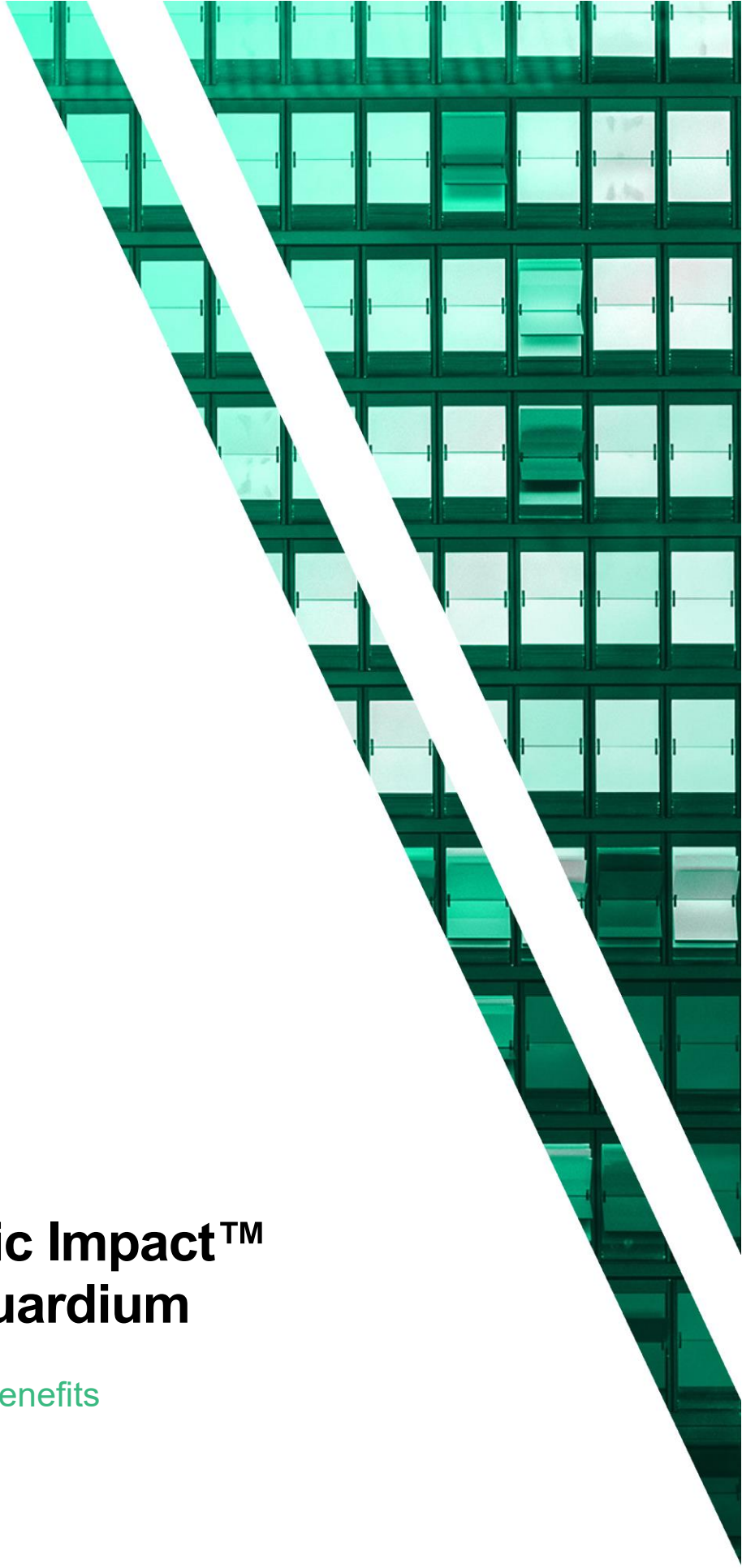
FORRESTER®



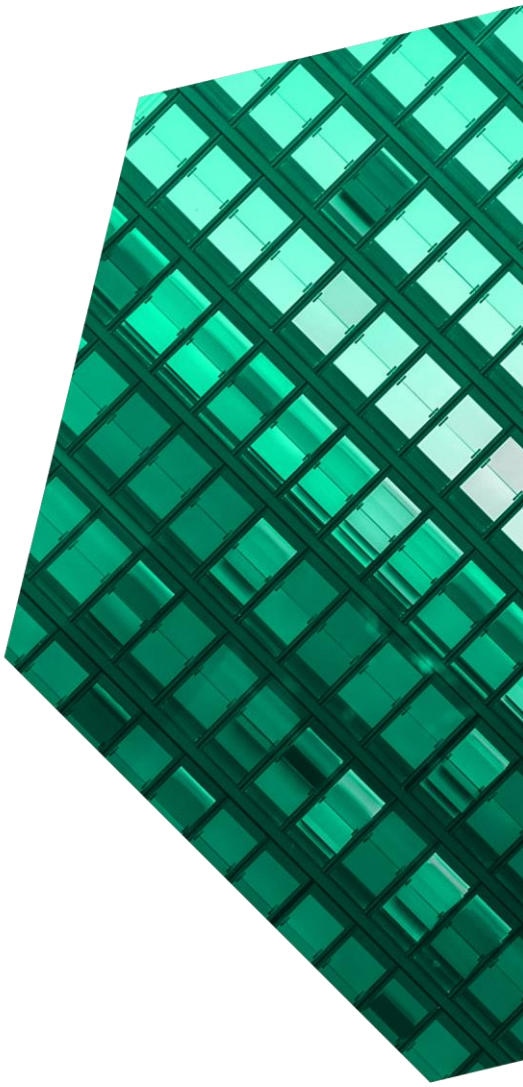
The Total Economic Impact™ Of IBM Security Guardium

Cost Savings And Business Benefits Enabled By Guardium

OCTOBER 2020

Table Of Contents

Consulting Team: Connor Maguire
Adrienne Capaldo



ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. For more information, visit forrester.com/consulting.

Executive Summary

> "I believe IBM Security Guardium does increase our resistance to breaches. It gives us more accountability and helps perform any kind of breach investigation efficiently. It even would help us be aware of a data breach, whereas before we might get billing for six months and never know it. I think it helps quickly resolve any breach that might happen." – IT security infrastructure engineer, energy and utilities

IBM Security Guardium offers a comprehensive suite of products designed to assist customers in protecting their key cornerstone data assets. The suite includes (but is not limited to) products such as Guardium Data Protection, Guardium Insights for IBM Cloud Pak for Security, Guardium Data Risk Manager, and Guardium Data Encryption.

These products are designed to empower customers to centralize their data environments, quickly and easily prove that their environments are compliant with various regulations, expose potential risks within these environments, and accelerate response to these threats.

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

The IBM Security Guardium product suite integrates with IBM's cloud-native platforms for security and data and analytics, IBM Cloud Pak for Security and IBM Cloud Pak for Data. Integration with these platforms extends data security, threat analytics, and compliance reporting across organizations' IT environments. These hybrid multicloud platforms bring together disparate tools and teams with an open approach to information gathering and sharing

KEY STATISTICS

Return on investment (ROI)
401%

Net present value (NPV)
$4.0M

— unifying investigation efforts and accelerating the speed and accuracy of their risk mitigation and remediation actions.

Data security has grown in importance as scrutiny over data collection practices has increased. The cost of failing to protect one's data expands far beyond the effort companies put into recovering lost information. Regulatory fines, stolen IP, and reputational damage can all considerably increase the cost of a breach.

As organizations grow, so do their data environments, increasing the potential surface area for malicious individuals to attack. IBM Security Guardium provides customers with the ability to secure their ever-increasing data environments without limiting their ability to navigate and analyze the information they store. IBM Security Guardium provides customers with a suite of products that increase their ability to monitor and protect their

efficient workflows to prove compliance across a variety of environments.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed decision makers at an organization with experience using Guardium Data Protection. Forrester used this experience to project a three-year financial analysis.

Prior to using Guardium Data Protection, the customer expected each data owner in the organization to maintain and secure their data environments separately. This left the company no coherent data security strategies and forced data owners to use time-intensive manual processes to prove they could meet regulatory compliance standards. Investing in IBM Security Guardium enabled the organization to automate many of the manual processes required in its legacy state, secure its data under one unified solution, and prove compliance much faster.

KEY FINDINGS

Quantified benefits. Risk-adjusted present value (PV) quantified benefits include:

- **Automation of database analysis processes, saving approximately 1,000 hours annually.** Prior to investing in IBM Security Guardium, the customer tasked its database administrator (DBA) staff with manually correlating and adjusting data to perform analysis reports on the heath of its data environment. Using the capabilities provided by IBM Security Guardium allowed this customer to automate these processes, saving DBAs significant time. These efficiencies saved the organization $822K over three years.
- **Reduced effort to perform a data environment audit by 75%.** The customer reported that by using IBM Security Guardium, the company could streamline the workflows it followed to complete audits of its data environments. In its legacy state, the organization required a large team of employees to collect, analyze, and present the information required to pass an audit. IBM Security Guardium has eliminated the need to collect data from disparate sources and provides one central location with all the required information readily available. The efficiencies created from this workflow saved $2.1M.
- **Reduced likelihood of a breach by 40%.** IBM Security Guardium helped the interviewed organization gain visibility into its data environment, enabling it to identify potential internal and external threats. The vulnerability management, threat monitoring and detection, and asset prioritization capabilities provided by IBM have enabled the customer to avoid the potentially significant costs of a data breach. Over three years, these costs amount to a total of $990K.
- **Increased ability to meet compliance regulations, saving $1.1M.** Investing in IBM Security Guardium helped the organization meet compliance regulations like those detailed in General Data Protection Regulation (GDPR) or California Consumer Privacy Act (CCPA) regulations. The deeper visibility into where sensitive information was stored as well as the preconfigured workflows to protect this information provided by IBM allowed the organization to quickly prove compliance and lower the likelihood of experiencing a regulatory fine by 2%.

Unquantified benefits. Benefits that are not quantified for this study include:

- **Increased actionability based on the insights provided by IBM Security Guardium.** IBM can provide customers insights into their data environments and suggest potential actions to optimize the security of their environments.
- **Integration of IBM with established enterprise tools.** Customers can integrate IBM Security

Guardium with their established enterprise productivity tools to gain deeper insights into what users do with their data. This can provide additional context to how sensitive information is accessed and how it is used throughout an organization.

Costs. Risk-adjusted PV costs include:

- **IBM Security Guardium usage fees.** These represent fees paid to IBM to use the product and an annual fee to maintain the solution. Over three years, this amounts to $859K.
- **Implementation and maintenance costs.** The organization spent time planning for and implementing IBM Security Guardium. Additionally, it allocated resources internally to maintain and support the solution internally. Over three years, the organization paid $141K.

The interview and financial analysis found that this customer experienced benefits of $5.0M over three years versus costs of $1.0M, adding up to a net present value (NPV) of $4.0M and an ROI of 401%.

ROI
401%

BENEFITS PV
$5.0M

NPV
$4.0M

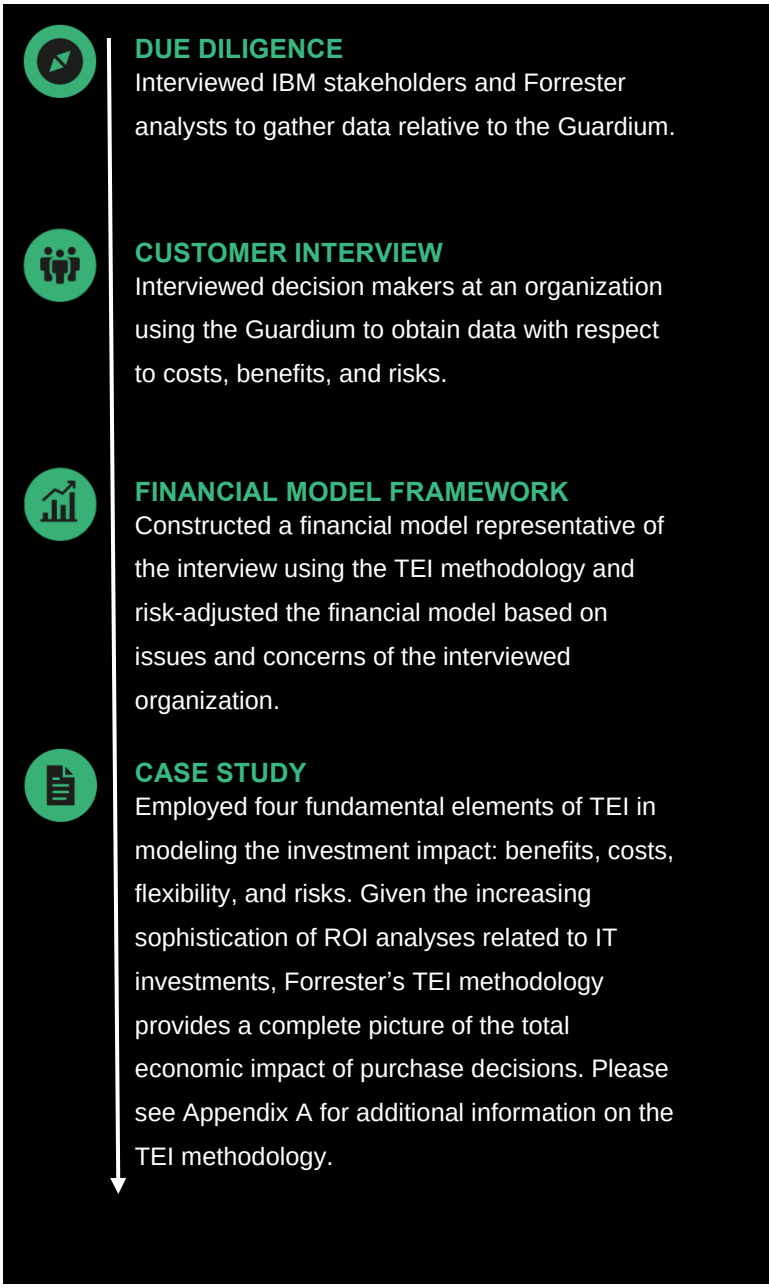
PAYBACK
<6 months

Benefits (Three-Year)

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.

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 can have on an organization.



The IBM Security Guardium Customer Journey

Drivers leading to an investment in Guardium

INTERVIEWED ORGANIZATION

Forrester interviewed an IBM Security Guardium customer with the following characteristics:

- A US-based energy and utilities company.
- Approximate annual revenue of $22B with 35,000 employees.
- Deployed Guardium Data Protection across 200 servers monitoring several petabytes of data.

KEY CHALLENGES

Prior to investing in IBM Security Guardium, application and data owners were tasked with managing and regulating their data independently. Often, they would implement independent strategies when it came to regulating and protecting the data for their individual business units. The lack of cohesion across the data environment led to several challenges, including:

- **Desire to meet compliance regulations.** An interviewee at the organization stated that in the legacy state, proving the data environment followed various regulatory standards was difficult. The disparate nature of the firm's data protection practices created significant manual work for the organization when it attempted to comply with new and emerging data privacy regulations.
- **Desire to gain increased visibility into the data environment.** Understanding what data is in a data environment is one of the key ways to protect said data. The interviewee stated that prior to investing in IBM Security Guardium, the company had a limited view into what information was in its data environment or how it was protected. This left the organization susceptible to potential breaches and loss of important or sensitive information.
- **Need to retire manual workflows.** In its legacy state, the customer relied heavily on manual workflows to complete internal or external audits and perform standard analysis on its data environment. These workflows were time-consuming and pulled DBAs from other important internal initiatives. The customer sought a solution that could automate these processes and allow DBAs to contribute to more pressing business needs.

USE CASE DESCRIPTION

For this analysis, Forrester created a financial model based on the experiences of the interviewed organization. The interviewee deployed Guardium Data Protection across 200 servers in its data environment, ranging in size from 100 GB to over 1 TB. The company purchased IBM Security Guardium to monitor all the accesses and modifications that involve the sensitive database servers that are relevant to the Sarbanes-Oxley Act (SOX), data privacy, and new regulations like GDPR. Guardium Data Protection monitors all network and local traffic—covering a wide variety of databases and applications and ensuring that the company can deploy a single solution enterprise wide.

As the interviewee detailed, in the legacy state, the company attempted to perform monthly analyses on its data environment to better understand how data was being used and accessed. Additionally, the organization is subject to several audits per year. Much like the database analysis, the workflow to complete an audit was highly manual and required significant resources to complete. For this use case, Forrester has modeled benefits and costs over three years.

Analysis Of Benefits

Quantified benefit data

Total Benefits

Ref.	Benefit	Year 1	Year 2	Year 3	Total	Present Value
Atr	Increased database analysis automation	$330,739	$330,739	$330,739	$992,218	$822,499
Btr	Increased auditing efficiencies	$858,600	$858,600	$858,600	$2,575,800	$2,135,211
Ctr	Increased database security	$398,160	$398,160	$398,160	$1,194,480	$990,165
Dtr	Increased ability to meet compliance regulations	$425,000	$425,000	$425,000	$1,275,000	$1,056,912
	Total benefits (risk-adjusted)	$2,012,499	$2,012,499	$2,012,499	$6,037,498	$5,004,787

INCREASED DATABASE ANALYSIS AUTOMATION

The first benefit highlights how IBM Security Guardium can streamline workflows within customer data environments, allowing organizations to quickly gain insights into how the data they store is being used. The customer stated, to understand the nuances of its data environment, the organization would task its DBAs with creating several manual processes designed to pull the desired information from the multiple databases they were maintaining.

"For each database, we had a series of queries we would run and then take the output and run this through a custom-made script, which we needed to correlate the data and adjust it for each database," explained the interviewee. "It was a manual process that took them a week or two of hard work every time they did it."

This workflow was highly manual and required employees to manually adjust the script for each database analyzed. This resulted in DBAs spending hours attempting to collect this information, ultimately delaying the speed at which the organization could analyze the reports it pulled. Investing in IBM Security Guardium allowed the customer to automate many of the manual adjustments needed to create the tables necessary to perform analysis.

The interviewee explained: "Now we take the queries from the databases and use them within IBM Security Guardium to create custom tables. Then we use Guardium regular reporting features to query those custom tables and spit out the reports we are looking for. Now we are able to run these reports and create the tables in a matter of minutes."

For the financial model, Forrester assumes:

- The organization assigned eight employees to run monthly analyses of its data environments.
- Prior to investing in IBM Security Guardium, employees spent 80 hours collecting the data and adjusting the scripts used to fetch the data to each database.
- With the automation provided by IBM Security Guardium, the organization reduced the amount of time required to complete these tasks to 1 hour each. Additionally, the organization reduced the number of DBAs required to complete this analysis to two FTEs.
- The average hourly cost of the employees involved in these workflows is $48.

The following risks may affect this benefit category:

- The frequency at which an organization chooses to perform analysis of its data environment.
- Other productivity and analysis tools, which may affect the total reduction in time IBM Security Guardium can provide a customer.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $822,499.

Increased Database Analysis Automation

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
A1	Resources involved in analysis prior to investing in IBM Security Guardium		8	8	8
A2	Time spent preparing and analyzing scripts before Guardium (hours per analysis)		80	80	80
A3	Cost of resources involved in database analysis		$48	$48	$48
A4	Database analyses per year		12	12	12
A5	Cost to perform database analysis prior to investing in IBM Security Guardium	A1*A2*A3*A4	$368,640	$368,640	$368,640
A6	Resources involved in analysis with Guardium		2	2	2
A7	Time spent preparing and analyzing scripts with IBM Security Guardium (hours per analysis)		1	1	1
A8	Cost of resources involved in database analysis		$48	$48	$48
A9	Cost to perform database analysis with Guardium	A6*A7*A8*A4	$1,152	$1,152	$1,152
At	Increased database analysis automation	A5-A9	$367,488	$367,488	$367,488
	Risk adjustment	↓10%			
Atr	Increased database analysis automation (risk-adjusted)		$330,739	$330,739	$330,739
	Three-year total: $992,218			**Three-year present value: $822,499**	

INCREASED AUDITING EFFICIENCIES

The interviewee noted that a significant benefit of using IBM Security Guardium was the efficiency it created during auditing processes. Prior to investing in IBM Security Guardium, the customer relied on native logging capabilities provided by its legacy systems to perform internal audits of its data environment. This process required data managers and application owners to manually pull information from these logs and send them to DBAs who would then aggregate the data and formally present the information to an auditor. This was a highly manual, error-prone process that left the organization at risk of incurring potential monetary fines as result of not adhering to proper audit standards.

With IBM, the customer could remove much of the manual burden from its database and application owners. IBM Security Guardium provides customers with prebuilt templates that significantly reduce the amount of manual work needed to complete an audit, saving those involved significant time.

The interviewee described these efficiencies: “I have to complete SOX audits for some of our divisions. I was able to shortcut all the manual work we used to have to do for an audit. When it came time for me to sit with auditor, it ended up being a pretty quick meeting. I was able to show exactly what we are looking for because of the compliance templates provided by IBM Security Guardium. So, it saves me a lot of time with auditing and kept the auditors happy.”

For the financial model, Forrester assumes:

- The organization is subject to eight major audits annually.
- In the legacy state, a team of 40 DBAs collected and presented database information from across the organization to auditors. These DBAs dedicated 120 hours to the data collection, processing, and presenting process. Five hundred database and application owners spent approximately 1 hour collecting the data required for an audit.
- The average hourly salary for employees involved in the audit process is $60.
- The prebuilt templates and increased visibility provided by IBM Security Guardium reduced the time spent performing audits by 75%.
- Only 50% of the time saved in this workflow is used for productive work.

The following risks may affect this benefit category:

- The number of audits an organization completes each year, will vary based on size, vertical, and location.
- The reduction in time enabled by IBM Security Guardium, which will depend on the other productivity solutions an organization uses during its audit process.
- The number of employees involved in audit workflows.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $2,135,211.

Increased Auditing Efficiencies					
Ref.	**Metric**	**Calculation**	**Year 1**	**Year 2**	**Year 3**
B1	Number of audits performed annually		8	8	8
B2	Number of DBAs involved in audits		40	40	40
B3	DBA time spent performing each audit prior to investing in IBM Security Guardium (hours)		120	120	120
B4	Number of other staff involved in audits		500	500	500
B5	Time spent performing audits by other staff prior to investing in IBM Security Guardium (hours)		1	1	1
B6	Average hourly salary for employees involved in audits		$60	$60	$60
B7	Cost to perform audits prior to investing in IBM Security Guardium	(B1*B2*B3*B6)+(B1*B4*B5*B6)	$2,544,000	$2,544,000	$2,544,000
B8	Reduction in time spent auditing with IBM Security Guardium		75%	75%	75%
B9	Productivity captured		50%	50%	50%
Bt	Increased auditing efficiencies	B7*B8*B9	$954,000	$954,000	$954,000
	Risk adjustment	↓10%			
Btr	Increased auditing efficiencies (risk-adjusted)		$858,600	$858,600	$858,600
	Three-year total: $2,575,800		**Three-year present value: $2,135,211**		

INCREASED DATABASE SECURITY

Guardium Data Protection allows users to protect their data on a database and application level, enabling them to establish workflows to protect sensitive information wherever it may live in their organization. Investing in Guardium Data Protection gave the interviewed organization insights into potential data risks within its environment, allowing decision makers to proactively make informed decisions on how to best protect their data. Additionally, Guardium Data Protection increased the interviewed organization's ability to detect potential threats and establish workflows to mitigate these threats quickly.

The increased security capabilities provided by IBM Security Guardium helped the organization avoid potentially significant costs it could have incurred if its data environment was breached. One employee at the interviewed organization said: "I believe IBM Security Guardium does increase our resistance to breaches. It gives us more accountability and helps perform any kind of breach investigation efficiently. It even would help us be aware of a data breach, whereas before we might get billing for six months and never know it. I think it helps quickly resolve any breach that might happen."

For the financial analysis, Forrester relies on its 2020 survey of 300 security professionals, which found that an energy organization can anticipate one potential

breach in an average year with an average cost of $1.85M to remediate. The average cost of a breach per employee is $53.[1]

For the financial model, Forrester assumes:

- Data breaches can stem from many different aspects of an organization's operations, including employee error, network vulnerabilities, and infrastructure failures. All these weak points can lead to malicious individuals gaining access to an organization's sensitive information. The probability that an organization experiences a data breach because of a vulnerability within its data environment is 20%.
- IBM Security Guardium's ability to help customers identify sensitive information, remove stale data, and protect against internal and external threats reduces the probability that an organization experiences a data breach by 40%.
- In addition to the cost associated with a breach, there is also a significant amount of downtime with each potential breach. Forrester's 2020 security survey finding shows that approximately 10% of employees are affected by each breach.[2]
- Employees experience an average of 2 hours of downtime during each breach, and the hourly fully burdened salary of an affected employee is $42.

The following risks may affect this benefit category:

- The actual cost of a data breach, which will vary based on organization size, vertical, and location.
- The amount of downtime experienced by employees, which will vary based on the existing security solutions customers have in their environments.
- The impact that IBM Security Guardium has on security threat detection and response, which will vary based on the sophistication of existing security solutions (other than IBM Security Guardium).

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $990,165.

Increased Database Security					
Ref.	**Metric**	**Calculation**	**Year 1**	**Year 2**	**Year 3**
C1	Average number of breaches anticipated annually for vertical		1	1	1
C2	FTE count of organization		35,000	35,000	35,000
C3	Average cost of a breach scaled to organization size (at $53/FTE)	C1*C2*$53	$1,855,000	$1,855,000	$1,855,000
C4	Percentage of breaches that might arise from file sharing		20%	20%	20%
C5	Reduced probability of a breach by implementing IBM Security Guardium		40%	40%	40%
C6	Reduced cost of a breach by implementing IBM Security Guardium	C3*C4*C5	$148,400	$148,400	$148,400
C7	Number of employees affected by a breach	C2*10%	3,500	3,500	3,500
C8	Average amount of downtime per employee (hours)		2	2	2
C9	Average cost of downtime per employee		$42	$42	$42
C10	Cost of employee downtime caused by a breach	C1*C7*C8*C9	$294,000	$294,000	$294,000
Ct	Increased database security	C6+C10	$442,400	$442,400	$442,400
	Risk adjustment	↓10%			
Ctr	Increased database security (risk-adjusted)		$398,160	$398,160	$398,160
	Three-year total: $1,194,480			**Three-year present value: $990,165**	

INCREASED ABILITY TO MEET COMPLIANCE REGULATIONS

All organizations that collect data face the potential risk associated with receiving a fine by a court or other regulatory entity if they fail to comply with data privacy standards. By investing in IBM Security Guardium, the interviewed organization received the capabilities needed to quickly meet compliance mandates.

IBM Security Guardium provides preconfigured workflows to automate the entire compliance auditing process. Customers can automate data discovery and classification, set up workflows to create audit records in real time, and assess potential data vulnerabilities quickly to ensure their environments are as secure as possible. Further, these prebuilt workflows and capabilities allow customers to quickly adapt to new and emerging compliance regulations.

For the financial model, Forrester assumes:

- Without proper regulatory measures in place to prove and ensure compliance, the organization could face a $25 million fine each year.
- By investing in IBM Security Guardium, the interviewed organization can better meet its security requirements and has reduced the probability of a fine to 2%.

The following risks may affect this benefit category:

- The actual cost of a fine, which will vary by organizational size and industry among other factors.
- The breadth of the use of IBM Security Guardium.

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $1,056,912.

Increased Ability To Meet Compliance Regulations

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
D1	Average potential regulatory fine		$25,000,000	$25,000,000	$25,000,000
D2	Probability of fine		2%	2%	2%
Dt	Increased ability to meet compliance regulations	D1*D2	$500,000	$500,000	$500,000
	Risk adjustment	↓15%			
Dtr	Increased ability to meet compliance regulations (risk-adjusted)		$425,000	$425,000	$425,000
	Three-year total: $1,275,000			**Three-year present value: $1,056,912**	

UNQUANTIFIED BENEFITS

Additional benefits that the customer experienced but was not able to quantify include:

- **Increased actionability based on the insights provided by IBM Security Guardium.** The interviewee noted that in addition to identifying potential threats or vulnerabilities in its data environment, IBM Security Guardium can suggest potential actions that can mitigate these issues as well as help the company prioritize which issues to address first. This helps customers tackle these potential vulnerabilities faster and ensure they are remediating the most vulnerable parts of their data environments first.
- **Integration of IBM Security Guardium with established enterprise tools.** Customers can integrate IBM Security Guardium with established enterprise tools to increase their visibility into how data is being accessed and what their users do with this data. Gaining further insights into what happens with data once it has been accessed allows organizations to continue to ensure that the data they collect is being is protected throughout its life within their data environments.

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement IBM Security Guardium and later realize additional uses and business opportunities, including:

- **Leveraging data security with IBM Security Guardium in the cloud.** As customers expand their footprint in the cloud, they can continue to leverage the security insights provided by IBM Security Guardium in their cloud deployments. The IBM Security Guardium product suite integrates with IBM Cloud Pak for Security, a cloud-native platform that allows users to

consolidate their security tools into a unified platform, giving them an increased understanding of critical risk and threat information that would otherwise be siloed across disparate teams. With IBM Security Guardium Insights for IBM Cloud Pak for Security, clients can connect data security insights to the broader security framework, take advantage of consistent case management and orchestration, and improve data security by sharing context across other security tools.

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

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Etr	IBM Security Guardium implementation and maintenance costs	$10,500	$52,500	$52,500	$52,500	$168,000	$141,060
Ftr	IBM Security Guardium usage fees	$607,200	$101,200	$101,200	$101,200	$910,800	$858,869
	Total costs (risk-adjusted)	$617,700	$153,700	$153,700	$153,700	$1,078,800	$999,929

OVERVIEW OF COSTS

For the financial model, Forrester assumes the interviewed organization incurred the following costs associated with its deployment of IBM Security Guardium:

- **IBM Security Guardium implementation and maintenance costs**. This represents the internal costs associated with the initial planning, implementation, and the ongoing support to maintain the solution by the customer.
- **IBM Security Guardium usage fees**. This cost category represents usage fees paid to IBM for the 200-core system.

Costs for using IBM Security Guardium can vary with:

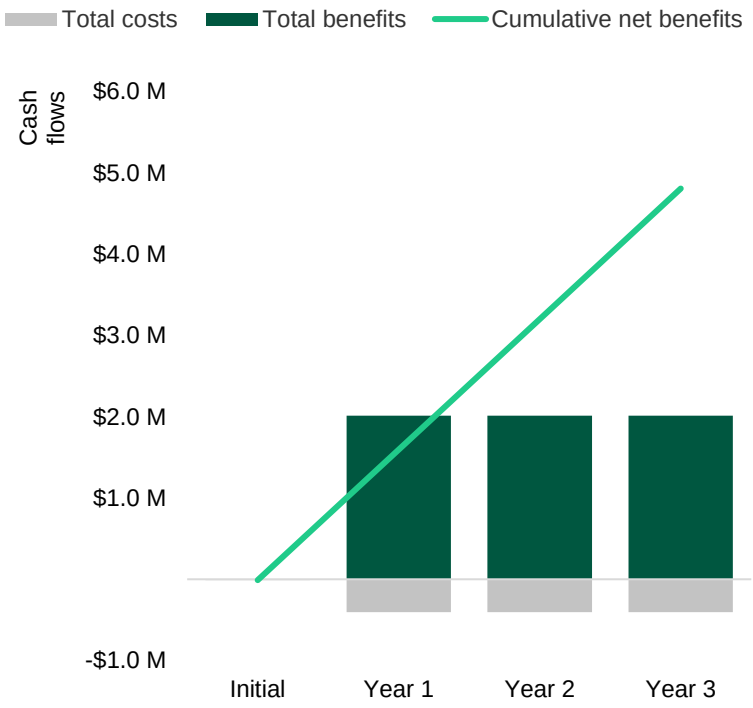
- The size of an IBM Security Guardium deployment and the associated products a customer chooses to deploy.
- The speed at which a customer chooses to deploy IBM Security Guardium across its data environment.
- The use of professional services during implementation and on a continuing basis.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $999,929.

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	($617,700)	($153,700)	($153,700)	($153,700)	($1,078,800)	($999,929)
Total benefits	$0	$2,012,499	$2,012,499	$2,012,499	$6,037,498	$5,004,787
Net benefits	($617,700)	$1,858,799	$1,858,799	$1,858,799	$4,958,698	$4,004,858
ROI						401%
Payback period (months)						<6

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."

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] “Cost Of A Security Breach,” Internal Forrester Survey Data, August 2020
[2] “Cost Of A Security Breach,” Internal Forrester Survey Data, August 2020


FORRESTER®