to Resilient.
- The organization estimated that over $1.5 million of its investments were not properly configured or working to the standard promised, resulting in either reconfiguration or removal of those services.
- Detection was primarily noted in the first year of Resilient deployment with smaller incremental gains in the years after.
- Recognition of the points of failure saved an additional amount of labor, when the security team would have passed false negatives or exerted additional effort on false positives.

Value recovered from the points of failure was estimated at a PV of $1,760,331 over the course of three years of usage.



Existing security asset value realization: 23% of total benefits

Existing Security Asset Value Realization Improvement: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
C1	Value of assets found to be misconfigured or underperforming		$1,500,000	$150,000	$150,000
C2	Avoided extraneous triage and analysis labor costs relating to nonperforming existing security assets		$150,000	$15,000	$15,000
Ct	Existing security asset value realization improvement	C1+C2	$1,650,000	$165,000	$165,000
	Risk adjustment	0%			
Ctr	**Existing security asset value realization improvement (risk-adjusted)**		**$1,650,000**	**$165,000**	**$165,000**

Unquantified Benefits

Beyond the quantified benefits represented above, the customer organization identified the dramatically improved security posture now present. Time previously spent on remediating incidents is now spent to do advanced heuristics on malware and threats — understanding the underlying nature to prevent additional outbreaks in the present and future. What is the value in that? Forrester has determined the following on breaches:

- 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. While it is impossible to say what percentage of organizations are breached, we know that it is a matter of when, rather than if. Organizations that have a solid IR plan and perform deep-level analysis on different threat vectors stand a much-improved chance on minimizing damage.
- Breaches that are not addressed with immediacy contain a number of financial ramifications in the short and long run. Lost revenues, legal settlements, regulatory fines from the likes of the Federal Financial Institutions Examination Council (FFIEC) and the Payment Card Industry (PCI), and long-term brand erosion should all be considered.

While prevention and detection are always important, incident response formulas should be equally as critical in the overall security scheme of the organization.

> "Resilient allows my team to operate much more efficiently, which in turn reduces the overall risk that threats pose to the organization. And that's what truly matters."
>
> - VP of cyber defense, financial services organization

Flexibility

The value of flexibility is clearly unique to each customer, and the measure of its value varies from organization to organization. There are multiple scenarios in which a customer might choose to implement Resilient and later realize additional uses and business opportunities, including:

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for a 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.

- **Resilient incident response is agnostic with the tools that it integrates with and orchestrates.** As newer and more capable prevention, detection, logging, and remediation tools are introduced to the security ecosystem, Resilient can continue to serve as the central orchestration mechanism with these tools and perpetually increase automation to security teams.

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A).

Total Costs

REF.	COST	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Dtr	License and support costs	$2,637,250	$0	$527,450	$527,450	$3,692,150	$3,469,440
Etr	Initial and ongoing orchestration, process, and integration buildouts	$36,960	$92,400	$92,400	$92,400	$314,160	$266,745
	Total costs (risk-adjusted)	**$2,674,210**	**$92,400**	**$619,850**	**$619,850**	**$4,006,310**	**$3,736,185**

The table above shows the total of all costs across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the interviewed organization expects risk-adjusted total costs to be a PV of slightly over $3.7 million.

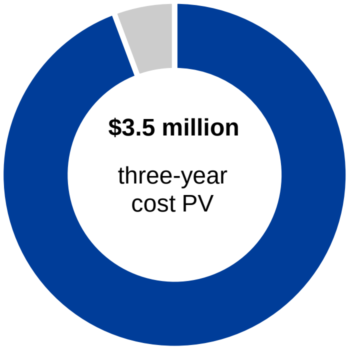
License And Support Costs

From the interview, Forrester has determined that the majority of costs are borne from the following items:

- The customer purchased a base software license, along with the user seat licenses for individual incident responders. The licensing purchased by the interviewed organization is of the perpetuity type.
- Support and service were a continued cost assumed on a yearly basis following the initial year of usage.
- Lastly, a development environment for the Resilient platform was necessary to develop integrations into the organization's 50-plus existing security tools.

Costs in this study are represented at near list pricing, reflecting only slight discounting. Purchases of other IBM security solutions may drive the cost of the Resilient solution down beyond what is reflected here. We encourage readers to explore the options with IBM or partners.

Compiling the costs of the licenses and service and support, the interviewed organization likely assumed PV costs of $4,415,651 after three years of usage.



Cost of license and service: **93%** of total costs

Perpetuity license pricing is reflected in this study. Purchases of additional IBM products from the IBM security portfolio may further decrease the reader's cost basis.

License And Support Costs: Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
D1	Base license and user licenses		$2,222,000		$278,300	$278,300
D2	Development environment license		$415,250		$83,050	$83,050
D3	Support and service				$166,100	$166,100
Dt	License and support costs	D1+D2+D3	$2,637,250	$0	$527,450	$527,450
	Risk adjustment	0%	□			
Dtr	**License and support costs (risk-adjusted)**		**$2,637,250**	**$0**	**$527,450**	**$527,450**

Initial And Ongoing Orchestration, Process, And Integration Buildouts

The IBM Resilient platform can be deployed outright with minimal effort and comes with a number of standard dynamic playbooks. As no two organizations are the same, however, process remodeling and security tool integration need to be undertaken to fully realize the automation and orchestration capabilities of Resilient. The interviewed organization started integration and process augmentation for the mission-critical tools within its stack of more than 50 tools.

- Initial planning and scripting of the various integrations required the efforts of five security FTEs over two weeks, committing a real total of 400 hours in this time. With this effort, the organization had integrated Resilient with its mission-critical and most commonly used tools. Automation savings almost immediately accrued, but the efforts for process engineering and tool integration didn't stop there.
- Over the next three years, the organization continued to integrate tools to continually improve the efficiency of incident response, cutting manual processes where it could. The effort spent by a Python developer equated to approximately half an FTE on an ongoing basis.
- The result was a continued reduction and effectiveness in the organization's ability to contain incidents in shorter periods of time.

Some organizations may lack the developer resources for advanced Python development in the security space; as such, there exists the risk that additional effort might need to be allocated to the tool integration process. Additionally, different organizations have varying complexities in their security architecture that may require additional effort. As such, Forrester has overlaid this cost category with what we identify as implementation risk.

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year risk-adjusted total PV of $266,745.

Two weeks
Initial implementation and deployment time

On average, the interviewed customer allocated 1,000 hours of developer effort to further finetune and optimize the response schemes within its security stack.

Implementation risk is the risk that a proposed investment may deviate from the original or expected requirements, resulting in higher costs than anticipated. The greater the uncertainty, the wider the potential range of outcomes for cost estimates.

Initial And Ongoing Orchestration, Process, And Integration Buildouts: Calculation Table

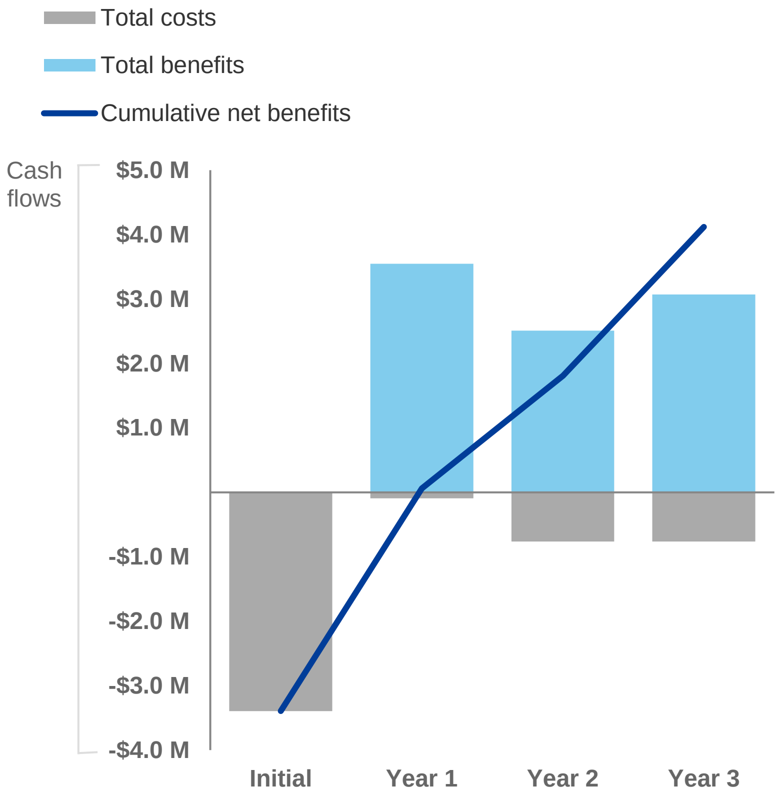
REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
E1	Initial hours required for process assessments, formation, and orchestration scripting	5 FTEs, 2 weeks	400			
E2	Ongoing orchestration and integration scripting improvements post initial deployment, annually	0.5 FTEs, ongoing		1,000	1,000	1,000
E3	Cost of senior-level Python developer fully burdened, hourly	$140,000*1.2x benefits modifier/2,000 hours	$84	$84	$84	$84
Et	Initial and ongoing orchestration, process, and integration buildouts	(E1+E2)*E3	$33,600	$84,000	$84,000	$84,000
	Risk adjustment	↑10%				
Etr	**Initial and ongoing orchestration, process, and integration buildouts (risk-adjusted)**		**$36,960**	**$92,400**	**$92,400**	**$92,400**

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

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. Forrester assumes a yearly discount rate of 10% for this analysis.

Cash Flow Chart (Risk-Adjusted)



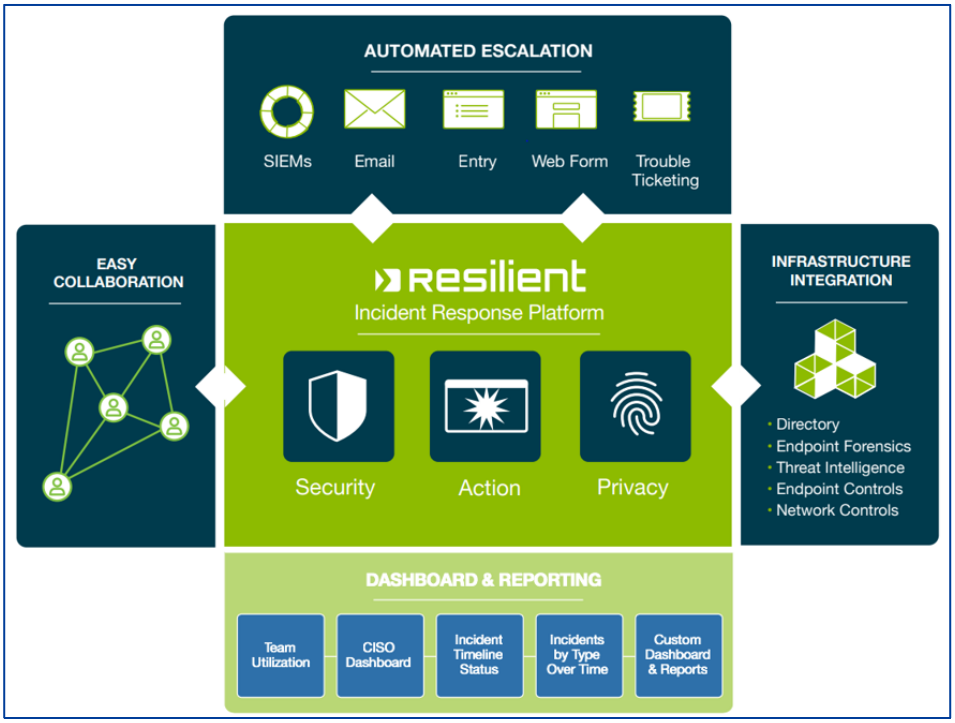
These risk-adjusted ROI, NPV, and payback period values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Table (Risk-Adjusted)

	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Total costs	($2,674,210)	($92,400)	($619,850)	($619,850)	($4,006,310)	($3,736,185)
Total benefits	$0	$3,548,442	$2,512,247	$3,071,843	$9,132,533	$7,610,015
Net benefits	($2,674,210)	$3,456,042	$1,892,397	$2,451,993	$5,126,223	$3,873,830
ROI						104%
Payback period						9.3 months

IBM Resilient: Overview

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

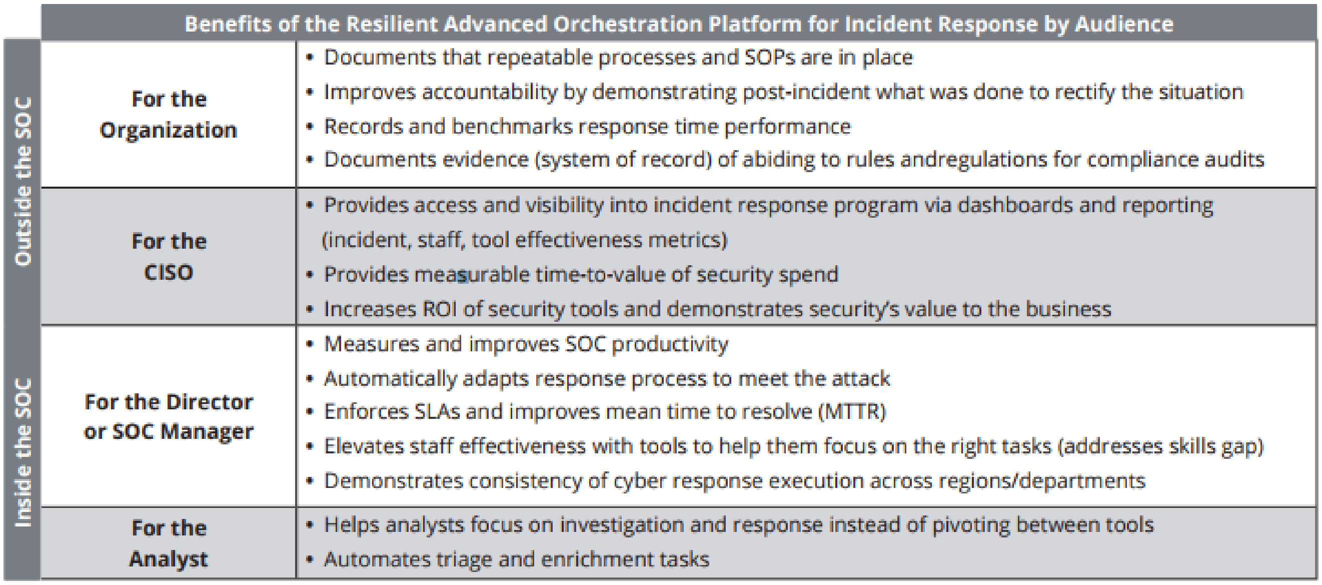


The Resilient Incident Response Platform (IRP) is the leading platform for orchestrating and automating incident response processes. With Resilient, security organizations can significantly drive down their mean time to find, respond to, and remediate using the platform. It quickly and easily integrates with organizations' existing security and IT investments, creating a single hub to drive fast and intelligent action. The platform's advanced orchestration capabilities enable adaptive response to complex cyber threats.

The latest orchestration innovations to the Resilient IRP include:

- **Dynamic Playbooks:** Provides the agility, intelligence, and sophistication needed to contend with complex attacks. Dynamic Playbooks automatically adapts to real-time incident conditions and ensures repetitive, initial triage steps are complete before an analyst even opens the incident.
- **Visual Workflows:** Enables analysts to orchestrate incident response with visually built, complex workflows based on tasks and technical integrations.
- **Incident Visualization:** Graphically displays the relationships between incident artifacts or indicators of compromise (IOCs) and incidents in an organization's environment.

The Resilient IRP enables cyber resilience across the organization:



	Benefits of the Resilient Advanced Orchestration Platform for Incident Response by Audience	
Outside the SOC	For the Organization	• Documents that repeatable processes and SOPs are in place • Improves accountability by demonstrating post-incident what was done to rectify the situation • Records and benchmarks response time performance • Documents evidence (system of record) of abiding to rules andregulations for compliance audits
	For the CISO	• Provides access and visibility into incident response program via dashboards and reporting (incident, staff, tool effectiveness metrics) • Provides measurable time-to-value of security spend • Increases ROI of security tools and demonstrates security's value to the business
Inside the SOC	For the Director or SOC Manager	• Measures and improves SOC productivity • Automatically adapts response process to meet the attack • Enforces SLAs and improves mean time to resolve (MTTR) • Elevates staff effectiveness with tools to help them focus on the right tasks (addresses skills gap) • Demonstrates consistency of cyber response execution across regions/departments
	For the Analyst	• Helps analysts focus on investigation and response instead of pivoting between tools • Automates triage and enrichment tasks

Appendix A: Total Economic Impact

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.

Total Economic Impact Approach

Benefits represent the value delivered to the business by the product. The TEI methodology places 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.

Costs consider all expenses necessary to deliver the proposed value, or benefits, of the product. The cost category within TEI captures incremental costs over the existing environment for ongoing costs associated with the solution.

Flexibility represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. Having the ability to capture that benefit has a PV that can be estimated.

Risks measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations in 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.

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.

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.

RETURN ON INVESTMENT (ROI)

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

DISCOUNT RATE

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

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.