A Forrester Total Economic Impact™
Study Commissioned By IBM
April 2018

The Total Economic Impact™ Of IBM Security Guardium

Cost Savings And Business Benefits Enabled By Guardium

FORRESTER®

Table Of Contents

Project Director:
Adrienne Capaldo

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

Key Benefits

Reduction in time spent on security and compliance requirements:
20%

Reduction in likelihood of data breach:
45%

Future hires avoided:
6 FTEs

Executive Summary

Data security presents a complex challenge to organizations. The value of sensitive data, and particularly customer data, has increased exponentially over time, but with it comes an increase in potential liability and exposure. Successful enterprise security and compliance strategy needs to balance out: the rapid growth of data within organizations' environments; the complexity of regulations and compliance across industries; and the threat of internal and external attacks. Additionally, companies struggle to understand how to proactively monitor and control user access privileges, and they often lack the visibility into what data is at risk, which can lead to potentially devastating security threats. Companies seek to safeguard their structured *and* unstructured data and support compliance across a variety of environments: on-premises, off-site, in a private, public, or hybrid cloud, on the mainframe, or in a big data environment.

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 as part of their overall enterprise data security and compliance strategy. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Guardium on their organizations.

To better understand the benefits, costs, and risks associated with a Guardium implementation, Forrester interviewed three customers with multiple years of experience using Guardium. IBM Security Guardium offers a family of integrated modules for managing the entire data security and compliance life cycle, which is built on a single, unified infrastructure with a unified user experience. Guardium is designed to support and secure a wide range of data environments, including: databases; data warehouses; file systems; and cloud, virtual, and big data-based systems.

Key Findings

Quantified benefits. The following risk-adjusted present value (PV) quantified benefits are representative of those experienced by the companies interviewed:

- **Improves process efficiency in meeting security and compliance requirements by 20%.** IBM Security Guardium improves the process efficiency in meeting security and compliance requirements. Through implementing Guardium, the composite organization improves and automates its database security, auditing protocols and reporting capabilities, enabling the staff to handle security requirements more efficiently.
- **Reduces costs of over $97K each year to recover from a breach.** Using Guardium helps to identify and protect against internal and external threats through monitoring and auditing, vulnerability management, data transformation, real-time security policies, and intelligent reporting. The investment in Guardium helps reduce the likelihood of a breach by 45% by Year 3. Due to this, the investment in Guardium helps to avoid potentially significant costs that could be incurred if a data breach were to occur.

FORRESTER®

ROI
343%

Benefits PV
$3.3 million

NPV
$2.6 million

Payback
<6 months

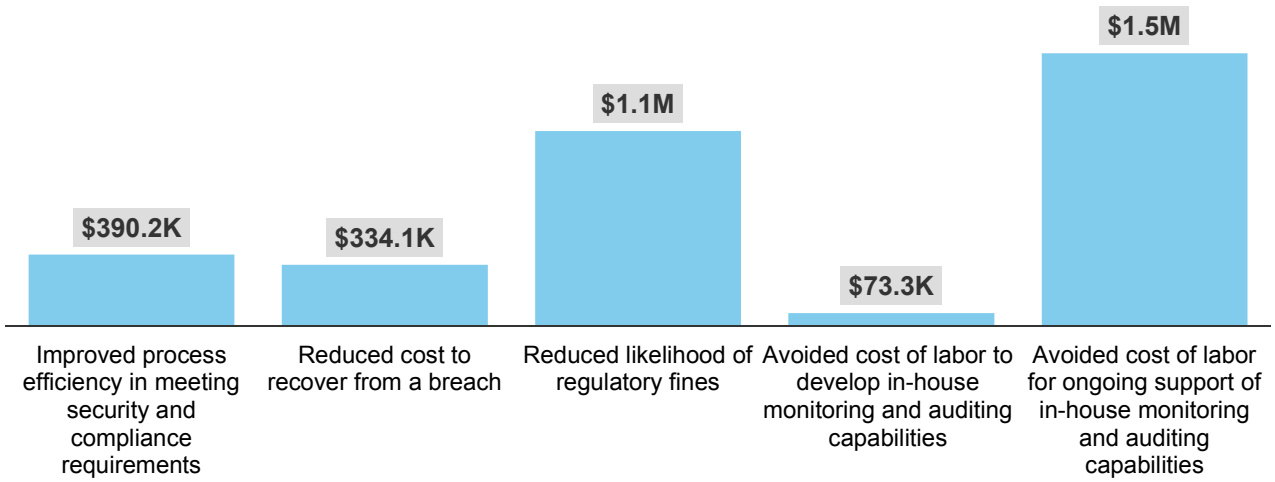
- **Reduces the likelihood of incurring regulatory fines, resulting in savings of over $1.1M over three years.** The investment in Guardium helps clients meet broad compliance and regulatory mandates, such as upcoming GDPR, and provides deeper visibility into the knowledge of sensitive data. Due to this, Guardium reduces the likelihood of incurring a fine to 2%.
- **Avoids the cost of labor to develop and support in-house monitoring and auditing capabilities.** Investing in Guardium means that an alternative in-house solution does not need to be developed, tested, or deployed for securely logging, storing, analyzing, and reporting on the database audit access information, thereby saving the organization the cost of 960 person-hours. It also means that the organization has access to significantly more robust functionality provided by Guardium. The organization also avoids the cost of 6 FTEs required to support an in-house solution.

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

- **Initial costs and annual maintenance of Guardium.** These represent fees paid to IBM for the Guardium solution for their 100-core system.
- **Planning, implementation, professional services, and ongoing support costs.** These represent the mix of internal and external costs associated with the initial planning, implementation, and professional services associated with Guardium, as well the ongoing support.

Forrester's interviews with three existing customers and subsequent financial analysis found that an organization based on these interviewed organizations experienced benefits of $3.3M over three years versus costs of over $752K, adding up to a net present value (NPV) of $2.6M and an ROI of 343%.

Benefits (Three-Year)



FORRESTER®

TEI Framework And Methodology

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

CUSTOMER INTERVIEWS
Interviewed three organizations using Guardium to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION
Designed a composite organization based on characteristics of the interviewed organizations.

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

CASE STUDY
Employed four fundamental elements of TEI in modeling IBM Security Guardium'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.

The IBM Security Guardium Customer Journey

BEFORE AND AFTER THE IBM SECURITY GUARDIUM INVESTMENT

Interviewed Organizations

For this study, Forrester conducted three interviews with IBM Security Guardium customers. Interviewed customers include the following:

INDUSTRY	REGION	INTERVIEWEE
Financial services	US	VP, cyber security management
Insurance	US	Team lead, security and access management
Insurance	US	Senior governance specialist

While interviewed organizations focused on financial services and insurance, IBM Security Guardium supports compliance and data security needs across a wide range of industries.

Key Challenges

Forrester spoke with interviewed organizations to gain deeper insight into the business challenges they faced around data security. Interviewed organizations revealed a number of common drivers for their need of better enterprise data security:

- A need to meet regulatory and compliance requirements.
- A need to increase data security and compliance around big data projects, such as Hadoop, NoSQL, and in-memory.
- The focus on a security, compliance, and data privacy strategy has increased and become more important within the organizations.
- A desire to become more proactive in data security and compliance strategy, as opposed to reactive.
- A requirement to have data security across a variety of environments.
- A desire for more automation in a security solution.
- The need to push beyond compliance to being truly secure.

> "Before Guardium, we had a kind of ugly manual process and patchwork approach. Frankly, it was not very effective at all. What we had before didn't work. That's why we brought in IBM Guardium."
>
> *Team lead, security and access management, insurance organization*

> "We're spread out between hundreds and hundreds of databases and trying to look at that information on a server-by-server basis was tough."
>
> *VP, cyber security management, financial services*

Key Results

Prior to the investment in Guardium, these organizations managed data security and compliance using a patchwork approach with various tools, internally developed solutions, and manual processes. These approaches were seen as inefficient and inadequate for today's security and compliance needs. Each interviewed organization selected Guardium over competing products. The interviews revealed that key results from the Guardium investment include:

- **Guardium helped the organizations meet compliance, reporting, and auditing requirements.** Guardium helps organizations address compliance and regulatory mandates, such as Sarbanes-Oxley, HIPAA, PCI/DSS, and new regulations like the EU's GDPR. In addition, the organizations reported that Guardium monitored the privileged users and blocked unauthorized access. The VP of cyber security management for a financial services institution shared, "Guardium gives us much more insight into the data and the people who are accessing the data than what we had before."
- **Guardium provides improved visibility into sensitive data that the organizations did not have in their previous environments.** The organizations reported that Guardium helped them to have better visibility into their sensitive data and to discover, understand, and classify it. With data growing at a rate of 20% across each of these organizations, having these insights were integral to securing the data. The interviews uncovered that, at times, organizations were not aware of their sensitive data, and Guardium has helped them to uncover potential sources of concern. As these organizations begin taking on more big data projects, where the dangers of data security are magnified, better understanding where their sensitive data lies becomes increasingly important. In addition, Guardium helped the organizations to uncover new insights into their data, helping them make smarter, better decisions with their enterprise data security than ever before.
- **Guardium helps to secure and protect organizations' sensitive data across their entire environment in one centralized system.** Along with helping organizations improve their sensitive data visibility, Guardium is helping these organizations protect and secure that sensitive data in real time. The team lead of security and access management shared, "Having a tool that's real-time gives you the reduced risk of someone doing something that they're not supposed to be doing, which you may have missed with native logging." Guardium works to continuously monitor and control access across an organization's entire environment by securing data repositories such as databases, data warehouses, Hadoop, NoSQL, and in-memory systems and file shares. It also ensures that it is protected, whether stored on- or off-premises, or in big-data, private, or hybrid cloud environments. Interviewed organizations found great value in having a centralized solution to monitor across platforms. As we heard from the senior governance specialist, "There was significant benefit to sticking with Guardium over having to purchase individual tools for each of these different databases and platforms."
- **The organizations felt that working with a strong partner in the space created a trustworthy environment.** IBM is a trusted market leader in the data security and compliance space, and companies felt that working with a market leader provided them with reliability and confidence. Additionally, the scalable solution means that Guardium can support environments of different sizes without additional headcount needed, and with its noninvasive design, it does not hurt the performance of the organizations' databases or data warehouses. As the VP of cyber security management at the financial services institution shared: "Our old solution did not scale as well. Now, we add more databases and the same size team can absorb that into their daily workload, without us having to hire new people." Investing in Guardium meant that these organizations could simplify their

> "Guardium has a lot of built-in reporting and features now, focusing on things like GDPR. So, we can take advantage of that built-in functionality to give us a faster start, without having to build up things from scratch."
>
> *Senior governance specialist, Insurance organization*

> "Guardium is one of the few solutions we've found that can do it all. Their coverage across different database platforms is very good — it's better than anything else that's on the market."
>
> *Team lead, security and access management, insurance organization*

> "Guardium takes all of the different database management systems and consolidates it into one tool versus us needing to use separate systems for Oracle, for SQL server and the like. We can look at all the information in a single pane of glass."
>
> *VP, cyber security management, financial services*

operations while improving the quality of their enterprise data security strategy.

Composite Organization

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an associated ROI analysis that illustrates the areas financially affected. The composite organization is representative of the three companies that Forrester interviewed and is used to present the aggregate financial analysis in the next section. The composite organization that Forrester synthesized from the customer interviews has the following characteristics:

Description of composite. The organization is a global financial services organization, with 20,000 employees and over $1 billion in annual revenue. The company requires security and auditing capabilities for its databases and files to effectively and efficiently comply with the auditing requirements demanded by Sarbanes-Oxley, PCI DSS, and data privacy. They are also concerned about the new GDPR requirements. All attempts to access financial data must be logged; questionable access requests must be analyzed to ensure that they are consistent with defined policies.

Deployment characteristics. The company has a large heterogeneous database environment. It currently has roughly 8,000 databases accessed by a number of enterprise applications. Its databases range from 100GB to 1TB in size, based on type of data stored and the annual growth of data. Its server configuration is made up of multicore IBM System x86 servers. The company purchased the Guardium solution to monitor all of the accesses and modifications that involve the sensitive database servers that are relevant to SOX, PCI DSS, HIPAA and data privacy, and new regulations like GDPR. All network and local traffic is monitored by the Guardium system. Guardium's extensive coverage of a wide variety of databases and applications ensured that the company could deploy a single solution enterprisewide.

Key assumptions

- 20,000 total employees
- 8,000 databases
- Key concerns include: SOX, PCI DSS, HIPAA, data privacy, and GDPR

Analysis Of Benefits

QUANTIFIED BENEFIT DATA AS APPLIED TO THE COMPOSITE

Total Benefits							
Ref.	**Benefit**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Atr	Improved process efficiency in meeting security and compliance requirements	$0	$106,875	$160,313	$213,750	$480,938	$390,242
Btr	Reduced cost to recover from a breach	$0	$97,740	$136,836	$175,932	$410,508	$334,122
Ctr	Reduced likelihood of regulatory fines	$0	$425,000	$425,000	$425,000	$1,275,000	$1,056,912
Dtr	Avoided cost of labor to develop in-house monitoring and auditing capabilities	$51,840	$0	$25,920	$0	$77,760	$73,261
Etr	Avoided cost of labor for ongoing support of in-house monitoring and auditing capabilities	$0	$594,000	$594,000	$594,000	$1,782,000	$1,477,190
	Total benefits (risk-adjusted)	$51,840	$1,223,615	$1,342,069	$1,408,682	$4,026,206	$3,331,727

Improved Process Efficiency In Meeting Security And Compliance Requirements

The first benefit examines how IBM Security Guardium improves the process efficiency in meeting security and compliance requirements. Through implementing Guardium, the composite organization improves and automates its data security, auditing protocols, and reporting capabilities, enabling the staff to handle security requirements more efficiently. The process is streamlined with automated and centralized controls and simplified audit review processes, thus reducing the time and cost of compliance. With near zero impact to the performance of the underlying data sources, Guardium ensures that organizations have the ability to know and report, in real time, on who is accessing (and reading, changing, or deleting) sensitive data. Thus, Guardium helps individuals such as database administrators, data privacy specialists, and auditors become more efficient and save the company money.

To calculate this benefit, Forrester assumes:

- The organization has forty-five database administrators (DBAs) and five FTEs (such as data privacy specialists or auditors) involved with security and compliance issues.
- DBAs spend an average of 40% of their time on security and compliance; the five other FTEs spend an average of 20% of their time working on processes that deal with meeting the regulatory and security requirements.

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 composite organization expects risk-adjusted total benefits to be a PV of more than $3.3 million.

Reduction in time spent on security and compliance requirements with Guardium: **20%** by Year 3

- With Guardium, the organization reduces the time spent on security and compliance requirements by 10% in Year 1; by Year 3, as the team members become increasingly proficient with Guardium, the team reduces time spent on these requirements by 20%.
- Forrester also adjusts productivity savings by assuming that only 50% of this time saved is used for productive work.

This process efficiency savings will vary with:

- Number of team members involved with security and compliance requirements.
- Average percent of time spent on security and compliance issues.
- Average salary.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $390,242.

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.

Improved Process Efficiency In Meeting Security and Compliance Requirements: Calculation Table

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
A1	Number of DBAs		45	45	45
A2	Number of other staff involved with security and compliance		5	5	5
A3	Percent of DBA time spent on security and compliance issues		40%	40%	40%
A4	Percent of other staff time spent on security and compliance		20%	20%	20%
A5	Average annual salary		125,000	125,000	125,000
A6	Percent reduction in time spent on security and compliance		10%	15%	20%
A7	Percent captured		50%	50%	50%
At	Improved process efficiency in meeting security and compliance requirements	((A1*A3)+(A2*A4)) *A5*A6*A7	$118,750	$178,125	$237,500
	Risk adjustment	↓10%			
Atr	Improved process efficiency in meeting security and compliance requirements (risk-adjusted)		$106,875	$160,313	$213,750

Reduced Cost To Recover From A Breach

Through its investment in Guardium, the composite organization gains greater efficiency and effectiveness in its data security, auditing, and reporting capabilities that improve compliance. Additionally, it is able to monitor user activity to detect and respond to potential threats in real time. Using Guardium helps to identify and protect against internal and external threats through monitoring and auditing, vulnerability assessment, data transformation, real-time security policies, and intelligent reporting.

Due to this, the investment helps the organization avoid potentially significant costs that it could incur if a data breach against its records were to occur. To calculate the value of this benefit for the composite organizaton, Forrester assumes:

Average cost of a data breach:
$3.62 million

- Based on research conducted by the Ponemon Institute, the average total cost of a data breach in 2017 was $3.62 million. This cost consists of both direct and indirect expenses. Direct expenses include: engaging discovery, legal, and investigation experts; outsourcing hotline support; providing free credit monitoring subscriptions; and discounts for future products and services. Indirect costs include: in-house investigations and communication; and customer loss resulting from turnover or diminished customer acquisition rates.[1]
- The probability of a breach is about 12% in any given year.
- With the features and functionality of Guardium, the organization is now able to significantly reduce the likelihood of a breach. As the security team becomes increasingly proficient in analyzing data, the likelihood of a breach becomes less likely year after year. By Year 3, the organization sees a 45% reduced likelihood of a data breach.

Reduced likelihood of data breach with Guardium:
45%

It is important to note that Forrester took a conservative approach to calculating this benefit. With Guardium's real-time security and monitoring, IBM can help proactively protect data and eliminate breaches. Forrester urges readers to consider this when evaluating the overall impact of Guardium on their environment. Additionally, it's important to consider how a breach could affect a big data project — with much more data involved, a breach could become increasingly dangerous and expensive for an organization.

The reduced cost to recover from a breach will vary from a number of forces, such as:

- The actual cost of the data breach.
- Industry, location, and company size variance on the probability of a data breach.
- The use and breadth of Guardium deployment.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $334,122.

Reduced Cost To Recover From A Breach: Calculation Table

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
B1	Average data breach cost		$3,620,000	$3,620,000	$3,620,000
B2	Probability of a data breach		12%	12%	12%
B3	Reduced likelihood of breach with IBM Guardium		25%	35%	45%
Bt	Reduced cost to recover from a breach	B1*B2*B3	$108,600	$152,040	$195,480
	Risk adjustment	↓10%			
Btr	Reduced cost to recover from a breach (risk-adjusted)		$97,740	$136,836	$175,932

Reduced Likelihood Of Regulatory Fines

Along with the cost of a data breach, there is significant risk associated with getting fined by a court or other regulatory body for failure to comply with regulations. Through its investment in Guardium, the composite organization provides the broad and deep capabilities clients need to help them meet compliance and regulatory mandates, and has deeper visibility into and knowledge of its sensitive data. The organization has

gained greater efficiency and effectiveness through automating the entire compliance auditing process, including compliance workflows, discovery and classification, real-time monitoring to create audit records, and vulnerability assessments to harden data sources. Furthermore, through leveraging hundreds of prebuilt, customizable reports and accelerators with out of the box policies and groups, organizations are able to simplify the process of achieving regulatory compliance while improving accuracy. Due to this, the organization is able to reduce the likelihood that it will be fined.

To calculate this benefit, Forrester assumes:

- Without proper measures in place to prove compliance, Forrester conservatively forecasts that the organization could face a $25 million fine each year.
- By investing in Guardium, the representative organization is better able to meet its security requirements and reduces the probability of a fine to 2%.

The reduced likelihood of regulatory fines can vary with:

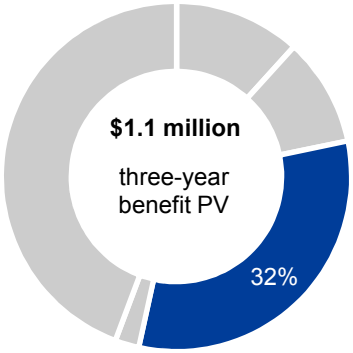
- The actual cost of a fine.
- The use and breadth of Guardium deployment.

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year risk-adjusted total PV of $1.06 million.

While not included in the calculation as it has not been enforced as of date of publication, the general data protection regulation (GDPR) goes into enforcement on May 25, 2018; it is important to consider how this will impact potential regulatory fines. Companies who do business within the EU will now need to comply with new data privacy requirements.

By helping to address key data protection requirements, Guardium helps to reduce the likelihood of facing a GDPR regulatory fine. According to Forrester, the GDPR is "the most financially punitive privacy law we have seen to date," allowing fines of up to 4% of violators' global revenues or €20 million, whichever is greater.[2] This could have a serious effect on the regulatory fine a company could face, meaning that there is a benefit to having Guardium help you understand and document where regulated data lies and who's touching it.

In addition, examining the potential for regulatory fines through the lens of big data, we can see that the cost of a fine or the probability of a fine could also be increased; while not directly calculated here, the use of Guardium helps organizations to reduce this risk.



Reduced likelihood of regulatory fines: **32%** of total benefits

Potential impact of GDPR: fines up to 4% of global revenues or €20 million

Reduced Likelihood Of Regulatory Fines: Calculation Table

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
C1	Average potential regulatory fine		$25,000,000	$25,000,000	$25,000,000
C2	Probability of fine		2%	2%	2%
Ct	Reduced likelihood of regulatory fine	C1*C2	$500,000	$500,000	$500,000
	Risk adjustment	↓15%			
Ctr	Reduced likelihood of regulatory fine (risk-adjusted)		$425,000	$425,000	$425,000

FORRESTER®

Avoided Cost Of Labor To Develop In-House Monitoring And Auditing Capabilities

The composite organization avoided the costs of developing an alternative solution with its investment in Guardium. The "alternative option" used for this comparison is based on the native logging capabilities provided by the database platforms for capturing and storing the audit logs. The organization would have to develop new software and scripts in-house for analyzing and reporting on this information, and then distribute the reports to those doing the audits and others with oversight responsibilities. However, it is important to note that the in-house solution would not have provided the real-time security controls offered by the Guardium product due to the batch nature of logging utilities. It also could not provide the same level of automated functionality and analysis.

To calculate the value of this benefit, Forrester considers:

- To develop an alternative solution, such as a manual, in-house solution for database monitoring and auditing, the composite organization would need three resources for eight weeks, or 960 person-hours (based on a 40-hour work week).
    - This time would be used to develop, test, and deploy the required functionality for securely logging, storing, analyzing, and reporting on the database audit access information.
- Two years down the line, an effort representing half the initial investment, or 480 person-hours, would be needed for enhancements.
- Forrester assumes an average fully loaded hourly salary of $60 for these resources.

Hours of avoided labor:
960 person-hours

A variety of factors could affect the cost associated to develop this solution, such as:

- Number of resources or hours required to build the solution.
- The average fully loaded salary of these resources.
- The breadth of enhancements required in Year 2.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $73,261.

Avoided Cost Of Labor To Develop In-House Monitoring And Auditing Capabilities: Calculation Table

Ref.	Metric	Calculation	Initial	Year 1	Year 2
D1	Person-hours needed to create in-house monitoring and auditing capabilities	8 weeks*3 resources	960		480
D2	Average fully loaded hourly salary		$60		$60
Dt	Avoided cost of labor to develop in-house monitoring and auditing capabilities	D1*D2	$57,600		$28,800
	Risk adjustment	↓10%			
Dtr	Avoided cost of labor to develop in-house monitoring and auditing capabilities (risk-adjusted)		$51,840	$0	$25,920

Avoided Cost Of Labor For Ongoing Support Of In-House Monitoring And Auditing Capabilities

In addition to the labor needed to develop the solution, the composite

organization would also require six additional resources to maintain it over time. These resources would include two dedicated DBAs responsible for providing ongoing database support for the storage and analysis of the logging/auditing data while also being responsible for the reporting of all database access by DBAs. The other support resources would be application support specialists responsible for ongoing auditing and reporting of all non-DBA (applications and non-DBA power users) access to the databases while also providing the database error diagnosis, troubleshooting, and performance improvement support that is enabled by the Guardium system currently.

To calculate this benefit, Forrester looks at:

- The six avoided resources that would be required each year to take on the tasks describe above.
- Assumes an average fully loaded annual salary across the six FTEs of $110,000.

Forrester considers the following factors that could cause variance in this benefit:

- The number of FTEs that would be required (and are hence avoided) to support the in-house system described above.
- The average annual salary of these resources.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $1.4 million.

Number of future hires avoided:
6 FTEs

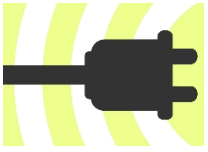
Avoided Cost Of Labor For Ongoing Support Of In-House Monitoring And Auditing Capabilities: Calculation Table

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
E1	FTEs avoided		6	6	6
E2	Average annual salary		$110,000	$110,000	$110,000
Et	Avoided cost of labor for ongoing support of in-house monitoring and auditing capabilities	E1*E2	$660,000	$660,000	$660,000
	Risk adjustment	↓10%			
Etr	Avoided cost of labor for ongoing support of in-house monitoring and auditing capabilities (risk-adjusted)		$594,000	$594,000	$594,000

Alternative Calculation — Savings From Retired Third-Party Solution

For organizations that are moving from a third-party solution to IBM Security Guardium, instead of considering the benefit of avoided cost of labor for developing and supporting an in-house solution, the organization would consider the avoided costs associated with its retired solution. Important costs to consider include:

- Annual cost of licensing the solution.
- Annual maintenance costs/percentage paid to third party.
- Annual cost of professional services associated with the solution.
- Annual cost of labor associated with maintaining the solution.



Alternative to avoided in-house development:
retired third-party solution

Additional Features And Functionality That Maximize Potential Benefits

Organizations often discover additional features, functionality, and modules that Guardium supports which enable them to get deeper value from their investment. As we heard from one insurance organization, "We've been exploring the other features within Guardium to try and expand the security functionality and get further benefits out of the tool." Several features and functionality that are included within the IBM Security Guardium product family can enable organizations to maximize their existing benefits. These features include:

- **Customizable compliance workflows and compliance accelerators**. Compliance workflows help organizations automate key processes such as report generation, distribution, electronic sign-offs, and escalations. In addition, Guardium has built-in expertise with features like the GDPR accelerator and the PCI DSS accelerator. These accelerators help you leverage prebuilt reports, policies, and groups to help you improve your efficiency with meeting these requirements through quickly assembling and centralizing auditable data and eliminating compliance-related manual work.
- **Improved encryption modules**. IBM Guardium Data Encryption helps to protect on-premises data from misuse through providing a variety of key encryption capabilities for files, databases, applications, and Teradata environments. The portfolio's encryption capabilities allow for rapid implementation, centralized key and policy management, and granular support for regulatory compliance. Furthermore, by leveraging its live-data transformation capabilities, organizations can encrypt files and databases without taking them offline.

  IBM Multi-Cloud Data Encryption protects data in dedicated private, hybrid, and public clouds, supporting distributed encryption with centralized management and advanced cryptographic splitting technology.

  Both Guardium Data Encryption and Multi-Cloud Data Encryption help organizations achieve pseudonymization, a recommendation set forth by the GDPR, which can improve an organization's ability to avoid regulatory fines.
- **Enhanced reporting and dashboards**. To optimize the Guardium experience, IBM has improved the dashboard with a new user interface that enables easier navigation with advanced portal search. Guardium leverages machine learning and outlier detection to help analyze risk and anomalous activity, with an investigation dashboard for streamlined analysis.
- **Big data lake, purpose-built for data security requirements.** IBM Security Guardium Big Data Intelligence is a big data lake that is purpose built for data security requirements. This NoSQL platform enables organizations to enrich Guardium's data protection capabilities with the ability to retain large quantities of historical data over long time horizons to deliver new analytics insights while also helping to streamline operations, thus reducing costs and improving the speed of report delivery.
- **Business-consumable data risk control center.** To help executives and their teams to uncover, analyze and visualize data-related business risks, IBM Data Risk Manager empowers organizations to see and communicate the business impact of data security information

Additional features and functionality:

- Customizable workflows and accelerators
- Improved encryption module
- Enhanced reporting and dashboards
- Big data lake, purpose-built for data security requirements
- Business-consumable data risk control center

and more efficiently take action to protect their mission-critical data. This helps save organizations time, while also facilitating more productive conversations between executives and other data stakeholders.

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 IBM Security Guardium and later realize additional uses and business opportunities, including:

- **Leveraging additional features and functionality.** As described above, leveraging many of the new or included Guardium features and functionality can improve the benefits received from the deployment of Guardium.
- **Rolling out Guardium to cover more environments.** Where Guardium covers a wide variety of data environments, including on-premises, off-site, private or hybrid clouds, or in a big data environment, organizations can increase their benefits by implementing Guardium across new environments.
- **Integrating Guardium with additional security products.** Guardium supports heterogeneous integration with other industry-leading security solutions, vulnerability standards, applications, and more via REST API. Guardium also allows for seamless integration with other IBM Security Solutions. Through leveraging these products together and combining and analyzing the security data each collects, organizations have the potential to garner stronger insights and achieve greater value than if these technologies were used alone.

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

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.

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
Ftr	Initial cost and annual maintenance of Guardium	$385,000	$69,300	$69,300	$69,300	$592,900	$557,339
Gtr	Planning, implementation, professional services, and ongoing support	$23,925	$68,750	$68,750	$68,750	$230,175	$194,896
	Total costs (risk-adjusted)	$408,925	$138,050	$138,050	$138,050	$823,075	$752,235

Overview of Costs

The composite organization incurred the following costs associated with their deployment of IBM Security Guardium:

- **Initial costs and annual maintenance of Guardium.** These represent fees paid to IBM for the Guardium solution of their 100-core system.
- **Planning, implementation, professional services, and ongoing support costs.** These represent the mix of internal and external costs associated with the initial planning, implementation, and professional services associated with Guardium, as well the ongoing support.

Costs can vary with:

- Scope of deployment.
- Professional services utilized.
- Average fully loaded salary of internal team members.

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year risk-adjusted total PV of $752,235.

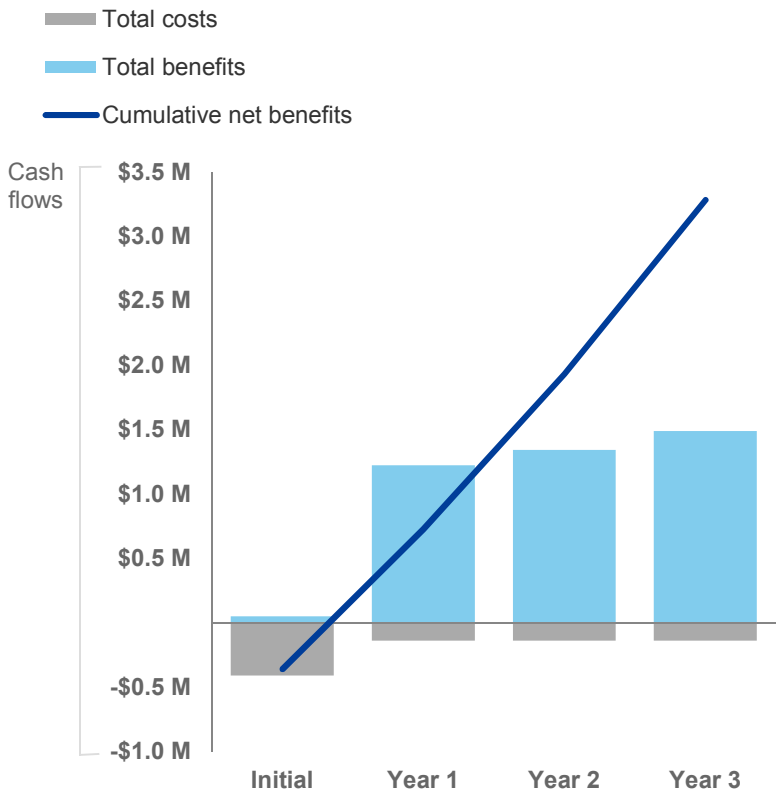
The table above shows the total of all costs across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total costs to be a PV of more than $752,235.

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.

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 Table (Risk-Adjusted)

	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Total costs	($408,925)	($138,050)	($138,050)	($138,050)	($823,075)	($752,235)
Total benefits	$51,840	$1,223,615	$1,342,069	$1,408,682	$4,026,206	$3,331,727
Net benefits	($357,085)	$1,085,565	$1,204,019	$1,270,632	$3,203,131	$2,579,492
ROI						343%
Payback period						<6

FORRESTER®

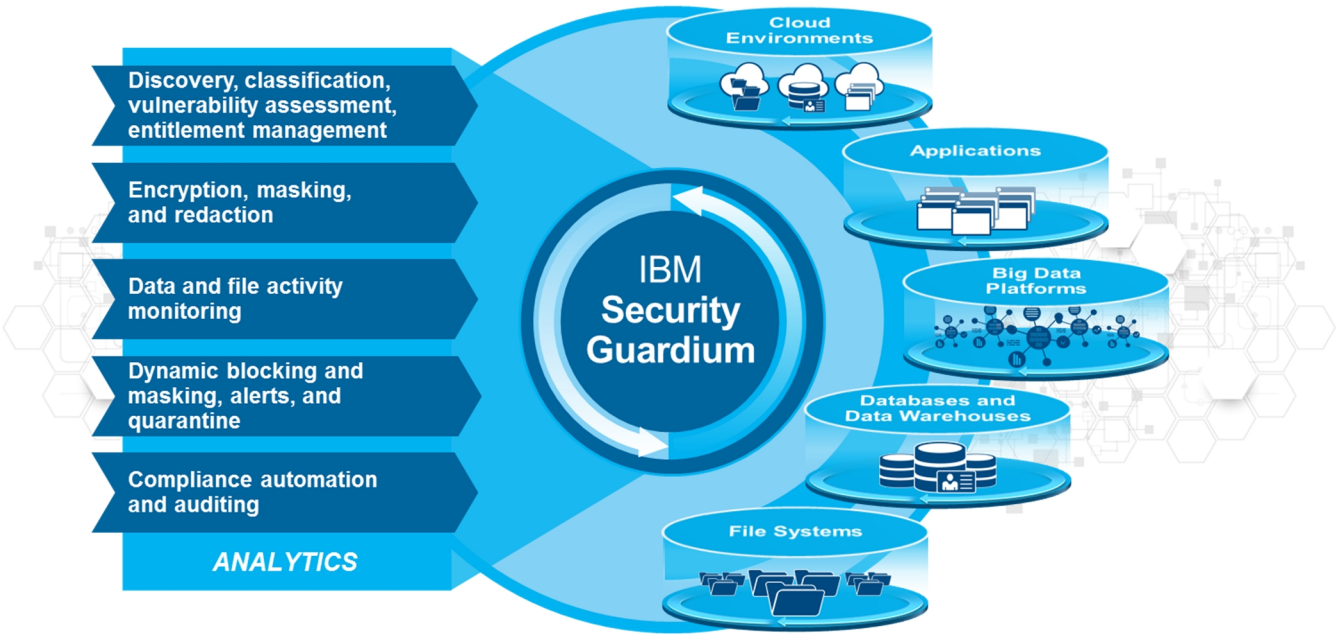
IBM Security Guardium: Overview

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

IBM Security Guardium is designed to safeguard critical data wherever it resides. This comprehensive data protection platform empowers security teams to automatically analyze what is happening across the data environment to help minimize risk, protect sensitive data from internal and external threats, and seamlessly adapt to changes that affect data security.

Guardium applies intelligence and automation to enable a centralized, strategic approach to securing the sensitive data that is vital for business success and survival. Leveraging Guardium's end-to-end graphical user interface, security teams can identify and remediate risks to sensitive data, whether the data is in motion or at rest. And this unified approach extends to a broad range of both structured and unstructured data repositories, including databases, data warehouses, Hadoop, NoSQL, in-memory systems, and file systems.

In fact, Guardium uses a flexible and modular approach to meet a wide range of data security and protection requirements — from basic compliance, monitoring, and encryption to comprehensive data protection — in a cost-effective, scalable way. Additionally, unlike a point solution, Guardium supports heterogeneous integration with other industry-leading security solutions, vulnerability standards, applications, and more. Guardium also provides best-of-breed integration with IBM Security solutions. As a strategic partner, IBM empowers organizations to reduce security vulnerabilities and manage risk across the most complex IT environments.



FORRESTER®

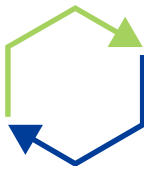
Appendix A: Total Economic Impact

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] Source: “2018 Cost of Data Breach Study: Global Overview,” Ponemon Institute, June 2017.
[2] Source: “Q&A: What Global Marketers Need To Know About European Privacy Laws,” Forrester Research, Inc., October 2016.