Forrester Total Economic Impact™ Study
Commissioned By IBM

Project Director:
Adrienne Capaldo
September 2015

The Total Economic Impact™ Of IBM Security Guardium

Data security presents a complex challenge to organizations. Not only is it a concern for them, but customers are more aware about the security of their data. The value of customer data has increased exponentially over time, but with it comes an increase in potential liability and exposure. Combine this with the rapid growth of data within organizations' environments, the complexity of regulations and compliance across industries, and the threat of internal and external attacks, and it highlights the importance of creating a successful enterprise security and compliance strategy. Additionally, companies are struggling 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.

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 surveyed and interviewed several 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 and 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.

Our interviews and subsequent financial analysis found that a composite organization experienced the risk-adjusted ROI, benefits, and costs shown below.

KEY FINDINGS: IBM SECURITY GUARDIUM EFFICIENTLY SECURES SENSITIVE ENTERPRISE DATA AND REDUCES RISK

ROI: 218%	NPV: $1.8 million	Payback: 7.4 months

METHODOLOGY

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 Guardium as part of their overall data security and compliance strategy. To achieve these objectives, Forrester conducted a survey of three large organizations that are using IBM Guardium.

Forrester then designed a composite organization based on the characteristics of these companies. A representative financial model was constructed using the TEI methodology.

Lastly, Forrester risk-adjusted the financial model based on issues and concerns the surveyed organizations highlighted. Some cost and benefit categories included a broad range of responses or had a number of outside forces that might have affected the results. For that reason, some cost and benefit totals have been risk-adjusted and are detailed in each relevant section.

The Rationale For Guardium

Forrester asked the surveyed companies about the business challenges their organizations faced around data security. The interviews revealed a number of common drivers for why the companies needed to invest in enterprise data security, which included:

- A need to meet regulation 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 prior audit failure that resulted in a need to minimize the risk of it happening in the future.

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 organization interviewed selected Guardium over competing products. The interviews revealed that Guardium was selected because:

- **Guardium helped the organizations meet compliance reporting and auditing requirements.** In addition, the organizations reported that Guardium monitored the privileged users and blocked unauthorized access. Guardium also has coverage across many different environments, including different data platforms, databases, data warehouses, Hadoop, big data, repositories, and files and applications, as well as protocols.
- **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. We found that, at times, organizations were not aware of all of their sensitive data, and Guardium helped them 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 regards to their enterprise data security than ever before.
- **Guardium helps to secure and protect organizations' sensitive data across their entire environment.** Along with helping organizations improve their visibility into their sensitive data, Guardium is helping these organizations protect and secure their sensitive data in real time. Guardium works to continuously monitor and control access across an organization's entire environment, securing data repositories such as databases, data warehouses, Hadoop, NoSQL, and in-memory systems and file shares.
- **IBM is a trusted leader in the data security and compliance space.** The organizations felt that working with a strong partner in the space created a trustworthy environment. Additionally, the scalable solution means that Guardium can support environments of different sizes, and with its noninvasive design, it does not hurt the performance of the organizations' databases or data warehouses. Investing in Guardium meant that these organizations could simplify their operations while improving the quality of their enterprise data security strategy.

Analysis

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

- The company is a US-based financial services organization with 20,000 employees and over $1 billion in annual revenue.
- The company requires security and auditing capabilities for its databases to effectively and efficiently comply with the auditing requirements demanded by Sarbanes-Oxley, PCI DSS, and data privacy. All attempts to access financial data must be logged; questionable access requests must be analyzed to ensure that they are consistent with defined policies. All network and local traffic is monitored by the Guardium system.
- 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, and data privacy. Guardium's extensive coverage of a wide variety of databases and applications ensured that the company could deploy a single solution enterprisewide.

Benefits

As a result of its investment in Guardium, the composite organization experienced a number of quantified benefits:

- Improved process efficiency in meeting security and compliance requirements.
- Reduced cost to recover from a breach.
- Reduced likelihood of regulatory fines.
- Avoided cost of labor to develop in-house monitoring and auditing capabilities.
- Avoided cost of labor for ongoing support of in-house monitoring and auditing capabilities.

IMPROVED PROCESS EFFICIENCY IN MEETING SECURITY AND COMPLIANCE REQUIREMENTS

Our first benefit looks at the ability to improve the process efficiency in meeting security and compliance requirements. Through implementing Guardium, the representative organization was able to improve and automate its database security, auditing protocols, and reporting capabilities, enabling the staff to handle security requirements more quickly. The process is streamlined with automated and centralized controls and simplified audit review processes, thus reducing the time and cost of compliance. Guardium helps individuals such as database administrators, data privacy specialists, and auditors become more efficient and save the company money.

To calculate the improved process efficiency in meeting security and requirements, we estimate that 45 DBAs and five other staff members, such as those mentioned above, are involved with security and compliance requirements. We assume that these DBAs spend an average of 40% of their time on security and compliance issues, while the other employees spend an average of 20% of their time working on processes that deal with meeting the regulatory and security requirements. We see that by implementing Guardium, the organization is initially able to reduce the amount of time it spends on these requirements by 10% in Year 1. As time goes by, team members become increasingly proficient with using Guardium, and by

Year 3, the organization is able to reduce the time it spends on security requirements by 20%. Forrester also adjusts productivity savings by assuming that only 50% of this time saved is used for productive work. Table 1 highlights how this was calculated.

There are a number of factors that could affect the team's ability to reduce the time it spends on security requirements. To compensate for these variations, Forrester has reduced the value of this benefit by 10%. The risk-adjusted present value total benefit over three years is $390,242.

Forrester urges the reader to consider the magnitude of impact this improved efficiency could have when it comes to ensuring the security and compliance of big data projects, though we don't directly calculate this here,

Table 1
Improved Process Efficiency In Meeting Security And Compliance Requirements

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 issues		20%	20%	20%
A5	Average annual salary		$125,000	$125,000	$125,000
A6	Percent reduction in time spent on security and compliance requirements with IBM Guardium		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**

Source: Forrester Research, Inc.

Reduced Cost To Recover From A Breach

Through its investment in Guardium, our representative organization has gained greater efficiency and effectiveness in its database 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 management, data transformation, real-time security policies, and intelligent reporting.

Due to this, the investment also helps the organization avoid potentially significant costs that it could incur if a data breach against its records were to occur. We estimate that the probability of a breach is about 12% in any given year. While the actual cost of a data breach could be astronomical, Forrester conservatively estimates the average potential cost of a data breach to our representative organization to be around $3 million in any given year, which includes the cost of discovery, legal, investigative, and administrative expenses, as well as the cost of supporting customers and the lost revenue associated with customer churn,

among other expenses. 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.

There are a number of outside forces that could affect the cost of a data breach or the reduced likelihood of a breach; to account for this, Forrester has reduced the value of this benefit by 10%. This results in a risk-adjusted present value total benefit of $276,897. Table 2 shows this calculation.

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.

Table 2
Reduced Cost To Recover From A Data Breach

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
B1	Average data breach cost		$3,000,000	$3,000,000	$3,000,000
B2	Probability of 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	$90,000	$126,000	$162,000
	Risk adjustment	↓ 10%			
Btr	**Reduced cost to recover from a breach (risk-adjusted)**		**$81,000**	**$113,400**	**$145,800**

Source: Forrester Research, Inc.

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, our representative organization has gained greater efficiency and effectiveness through automating the entire compliance auditing process.

Due to this, the organization is able to reduce the likelihood that it will be fined. To calculate this risk, we look at the amount of a potential fine. While it is difficult to forecast the actual cost of a fine, Forrester conservatively estimates that the organization could face a $25 million fine each year without proper measures in place to prove compliance. 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 calculation is shown in Table 3. Forrester understands that there are a number of variables that could potentially affect this calculation. To assume for that risk, we have adjusted the benefit down by 15%, for a total three-year present value risk-adjusted benefit of $1,056,912.

When we look at 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 be increased; while we don't directly calculate this here, the use of Gaurdium helps organizations to reduce this risk.

Table 3
Reduced Likelihood Of Regulatory Fines

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 fines	C1*C2	$500,000	$500,000	$500,000
	Risk adjustment	↓ 15%			
Ctr	**Reduced likelihood of regulatory fines (risk-adjusted)**		**$425,000**	**$425,000**	**$425,000**

Source: Forrester Research, Inc.

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 was 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.

In order 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 man-hours, 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 man-hours, would be needed for enhancements. Table 4 highlights this calculation.

There are a number of factors that could affect the team's ability to develop this solution. To compensate for these variations, Forrester has reduced the value of this benefit by 10%. The total three-year present value risk-adjusted cost savings come to $73,261.

Table 4
Avoided Cost Of Labor To Develop In-House Monitoring And Auditing Capabilities

Ref.	Metric	Calculation	Initial	Year 1	Year 2
D1	Man-hours needed to create in-house monitoring and auditing capabilities	8 weeks * 3 resources	960		480
D2	Average 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**

Source: Forrester Research, Inc.

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 need three resources to maintain it over time. The first resource would be a dedicated DBA 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 second and third ongoing support resources would be two 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.

These three resources are assumed to be compensated at an average fully loaded salary of $125,000. Table 5 illustrates this calculation. The total three-year present value risk-adjusted cost savings come to $839,313.

Again, to compensate for factors that could affect this calculation, Forrester risk-adjusted this benefit down by 10%.

Table 5
Avoided Cost Of Labor For Ongoing Support Of In-House Monitoring And Auditing Capabilities

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
E1	FTEs avoided		3	3	3
E2	Average annual salary		$125,000	$125,000	$125,000
Et	Avoided cost of labor for ongoing support of in-house monitoring and auditing capabilities	E1*E2	$375,000	$375,000	$375,000
	Risk adjustment	↓ 10%			
Etr	**Avoided cost of labor for ongoing support of in-house monitoring and auditing capabilities (risk-adjusted)**		**$337,500**	**$337,500**	**$337,500**

Source: Forrester Research, Inc.

Total Benefits

The total quantified benefits, as well as present values (PVs) discounted at 10%, are shown in the table below. Over three years, the composite organization expects risk-adjusted total benefits to be a PV of $2.6 million.

Table 6
Total Benefit Cash Flows (Risk-Adjusted Estimates)

Ref.	Benefit Category	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	$81,000	$113,400	$145,800	$340,200	$276,897
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	$337,500	$337,500	$337,500	$1,012,500	$839,313
	Total benefits (risk-adjusted)	**$51,840**	**$950,375**	**$1,062,133**	**$1,122,050**	**$3,186,398**	**$2,636,625**

Source: Forrester Research, Inc.

Costs

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

› Initial cost and annual maintenance of Guardium.

› Planning, implementation, and professional services.

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

Total Costs

The total costs, as well as present values (PVs) discounted at 10%, are shown in the table below. Over three years, the composite organization expects risk-adjusted total costs to be a PV of $828,085.

Table 7
Total Cost Cash Flows (Risk-Adjusted Estimates)

Ref.	Cost Category	Initial	Year 1	Year 2	Year 3	Total	Present Value
Ftr	Initial cost and annual maintenance of Guardium	$555,500	$99,990	$99,990	$99,990	$855,470	$804,160
Gtr	Planning, implementation, and professional services	$23,925	$0	$0	$0	$23,925	$23,925
	Total costs (risk-adjusted)	**$579,425**	**$99,990**	**$99,990**	**$99,990**	**$879,395**	**$828,085**

Source: Forrester Research, Inc.

Results Summary

The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the composite organization's investment in IBM Security Guardium..

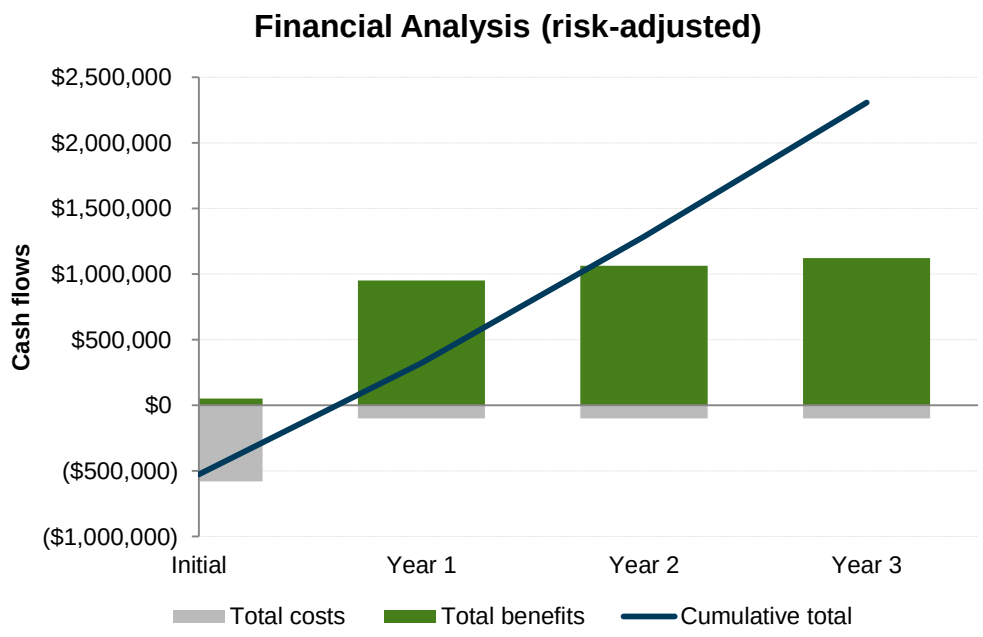
The table below shows the risk-adjusted ROI, NPV, and payback period values.

Cash Flow Analysis (Risk-Adjusted Estimates)

Summary	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($579,425)	($99,990)	($99,990)	($99,990)	($879,395)	($828,085)
Total benefits	$51,840	$950,375	$1,062,133	$1,122,050	$3,186,398	$2,636,625
Total	**($527,585)**	**$850,385**	**$962,143**	**$1,022,060**	**$2,307,003**	**$1,808,540**
ROI						**218%**
Payback period (months)						**7.4**

Source: Forrester Research, Inc.

The graph below shows the risk-adjusted cash flow.



Source: Forrester Research, Inc.

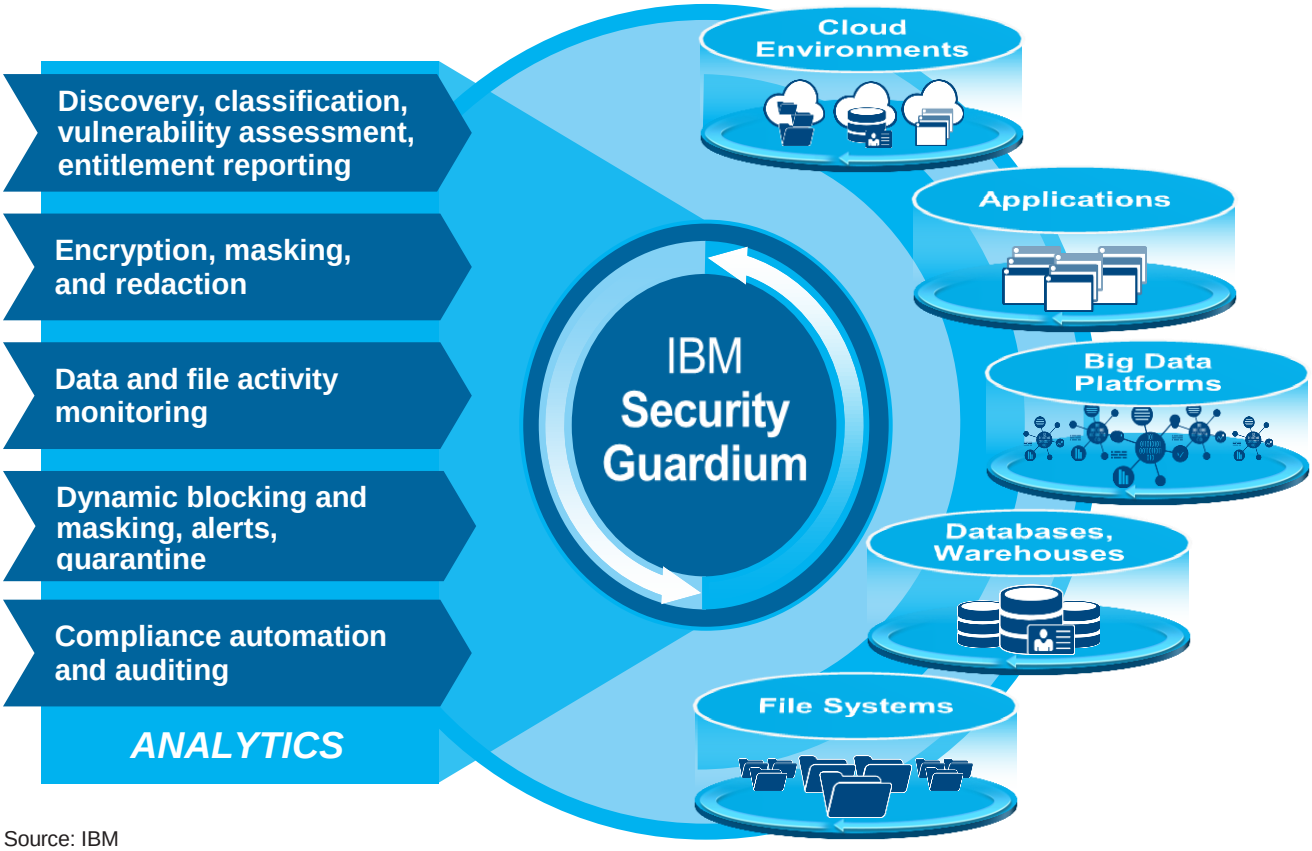
About IBM Guardium

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

IBM Security Guardium, formerly known as IBM InfoSphere 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 provides a comprehensive approach to protecting the data that is the heart of most organizations — 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.



Source: IBM

DISCLOSURES

- The study is commissioned by IBM and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.
- Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the report to determine the appropriateness of an investment in IBM Security Guardium.
- IBM reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.

GLOSSARY

Discount rate: The interest rate used in cash flow analysis to take into account the time value of money. Companies set their own discount rate based on their business and investment environment. Forrester assumes a yearly discount rate of 10% for this analysis. Readers are urged to consult their respective organizations to determine the most appropriate discount rate to use in their own environment.

Net present value (NPV): The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made, unless other projects have higher NPVs.

Present value (PV): The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.

Payback period: The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

Return on investment (ROI): A measure of a project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits minus costs) by costs.

Internal rate of return (IRR): The interest rate that will bring a series of cash flows (positive and negative) to an NPV of zero.

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.

ABOUT TEI

Total Economic Impact™ (TEI) 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. The TEI methodology consists of four components to evaluate investment value: benefits, costs, risks, and flexibility.
http://www.forrester.com/marketing/product/consulting/tei.html