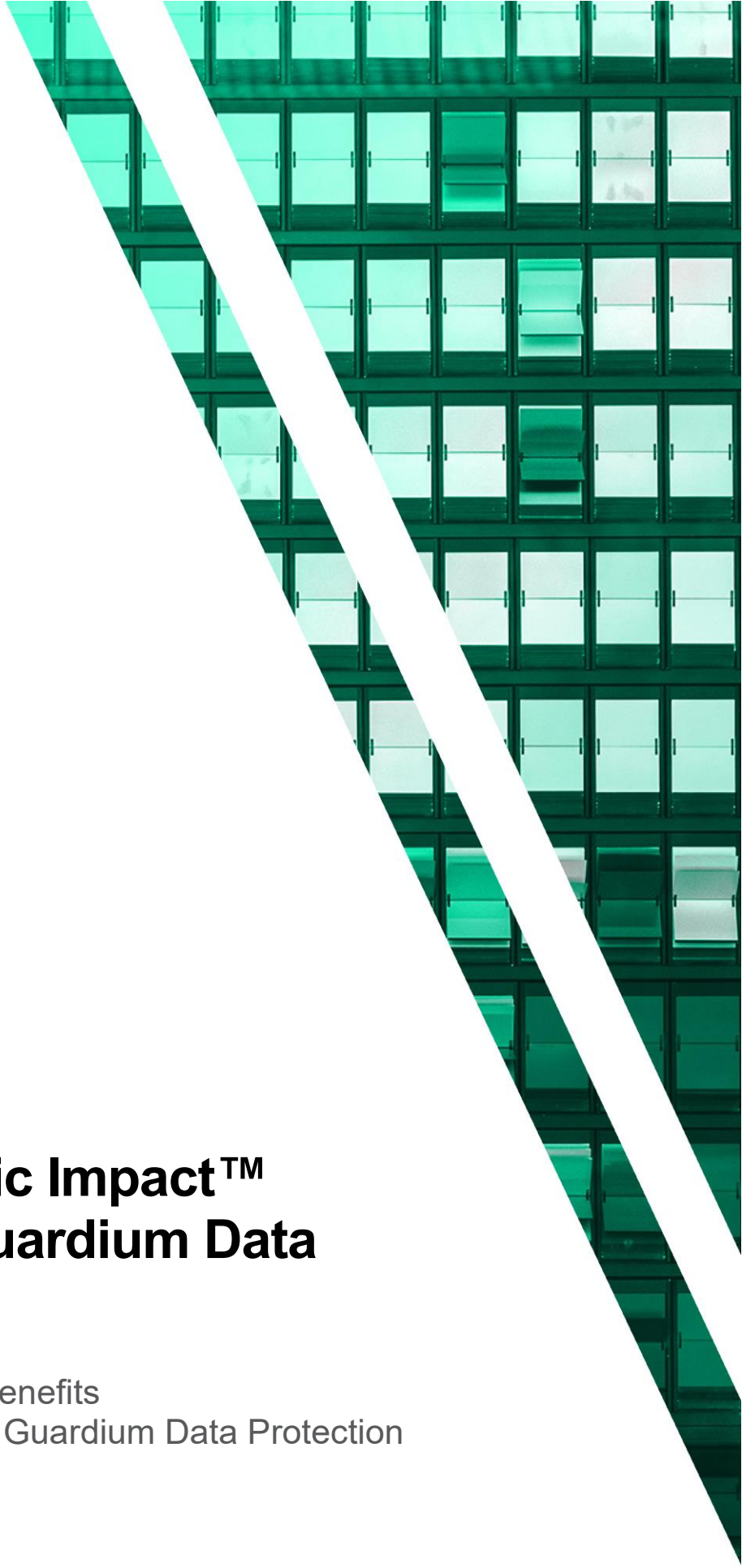
FORRESTER®



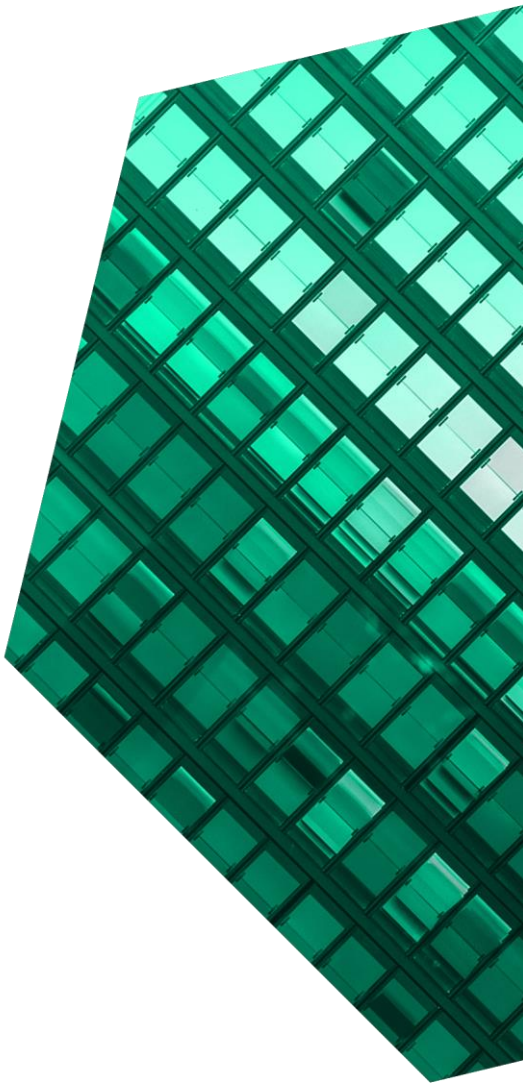
The Total Economic Impact™ Of IBM Security Guardium Data Protection

Cost Savings And Business Benefits Enabled By The IBM Security Guardium Data Protection

JUNE 2023

Table Of Contents

Consulting Team: Maria Kulikova
Carmen Serradilla Ortiz



ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key transformation outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute on their priorities using a unique engagement model that tailors to diverse needs and ensures lasting impact. For more information, visit forrester.com/consulting.

Executive Summary

Organizations are increasingly looking for a database security solution that can easily integrate with various types of databases, provide excellent data security, and meet compliance requirements. IBM Security has developed a product that addresses these market needs. The IBM Security Guardium Data Protection product is flexible and provides prebuilt auditing workflows and visibility into security assessment via its centralized reporting functionality.

The data security market is dynamic and competitive. Organizations are searching for solutions that can enable data security controls for all types of databases and support compliance regulations. IBM Security Guardium Data Protection empowers customers to secure and protect their data environments, automate reporting, and provide the necessary processes for auditing and compliance.

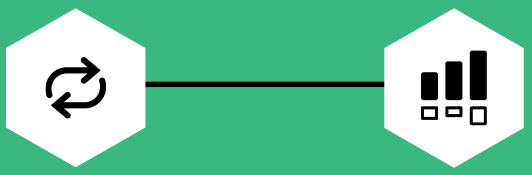
IBM Security commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying IBM Security Guardium Data Protection.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of the IBM Security Guardium Data Protection product on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four representatives with experience using the IBM Security Guardium Data Protection product. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that is a global firm with revenue of $5 billion per year.

Prior to using the IBM Security Guardium Data Protection product, these interviewees noted how their organizations used manual processes to aggregate security information across different databases and to produce reports for auditing. These limitations led to a lack of visibility into the overall data security at their organizations, which potentially exposed them to data breaches and made them unable to efficiently respond to audit requests.

After the investment in the IBM Security Guardium Data Protection product, the interviewees were able to monitor all data through a centralized location, get standard reports across databases, and use the prebuilt workflows for audits. Key results from the investment include productivity gains due to data

KEY STATISTICS



Return on investment (ROI)
406%

Net present value (NPV)
$4.70M

Auditing time saved

70%

security automation, gains in auditing processes efficiencies, and reduced risk of a data breach.

KEY FINDINGS

Quantified benefits. Three-year, risk-adjusted present value (PV) quantified benefits for the composite organization include:

- **Increased database security monitoring automation.** The composite organization experiences 25% less demand on DSAs' (Data Security Analysts') time since the IBM Security Guardium Data Protection product streamlined security monitoring and centralized database security reporting. This benefit accounts for $811,300 over three years.
- **Increased auditing efficiencies.** The composite organization realizes significant productivity savings for the DSAs due to the improved automated auditing workflows. Overall, it takes 70% less time for DSAs to complete tasks IBM Security Guardium assists with. This saves the composite organization $2.2 million over three years.
- **Increased ability to meet compliance regulations.** By implementing IBM Security Guardium Data Protection, the composite organization has the necessary prebuilt audit and compliance workflows that allow it to quickly respond to audit requests and prove compliance. This benefit accounts for $1.1 million over three years.
- **Increased database security.** The composite organization can detect potential data risks within its environment, allowing security specialists to understand which databases need stronger data protection and reduce the risk of a data breach. This benefit accounts for $1.7 million over three years.

Unquantified benefits. Benefits that provide value for the composite organization but are not quantified in this study include:

- **Integration compatibility with a multitude of databases and other enterprise tools.** This flexibility helps the composite organization to deploy the product quickly and to continue to scale up as needed.
- **User community support to drive better customer experience.** IBM Security provides extensive online learning tools, and an annual customer event, TechXchange (formerly IBM Security Master Skills University), provides great opportunities for customer support from other customers and IBM itself.

Costs. Three-year, risk-adjusted PV costs for the composite organization include:

- **Implementation and maintenance costs.** The initial deployment by the composite organization team and ongoing maintenance costs to the composite organization is $96,000.
- **Total fees.** The composite organization incurs an annual license fee. The fee includes dedicated deployment services and customer support. The composite organization pays an initial fee of $690,000 and then $150,000 in annual license fees.

The representative interviews and financial analysis found that a composite organization experiences benefits of $5.86 million over three years versus costs of $1.16 million, adding up to a net present value (NPV) of $4.70 million and an ROI of 406%.

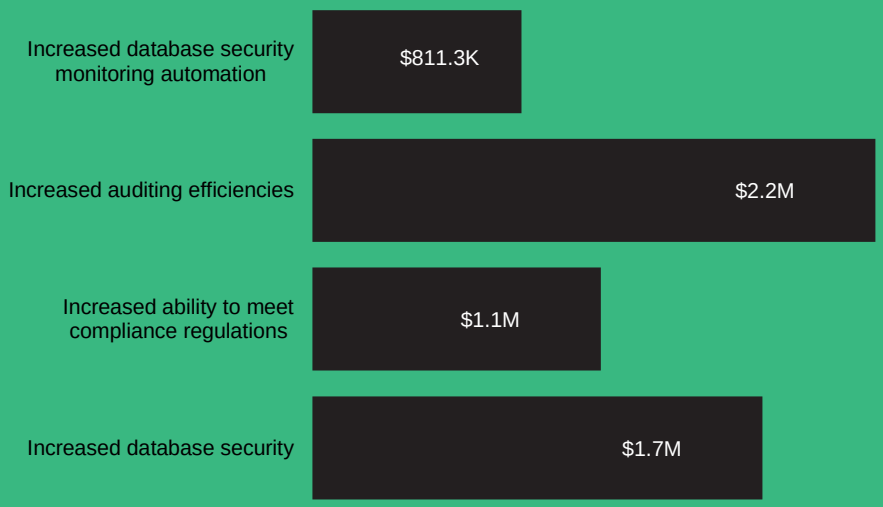
ROI
406%

BENEFITS PV
$5.86M

NPV
$4.70M

PAYBACK
<6 months

Benefits (Three-Year)



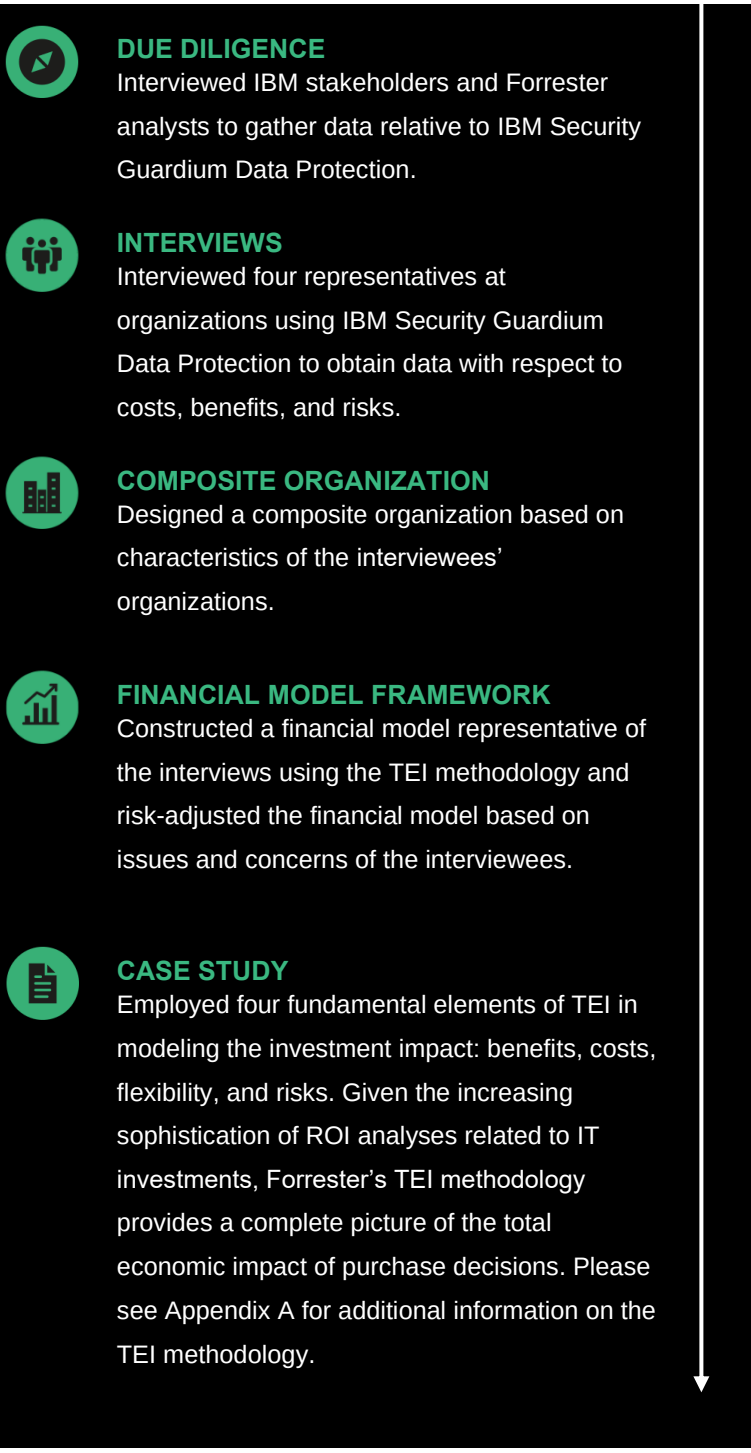
“There is no other product on the market today that can do as much as [IBM Security Guardium Data Protection] does. … I can do more with less. What more can [you] ask for than doing more [for less] with this product?”

— IT security specialist, federal agency

TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in IBM Security Guardium Data Protection.

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 Security Guardium Data Protection can have on an organization.



The IBM Security Guardium Data Protection Customer Journey

Drivers leading to the IBM Security Guardium Data Protection investment

Interviews			
Role	**Industry**	**Region**	**Revenue**
Manager of cybersecurity engineering	Banking	US	$1 to $10 billion USD
Database security and compliance supervisor	Automotive	Global	$100 to $200 billion USD
IT security specialist	Federal agency	US	N/A
Director of enterprise cyber security	Financial services	Global	$20 to $50 billion USD

KEY CHALLENGES

Prior to investment in IBM Security Guardium Data Protection, interviewees' organizations used in-house processes to monitor all databases separately and collect reports on databases' activity. Interviewees said that their lack of centralized monitoring and reporting hindered their ability to protect their data and left them susceptible to potential breaches and loss of sensitive information.

The interviewees noted how their organizations struggled with common challenges, including:

- **Desire to improve databases' security monitoring.** Interviewees said the lack of centralized monitoring and standardized reporting hindered their efforts to keep data safe and secure. It also exposed their organizations to potential data breaches.
- **Desire to meet compliance regulations.** Interviewees noted that decentralized legacy systems made it more difficult to meet compliance mandates and put their organizations at risk of fines.
- **Need to retire manual workflows.** Interviewees discussed the need to automate their organizations' data monitoring and auditing workflows. The legacy workflows required a significant amount of time from DSAs.

"We're able to use one tool. We don't have to use multiple ones to get full coverage, and the other benefit is that Guardium Data Protection — from both a vulnerability scanning perspective and from an auditing perspective — homogenizes your data."

IT security specialist, federal agency

SOLUTION REQUIREMENTS

The interviewees' organizations searched for a solution that could:

- Offer a centralized data security product.
- Offer standard reporting.
- Provide seamless scalability.

- Provide auditing reporting for compliance.

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of the four interviewees, and it is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The global organization has $5 billion in annual revenue. The composite organization used a combination of legacy systems and manual processes for its data security and compliance needs in its prior state. It is looking for a centralized data security product to retire manual processes, streamline data security monitoring, and create a better workflow for auditing purposes. The composite organization has a team of three security specialists and 10 DSAs for security monitoring. The composite organization has 1,000 databases that require security monitoring.

Deployment characteristics. The composite organization decides to implement the IBM Security Guardium Data Protection product and set up the necessary workflows so the security specialists and DSAs can start using the product quickly and efficiently.

"IBM Security Guardium Data Protection has the widest breadth of capability out there on the market that we're aware of today."

IT security specialist, federal agency

Key Assumptions

- **$5 billion in annual revenue**
- **Global organization**
- **Industry agnostic**
- **1,000 databases**
- **3 security specialists**
- **10 DSAs**

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits						
Ref.	**Benefit**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Atr	Increased database security monitoring automation	$326,250	$326,250	$326,250	$978,750	$811,335
Btr	Increased auditing efficiencies	$878,365	$878,365	$878,365	$2,635,096	$2,184,365
Ctr	Increased ability to meet compliance regulations	$450,000	$450,000	$450,000	$1,350,000	$1,119,083
Dtr	Increased database security	$702,000	$702,000	$702,000	$2,106,000	$1,745,770
	Total benefits (risk-adjusted)	$2,356,615	$2,356,615	$2,356,615	$7,069,846	$5,860,553

INCREASED DATABASE SECURITY MONITORING AUTOMATION

Evidence and data. Interviewees spoke of their organizations being able to save time on scanning and gathering information on all their databases' activities.

- The Director of enterprise cyber security at the financial services organization observed a 10% reduction in DSAs time spent on database monitoring due to centralization and automation of those tasks. The interviewee then said, "If we didn't have Guardium, we would need to support different databases, integration with other tools, and coverage of different types of databases."
- The automotive organization saw improvements in its security reporting and less time spent on manual processes. Its database security and compliance supervisor said, "Before we purchased this product, our manual processes were kind of spread all over the place."

Modeling and assumptions. For the composite organization Forrester assumes:

- It employs 10 DSAs.
- The average fully burdened salary of a DSA is $145,000.
- The percentage of time saved is 25%.

"I can deploy consistent rules and policies across all databases. I am adding 100 databases, 200 databases without any issues. I have the control, and the centralization of consolidated data is key. So I can bring all the data into one place, and I can easily analyze it and find the data discrepancies."

Database security and compliance supervisor, automotive

Risks. Increased database security monitoring automation may vary depending on the following:

- The number of DSAs involved.
- The salaries of DSAs.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $811,300.

Increased Database Security Monitoring Automation

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Number of DSAs	Composite	10	10	10
A2	Average fully burdened salary	TEI standard	$145,000	$145,000	$145,000
A3	Percentage of time saved	Interviews	25%	25%	25%
At	Increased database security monitoring automation	A1*A2*A3	$362,500	$362,500	$362,500
	Risk adjustment	↓10%			
Atr	Increased database security monitoring automation (risk-adjusted)		$326,250	$326,250	$326,250
	Three-year total: $978,750			**Three-year present value: $811,335**	

INCREASED AUDITING EFFICIENCIES

Evidence and data. Interviewees discussed the significant time savings their organizations experienced after the IBM Security Guardium Data Protection product implementation. This was due to the improved automated auditing workflows.

- The automotive organization saw a 70% reduction in time spent on auditing requests and related processes. The database security and compliance supervisor said: "The major part is how we set up the IBM Security Guardium Data Protection for search. After that, I can scale it easily. That's the benefit of using this tool."
- The IT security specialist at the federal agency said, "From an auditing [standpoint], that's an even more important area because there's not a lot of tools out there in the market today that can audit multiple platforms and multiple database types. IBM Security Guardium Data Protection is able to do that and that's where we can really save."

Modeling and assumptions. For the composite organization Forrester assumes:

- The number of audit requests for monitored databases is 500 per year.
- The number of hours spent per audit request prior to Guardium is 40.
- The percentage of time saved is 70%.
- The average fully burdened salary of a DSA is $145,000, or $70 per hour.

Risks. Increased auditing efficiencies may vary depending on the following:

- The number of audit requests per year.
- The salaries of DSAs.
- The number of hours spent per audit request.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $2.2 million.

Increased Auditing Efficiencies

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Number of audit requests for monitored databases	Interview	500	500	500
B2	Hours spend per audit request prior to IBM Security Guardium Data Protection	Interview	40	40	40
B3	Percentage of time saved	Interview	70%	70%	70%
B4	Number of hours saved	B1*B2*B3	14,000	14,000	14,000
B5	Average hourly fully burdened salary	TEI standard	$70	$70	$70
Bt	Increased auditing efficiencies	B4*B5	$975,962	$975,962	$975,962
	Risk adjustment	↓10%			
Btr	Increased auditing efficiencies (risk-adjusted)		$878,365	$878,365	$878,365
	Three-year total: $2,635,096			**Three-year present value: $2,184,365**	

INCREASED ABILITY TO MEET COMPLIANCE REGULATIONS

Evidence and data. Interviewees discussed their organizations' increased ability to meet compliance regulations. They noted that the IBM Security Guardium Data Protection product had the necessary audit and compliance workflows set up, which was an important factor in their decision to start using it.

IBM Security Guardium Data Protection provided the organization with preconfigured workflows to automate the entire compliance auditing process. These prebuilt workflows allowed customers to quickly adapt the product to their own use cases and to have the flexibility to adapt to new compliance regulations.

The federal agency saw a notable improvement in its audit workflows. The IT security specialist said: "IBM Security Guardium Data Security homogenizes everything together from different database platforms and allows us to create rules to identify what is auditable versus what is actionable and present that data downstream. The benefit is that the product is able to do that in near real time, and that's huge for us."

Modeling and assumptions. For the composite organization Forrester assumes:

> **"We are going with 0% gap for SOX [Sarbanes-Oxley Act] compliance. We can produce what they ask. That's the best measurement for us."**
>
> *Database security and compliance supervisor, automotive*

- The average potential regulatory fine is $25,000,000.
- The probability of a fine is 2%.

Risks. Increased ability to meet compliance regulations may vary depending on the average size of a fine in an industry.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $1.1 million.

Increased Ability To Meet Compliance Regulations

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Average potential regulatory fine	Composite	$25,000,000	$25,000,000	$25,000,000
C2	Probability of fine	Assumption	2%	2%	2%
Ct	Increased ability to meet compliance regulations	C1*C2	$500,000	$500,000	$500,000
	Risk adjustment	↓10%			
Ctr	Increased ability to meet compliance regulations (risk-adjusted)		$450,000	$450,000	$450,000
	Three-year total: $1,350,000			**Three-year present value: $1,119,083**	

INCREASED DATABASE SECURITY

Evidence and data. Interviewees talked about their organizations' increased ability to detect potential data risks within their environments, which allowed decision-makers to make informed decisions on how to best protect their data.

- The federal agency saw an improvement in internal vulnerability assessments. Its IT security specialist mentioned: "First and foremost, it's [IBM Security Guardium Data Protection] breadth of coverage from security perspective. I don't need other products. I can just have this product for my auditing and scanning needs."
- The financial services organization saw an increased ability to identify and protect sensitive data in its environment. The director of enterprise cyber security noted: "One of the big benefits we found is that IBM Security Guardium Data Protection has an excellent data investigation tool for scanning the databases so we can identify PII [personal identifiable information]. Helping catalog and identify our PII is a great benefit."

Modeling and assumptions. For the composite organization Forrester assumes:

- The average cost of a data breach is $6,500,000.
- The probability of a data breach is 12%.

> **"[IBM Security Guardium Data Protection] helps us understand our risk posture, know how and where problem areas are across the enterprise, and be able to identify if anything has been exploited. We are able to use that [information] or capture it in near real time."**
>
> *IT security specialist, federal agency*

Risks. Increased database security benefit may vary depending on the cost of a data breach to specific organizations.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $1.7 million.

Increased Database Security

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Estimated average cost of data breach	Composite	$6,500,000	$6,500,000	$6,500,000
D2	Probability of data breach	Assumption	12%	12%	12%
Dt	Increased database security	D1*D2	$780,000	$780,000	$780,000
	Risk adjustment	↓10%			
Dtr	Increased database security (risk-adjusted)		$702,000	$702,000	$702,000
	Three-year total: $2,106,000			**Three-year present value: $1,745,770**	

UNQUANTIFIED BENEFITS

Interviewees mentioned the following additional benefits that their organizations experienced but were not able to quantify:

- **Integration compatibility with a multitude of databases and other enterprise tools.** The IT security specialist at the federal agency mentioned, "We can integrate IBM Security Guardium Data Protection with our other inventory tools to be able to feed in new database instances."
- **User community support to drive better customer experience.** Interviewees discussed how IBM facilitates different ways for customers to communicate and share their experiences.
    - **Organizations have the option to attend TechXchange (formerly IBM Security Master Skills University), an annual event that brings customers together.** The director of enterprise cyber security in financial services stated: "I took the whole team. And the junior engineers just love it because it's so much. They get to hear from not just the people that are mentoring them but other people in the industry that are asking different questions. So it's a very enlightening experience. I would say the junior engineers get more out of it, but the more senior engineers still find value there."
    - **Customer support that drives faster implementation and adoption of the IBM Security Guardium Data Protection product.** The database security and compliance supervisor in the automotive industry mentioned: "IBM is creating a lot of learning series videos for new users. What the process means, what the architecture looks like, these types of information they can learn quickly."

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement the IBM Security Guardium Data Protection product and later realize additional uses and business opportunities, including a strategic partnership that leads to faster results and superior future company strategy. Interviewees discussed the quality and type of business relationship that their organizations have with IBM and the strength of the partnership. The IT security specialist at the federal agency said: "The IBM Security Guardium Data Protection product is on critical growth. They are constantly developing and looking for new ways to improve the product and, to me, that's gold, especially in the security arena."

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

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Etr	Implementation and maintenance costs	$20,495	$30,450	$30,450	$30,450	$111,845	$96,220
Ftr	Total fees	$690,000	$150,000	$150,000	$150,000	$1,140,000	$1,063,028
	Total costs (risk-adjusted)	$710,495	$180,450	$180,450	$180,450	$1,251,845	$1,159,248

IMPLEMENTATION AND MAINTENANCE COSTS

Evidence and data. The interviewees described the IBM Security Guardium Data Protection implementation process as relatively straightforward.

- Implementation periods varied across interviewees due to the complexities of their previous systems and requirement variations.
- The financial services organization saw that the IBM Security Guardium Data Protection product provided flexibility during implementation and future upgrades. Its director of enterprise cyber security noted, “We love the fact that they at least attempt to talk to every database in known existence.”

Modeling and assumptions. For the composite organization, Forrester assumes:

- The initial implementation process takes 280 hours.
- The average fully burdened salary of a DSA is $145,000, or $70 per hour.
- The ongoing maintenance cost is $29,000 per year (20% of 1 FTE).

Risks. The implementation and ongoing maintenance costs may vary due to the following:

- The complexity of the previous systems and their overall architecture.
- The available capacity and skill set of DSAs.
- The salaries of the DSAs.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $96,000.

Implementation And Maintenance Costs						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Hours spent on implementation	Interview	280			
E2	Average DSA hourly fully burdened salary	TEI standard	$70			
E3	Implementation cost	E1*E2	$19,519			
E4	Ongoing maintenance cost	Composite	$0	$29,000	$29,000	$29,000
Et	Implementation and maintenance costs	E3+E4	$19,519	$29,000	$29,000	$29,000
	Risk adjustment	↑5%				
Etr	Implementation and maintenance costs (risk-adjusted)		$20,495	$30,450	$30,450	$30,450
	Three-year total: $111,845			**Three-year present value: $96,220**		

TOTAL FEES

Evidence and data. The interviewees said that their organizations incurred an annual license fee for the IBM Security Guardium Data Protection product. The fee included dedicated deployment services and customer support.

Modeling and assumptions. For the composite organization, Forrester assumes the composite organization pays an initial fee of $690,000 and then $150,000 in annual license fees.

Risks. Pricing may vary depending on the following:

- The size of the IBM Security Guardium Data Protection deployment.
- The use of professional services during deployment and on a continuing basis.

Results. Forrester estimates this cost to be a three-year, total PV of $1 million.

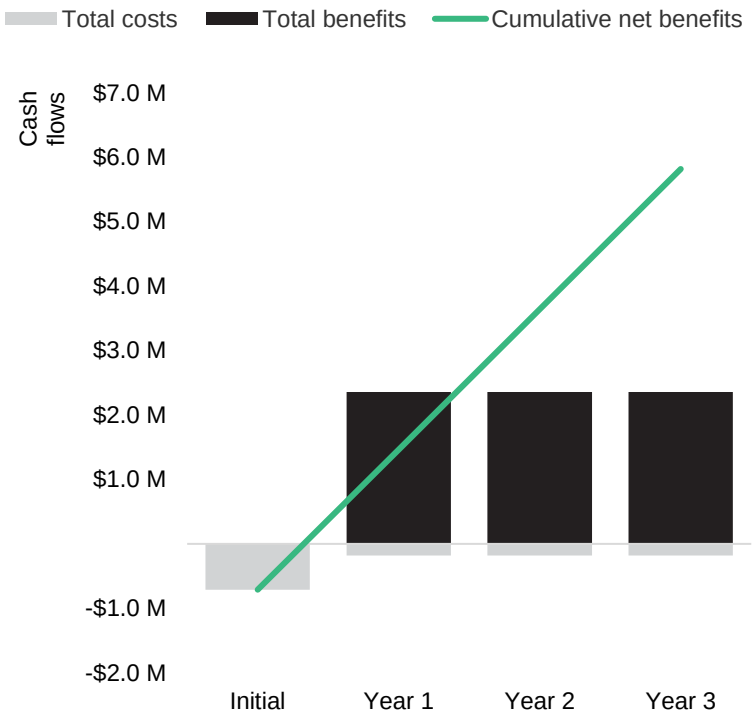
> **"We have an excellent sales engineer who is constantly onsite with us, working with us whenever I need something. [This is] up to and including flying out the executives to talk to us about our problems."**
>
> *Director of enterprise cyber security, financial services*

Total Fees						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
F1	Perpetual License fee and deployment	Composite	$690,000	$150,000	$150,000	$150,000
Ftr	Total fees		$690,000	$150,000	$150,000	$150,000
	Three-year total: $1,140,000			**Three-year present value: $1,063,028**		

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



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

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 Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($710,495)	($180,450)	($180,450)	($180,450)	($1,251,845)	($1,159,248)
Total benefits	$0	$2,356,615	$2,356,615	$2,356,615	$7,069,846	$5,860,553
Net benefits	($710,495)	$2,176,165	$2,176,165	$2,176,165	$5,818,001	$4,701,305
ROI						406%
Payback						<6 months

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.

Appendix B: Endnotes

[1] 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.


FORRESTER®