A Forrester Total Economic Impact™
Study Commissioned By Imperva
January 2018

The Total Economic Impact™ Of Imperva SecureSphere

FORRESTER®

Table Of Contents

Project Director:
Sebastian Selhorst

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 quotes from the interviewed customers

"Imperva's SecureSphere capabilities are fantastic tools in helping a CISO detect, prevent, and manage risk."

Chief information security officer (CISO) at a data analytics and risk assessment company

"Imperva is a key element of what we do to pass all of our regulatory requirements. And in addition to compliance, Imperva helps us to be proactive in terms of protecting our sensitive databases from security threats."

Director of IT operations at a global technology company

Executive Summary

Data is the lifeblood of today's digital businesses; organizations need to protect it from theft, misuse, and abuse. Hacked customer data can erase millions in profits, stolen IP can destroy competitive advantage, and unnecessary privacy abuses can bring unwanted scrutiny and fines from regulators while damaging reputations. Businesses are therefore required to audit, monitor, and secure sensitive information, such as financial records, personally identifiable information (PII), or medical records to comply with ever-increasing regulatory mandates.

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

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed two customers with multiple years of experience using SecureSphere. These companies must comply with a multitude of regulations and protect data on hundreds of databases. For several years prior to using SecureSphere, these companies had another database security and monitoring solutions in place. However, they found that these legacy solutions were not very scalable, were labor-intensive, and were costly to administer and maintain. These challenges led to the choice of deploying Imperva SecureSphere.

Key Findings

Quantified benefits. The following risk-adjusted quantified benefits are representative of those experienced by the companies interviewed:

- **Legacy software solution cost savings and avoidance with a three-year, risk-adjusted present value (PV) of $2.4 million.** The interviewed organizations reported that their legacy database security solutions were rather expensive. By decommissioning its legacy solution, an organization can save on maintenance and support costs and avoid costs for future upgrades.
- **Productivity gains for data security staff with a risk-adjusted PV of approximately $884,000 over three years.** More automated tasks and simpler administration and management of the Imperva SecureSphere solution as compared to the legacy database security product can lead to productivity gains for the database security staff. Both interviewed organizations reported that they were now able to cover more database servers with less staff.
- **Audit-related cost savings estimated at a risk-adjusted PV slightly over $190,000 over three years.** Improved discovery capabilities gave the organizations the means to reduce audit scopes and save on audit costs.
- **Legacy infrastructure cost savings and avoidance estimated to a risk-adjusted PV of approximately $105,000 over three years.** The interviewed companies noted that Imperva SecureSphere has a smaller IT footprint as compared to their legacy systems. This can free up space and capacity in the data center and result in operational cost savings.

FORRESTER®

ROI
57%

Benefits PV
$3.6 million

NPV
$1.3 million

Payback
16 months

Unquantified benefit. One of the interviewed organizations experienced the following benefit, which is not quantified for this study:

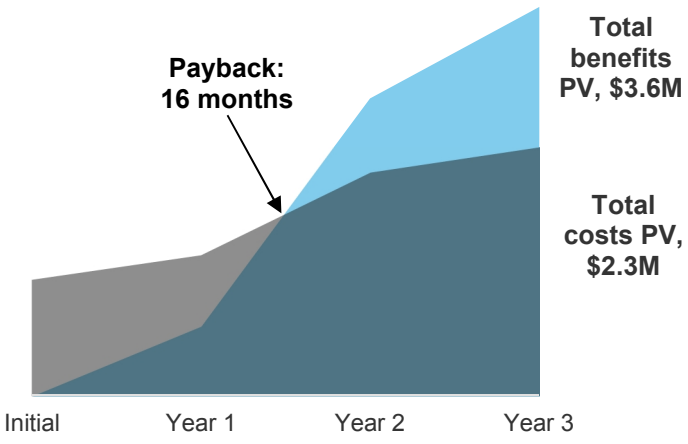
- **Reduced threat surface.** One of the interviewees, a chief information security officer at a data analytics and risk assessment company, considered that Imperva SecureSphere helped his organization to avoid data breaches. He reported: "Imperva has been an effective control to prevent lateral movement of malicious activity on our databases. Even though I don't want to give Imperva 100% credit for it, I think it probably helped us stop some data breaches."

Costs. The following risk-adjusted quantified costs are representative of those experienced by the companies interviewed:

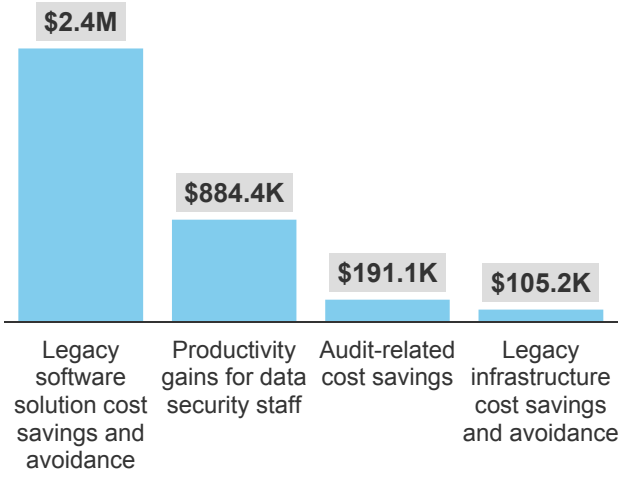
- **Software licenses and support costs of approximately $2 million.** These costs consider the approximate software license and maintenance fees for the Imperva solution over the three years of the analysis.
- **Initial setup and training costs of approximately $180,000.** These costs account for the internal efforts of the initial setup, the professional services, and training.
- **Infrastructure-related costs of approximately $44,000.** These costs include the initial hardware costs as well as the ongoing maintenance and data center facility costs for the on-premises infrastructure.

Forrester's interviews with two existing customers and subsequent financial analysis found that an organization based on these interviewed organizations experienced benefits of $3.6 million over three years versus costs of $2.3 million. This adds up to a net present value (NPV) of $1.3 million, an ROI of 57%, and a payback period of 16 months.

Financial Summary



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 Imperva SecureSphere.

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 Imperva SecureSphere 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 Imperva stakeholders and Forrester analysts to gather data relative to SecureSphere.

CUSTOMER INTERVIEWS
Interviewed two organizations using Imperva SecureSphere 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 Imperva's SecureSphere'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.

FORRESTER®

The SecureSphere Customer Journey

BEFORE AND AFTER THE SECURESPHERE INVESTMENT

Interviewed Organizations

For this study, Forrester conducted interviews with two Imperva SecureSphere customers. Interviewed customers include the following:

INDUSTRY	INTERVIEWEE	SCENARIO	NUMBER OF DATABASE SERVERS MONITORED
Global technology company	Director of IT operations	Switching from another commercial database security and monitoring solution to SecureSphere	Approximately 1,000
Data analytics and risk assessment company	Chief information security officer	Switching from another commercial database security and monitoring solution to SecureSphere	Approximately 200

Key Challenges

Prior to adopting Imperva SecureSphere, both companies were using another commercial database security and monitoring solution and had the following challenges:

- **Maintaining compliance with ever-increasing regulatory requirements.** Both companies are required to maintain and demonstrate compliance to an increasing number of data security regulations around the globe. They need to audit, monitor, and secure sensitive information stored in hundreds of different databases. Information to protect ranges from financial records and HR records to credit card information.
- **Controlling rising operational costs.** Both organizations indicated that the software maintenance and support fees that they paid for their respective legacy database security solution were too high compared to similar vendor solutions. They also reported that their legacy tools were rather difficult to maintain, configure, and administer. The consoles were not very intuitive, and many tasks were very labor-intensive, e.g. creating rules that trigger alerts or upgrading agents.
- **Expanding the scope of the databases covered in a cost-efficient manner.** Both companies wanted to expand the scope of databases monitored by their legacy database security tool but found the deployment complicated and costly to operate as it required a lot of additional IT infrastructure elements and computing power.
- **Avoiding outages.** One of the interviewees reported that, over the years, its legacy database security solution grew unstable and had caused several outages.

The organizations were looking for a new database security and monitoring tool that would allow them to:

- Maintain their security compliance to required regulations.
- Save on maintenance and support costs.
- Be more efficient in terms of administration and management of the solution.
- Scale out efficiently to protect data in further databases.

> "Our legacy database activity monitoring tool was causing us a lot of outages and was increasingly costly to maintain. That's why we started looking at alternatives and came across Imperva SecureSphere."
>
> *Chief information security officer, data analytics and risk assessment company*

FORRESTER®

The organizations looked at native auditing tools but concluded that they would take too much overhead. Native auditing tools would also introduce a conflict of interest as the logs of these tools could be manipulated by a database administrator (DBA).

After evaluating multiple vendors, the interviewed organizations chose Imperva SecureSphere and began deployment. In selecting SecureSphere, the organizations cited higher performance, better scalability, and lower costs. Both organizations started with a like-for-like migration covering the same databases that were monitored by the legacy solution. The legacy solution was then decommissioned and the scope of databases extended over the years.

> "We looked at the native auditing tools. But the problem with those native tools is that it takes a DBA to turn them on and maintain them. And that's a conflict of interest because we're trying to make sure that the DBAs are, in fact, following the rules."
>
> *Director of IT operations, global technology company*

Key Results

The interviews revealed that by switching from their legacy database security tool to Imperva SecureSphere, the interviewed organizations achieved the following results:

- **Maintenance and support cost savings due to the retirement of the legacy database security solution.** Both organizations decommissioned and removed their legacy applications and reported rather substantial cost savings. The director of IT operations stated: "We were able to buy Imperva SecureSphere, pay for the maintenance, and have a payback within two years. That is just considering the purchase and the maintenance for Imperva compared to the maintenance costs alone of our legacy solution. It was very significant savings for us."
- **Productivity gains for the database security staff.** Both interviewed organizations reported that Imperva SecureSphere is easier to administer and maintain as compared to their respective legacy database security solutions. They were not only able to reduce the size of their database security teams, but their data security staff can now also be more proactive than reactive with regards to data protection. The chief information security officer shared the following: "With our legacy system, we were so busy fighting fires — we were in a whole different mode. With Imperva and its discovery tools, we are in a place where we get more visibility on where critical data exists; we better understand how to deploy it and where to deploy it. We are getting more bang for our buck and monitor more databases with less people."
- **Reduction of audit scopes.** The chief information security officer reported that, compared to his organization's legacy solution, Imperva SecureSphere had superior discovery capabilities. The company was using these to reduce the scope of audits, which resulted in direct cost savings. He stated: "Imperva helps us to determine where critical data exists, which databases are subject to which regulation, and what controls need to be placed around those databases. It helps us to consolidate our infrastructure and save money because we can reduce the scope of audits. The savings for us are in the hundreds of thousands of dollars per year."
- **Reduced IT infrastructure spending.** Both interviewed organizations appreciated the efficiency of the Imperva SecureSphere solution and its relatively smaller IT infrastructure footprint. They reported that they can now monitor more database servers with less hardware and fewer people.

> "We just felt Imperva surpassed our legacy system's capability in terms of performance and in terms of cost. It becomes a no-brainer at that point. We are getting everything we need, including better support, and we are paying less."
>
> *Chief information security officer, data analytics and risk assessment company*

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 two 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:

- Is a large business service company with global operations and approximately 8,000 employees worldwide.
- Has a total of approximately 1,000 database servers from a variety of vendors.
- Initially monitored 300 database servers with sensitive information.
- Had an initial data security team of five IT database security specialists.
- Was using a legacy database security and monitoring tool and facing the same kind of challenges as the interviewed organizations.
- Chose to replace its legacy database security solution by Imperva SecureSphere.

Initially, SecureSphere was setup to cover the same scope of database servers. One year after the initial deployment of SecureSphere, the organization chose to extend the scope of the monitored database servers to also include highly restricted databases, increasing the number of covered database servers from 300 to 500.

Key assumptions for the composite organization

- 1,000 database servers in total
- 300 database servers monitored
- Team of five data security specialists

Financial Analysis

QUANTIFIED BENEFIT AND COST DATA AS APPLIED TO THE COMPOSITE

Total Benefits

REF.	BENEFIT	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Atr	Legacy software solution cost savings and avoidance	$361,000	$1,928,500	$598,500	$2,888,000	$2,371,645
Btr	Productivity gains for data security staff	$270,000	$405,000	$405,000	$1,080,000	$884,448
Ctr	Audit-related cost savings	$54,000	$90,000	$90,000	$234,000	$191,089
Dtr	Legacy infrastructure cost savings and avoidance	$13,300	$91,960	$22,800	$128,060	$105,221
	Total benefits (risk-adjusted)	**$698,300**	**$2,515,460**	**$1,116,300**	**$4,330,060**	**$3,552,403**

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 approximately $3.6 million.

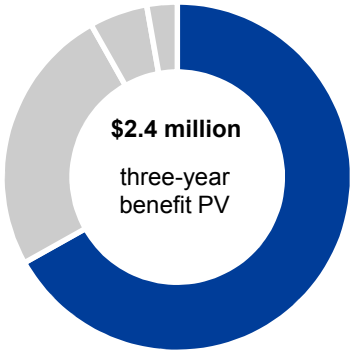
Legacy Software Solution Cost Savings And Avoidance

Both interviewed organizations had a legacy database security and monitoring tool in place for many years but reported that their respective software maintenance and support fees were too high compared to similar solutions from other vendors. One interviewee even stated that just saving the maintenance and support costs of the legacy database security solution alone paid for the whole Imperva SecureSphere product, including the maintenance.

For the composite organization, Forrester assumes:

- Annual maintenance and support cost savings of $380,000 for the initial scope of 300 database servers.
- Avoided licensing upgrade costs of $1.4 million in Year 2 to cover the extended scope of a total of 500 database servers.
- Avoided additional maintenance and support costs for the extended scope of $250,000 per year starting from Year 2 of the analysis.

Finally, Forrester adjusted this benefit down by 5% to account for uncertainty of the different cost saving estimations, resulting in a risk-adjusted total present value for this benefit of approximately $2.4 million over three years.



Legacy software solution cost savings and avoidance: 67% of total benefits

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.

Legacy Software Solution Cost Savings And Avoidance: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
A1	Software maintenance cost savings (existing scope)		$380,000	$380,000	$380,000
A2	Avoided licensing upgrade costs (extended scope)	Assumption for covering 200 more database servers		$1,400,000	
A3	Avoided software maintenance costs (extended scope)	Assumption for covering 200 more database servers		$250,000	$250,000
At	Legacy software solution cost savings and avoidance	A1+A2+A3	$380,000	$2,030,000	$630,000
	Risk adjustment	↓5%			
Atr	**Legacy software solution cost savings and avoidance (risk-adjusted)**		**$361,000**	**$1,928,500**	**$598,500**

FORRESTER®

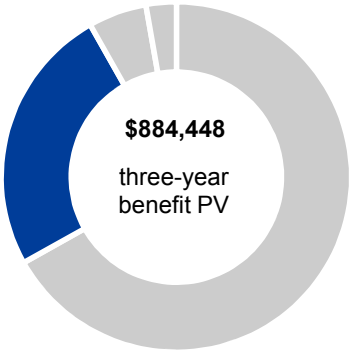
Productivity Gains For Data Security Staff

Both interviewed organizations noted that Imperva SecureSphere is easier to administer and maintain than their respective legacy database security solutions. They reported that a lot of tasks that used to be very manual and time-consuming are now automated. Data security staff now have better visibility and find it easier to manage rules, set up alerts, and upgrade agents. The organizations also reported that Imperva SecureSphere allows them to cover more database servers with less data security staff. In addition, the data security staff is now spending less time fighting fires and more time on proactively protecting the data.

For the composite organization, Forrester assumes that:

- With the legacy database security tool, the organization required approximately one full-time data security professional per 60 database servers covered.
- With Imperva SecureSphere, the organization requires approximately one full-time data security professional for every 100 database servers.
- A senior database security professional earns an average fully loaded annual salary of $150,000.

Finally, Forrester adjusted this benefit down by 10% to account for uncertainty of the productivity and salary estimations, resulting in a risk-adjusted total present value for this benefit of approximately $884,000 over three years.



Productivity gains for data security staff: 25% of total benefits

Productivity Gains For Database Security Staff: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
B1	Number of current data security professionals	Assume 1 FTE for 60 database servers	5.0	5.0	5.0
B2	Estimated number of data security professionals avoided (extension)	Assume 1 FTE for 60 database servers		3.0	3.0
B3	Number of data security professionals (with Imperva)	Assume 1 FTE for 100 database servers	3.0	5.0	5.0
B4	Average fully loaded annual salary rate (IT security)		$150,000	$150,000	$150,000
Bt	Productivity gains for data security staff	(B1+B2-B3)*B4	$300,000	$450,000	$450,000
	Risk adjustment	↓10%			
Btr	**Productivity gains for data security staff (risk-adjusted)**		**$270,000**	**$405,000**	**$405,000**

FORRESTER®

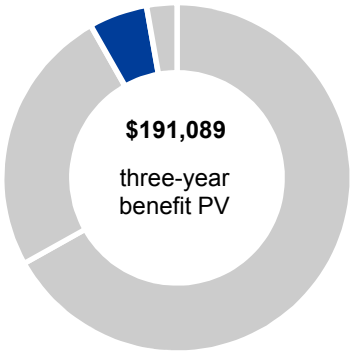
Audit-Related Cost Savings

One interviewee reported that Imperva SecureSphere provides better discovery capabilities than the organization's legacy database security tool. Imperva helps the organization to determine where critical data exists, which databases are subject to which regulation, and what controls need to be placed around those databases. It therefore also helps the company to consolidate its infrastructure, reduce the scope of audits, and, therefore, save money. For this particular company, the estimated savings were in the hundreds of thousands of dollars per year.

Based on this high-level estimation from one of the interviewees, Forrester adjusted this number to the composite organization and conservatively assumes:

- Audit cost savings of $60,000 in Year 1 with the initial scope of 300 databases.
- Audit cost savings of $100,000 in years 2 and 3 with the extended scope of 500 databases.

The extent to which an audit scope can be reduced will vary from organization to organization. Forrester therefore adjusted this benefit down by 10% to account for uncertainty of the estimated savings, resulting in a risk-adjusted total PV for this benefit of approximately $190,000 over three years.



Audit-related cost savings: 5% of total benefits

Audit-Related Cost Savings: Calculation Table

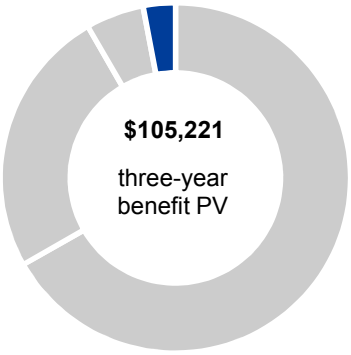
REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
Ct	Audit-related cost savings due to reduced audit scope	Assumption	$60,000	$100,000	$100,000
	Risk adjustment	↓10%			
Ctr	**Audit-related cost savings (risk-adjusted)**		**$54,000**	**$90,000**	**$90,000**

Legacy Infrastructure Cost Savings And Avoidance

Both interviewed organizations appreciated the efficiency of the Imperva SecureSphere solution and its relatively smaller IT infrastructure footprint. They reported that the Imperva solution requires fewer virtual appliances — and therefore physical servers — than their legacy solution. The retirement of the IT infrastructure that was supporting the legacy database security tool resulted in operational cost savings.

For the composite organization, Forrester assumes that:

- With the legacy solution, one virtual appliance was required for every four database servers covered.
- With the legacy solution, one physical server was required for every ten virtual appliances.
- The retirement of the IT infrastructure that was supporting the initial scope of 300 database servers resulted in data center facility and ongoing administration cost savings of $14,000 per year.
- For the extension to a total of 500 database servers in Year 2, the composite organization avoids investing in, setting up, and maintaining five additional servers.



Legacy infrastructure cost savings and avoidance: 3% of total benefits

FORRESTER®

Finally, Forrester adjusted this benefit down by 5% to account for uncertainty of the different cost saving estimations, resulting in a risk-adjusted total present value for this benefit slightly over $105,000 over three years.

Legacy Infrastructure Cost Savings And Avoidance: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
D1	Number of virtual appliances (legacy system, initial scope)	Assume 1 appliance for 4 database servers	75	75	75
D2	Number of physical servers retired (initial scope)	Assume 10 virtual appliances per physical server (rounded down)	7.0	7.0	7.0
D3	Legacy infrastructure cost savings (legacy system, initial scope)	Assume $2,000 per server per year	$14,000	$14,000	$14,000
D4	Estimated number of additional virtual appliances avoided (extension)			50	
D5	Number of additional physical servers avoided (extension)	Assume 10 virtual appliances per physical server		5	
D6	Hardware cost avoidance (extension)	Assume $10,000 per server		$50,000	
D7	Data center facility and ongoing administration cost avoidance (extension)	Assume $2,000 per server per year		$10,000	$10,000
D8	Internal labor setup costs avoided (extension)	Assume 3 hours*200 database servers*$38		$22,800	
Dt	Legacy infrastructure cost savings and avoidance	D3+D6+D7+D8	$14,000	$96,800	$24,000
	Risk adjustment	↓5%			
Dtr	**Legacy infrastructure cost savings and avoidance (risk-adjusted)**		**$13,300**	**$91,960**	**$22,800**

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 SecureSphere and later realize additional uses and business opportunities, including:

- **Further reducing the threat surface by extending the scope of database servers covered.** After having secured the most sensitive data, there is a kind of trade-off for the less sensitive data in an organization between the risk of a data breach and the costs to protect this data. By having put in place a scalable and cost-efficient database security solution, an organization might consider extending the scope to even less sensitive data and create an even more secure environment.

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.

Total Costs

REF.	COST	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Dtr	Software licenses and support costs	$900,000	$180,000	$900,000	$300,000	$2,280,000	$2,032,832
Etr	Initial setup and training costs	$133,350	$50,190	$0	$0	$183,540	$178,977
Ftr	Infrastructure-related costs	$21,000	$14,700	$6,300	$6,300	$48,300	$44,304
	Total costs (risk-adjusted)	**$1,054,350**	**$244,890**	**$906,300**	**$306,300**	**$2,511,840**	**$2,256,113**

Software Licenses And Support Costs

The software licenses and support costs for the Imperva SecureSphere solution that are indicated here are based on approximate prices paid by the interviewed organizations and then adjusted according to the number of database servers covered by the composite organization.

In our scenario, the organization started with 300 database servers and then expanded the scope to include 200 more database servers starting from Year 2 of the analysis.

The total SecureSphere license and support costs over the three years are estimated to approximately $2 million (PV) for the composite organization.

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 approximately $2.3 million.

Software Licenses And Support Costs: Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
E1	Software license costs	Assumption	$900,000	$0	$600,000	
E2	Software maintenance and support costs	Assume 20% of total licenses costs		$180,000	$300,000	$300,000
Etr	**Software licenses and support costs**	**E1+E2**	**$900,000**	**$180,000**	**$900,000**	**$300,000**

Initial Setup And Training Costs

The interviewed organizations reported that the deployment of the Imperva solution was straightforward; however, the deployment had to be carefully planned as the removal of the legacy and the installation of the new database agents required rebooting the servers.

For the deployment of the solution for the composite organization, Forrester assumes:

- Initial internal labor efforts are estimated to 1,500 man-hours for the initial deployment of SecureSphere, including the setup of the 300 database servers and the removal of the legacy solution. For the extension of 200 database servers that are rolled out at the end of Year 1, Forrester assumes that it takes another 600 man-hours.

"We turned off the legacy solution, uninstalled those agents, and got Imperva up and running in four months."

Director of IT operations, global technology company

- An average fully loaded hourly salary rate of $38 for these engineers, corresponding to a fully loaded annual salary of approximately $100,000.
- Professional service costs of $50,000 for the initial deployment and $25,000 for the extension at the end of Year 1.
- Initial training costs of $20,000.

The deployment efforts and costs will vary depending on the complexity of the database environment. Forrester therefore adjusted this cost upward by 5%, yielding a three-year risk-adjusted total PV of approximately $180,000.

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

Initial Setup And Training Costs: Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
E1	Number of internal man-hours for initial setup (including removal of legacy system)		1,500	600		
E2	Average fully loaded hourly salary rate	Rounded	$38	$38		
E3	Internal labor costs	F1*F2	$57,000	$22,800		
E4	Professional services costs		$50,000	$25,000		
E5	Training costs		$20,000			
Et	Initial setup and training costs	F3+F4+F5	$127,000	$47,800	$0	$0
	Risk adjustment	↑5%				
Etr	**Initial setup and training costs (risk-adjusted)**		**$133,350**	**$50,190**	**$0**	**$0**

Infrastructure-Related Costs

The interviewed organizations reported that the infrastructure footprint required for the Imperva SecureSphere solution was much smaller than the infrastructure required for their legacy solutions.

For the deployment of the composite organization, Forrester assumes:

- One virtual appliance for every 20 database servers.
- One physical server for every 10 virtual appliances.
- Average price of a server of $10,000 including three-year hardware maintenance.
- Data center facility and ongoing administration costs of $2,000 per server per year.

The composite organization deployed two new servers in the initial period and an additional server at the end of Year 1 to prepare for the expansion in Year 2.

To account for the uncertainties of these assumptions and cost estimations, Forrester adjusted this cost upward by 5%, yielding a three-year risk-adjusted total PV of approximately $44,000.

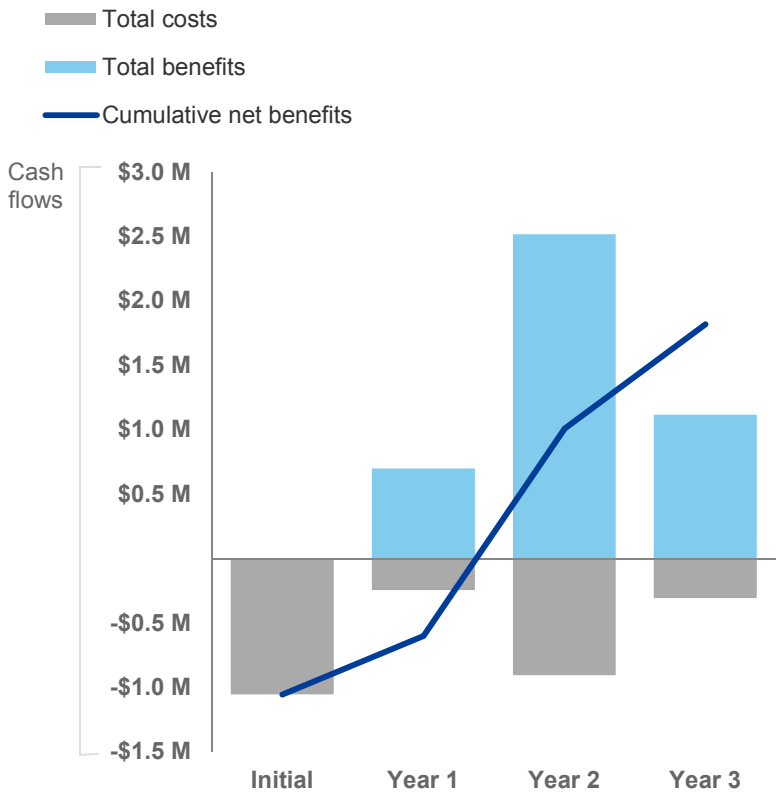
Infrastructure-Related Costs: Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
G1	Number of virtual appliances	Assume 1 virtual appliance for 20 database servers	15	10		
G2	Number of physical servers	Assume 10 virtual appliances per physical server	2	1		
G3	Average cost per physical server (incl. three-year maintenance)	Assumption	$10,000	$10,000		
G4	Hardware costs	G2*G3	$20,000	$10,000		
G5	Data center facility and ongoing administration costs	Assume 20% of total HW costs		$4,000	$6,000	$6,000
Gt	Infrastructure-related costs	G4+G5	$20,000	$14,000	$6,000	$6,000
	Risk adjustment	↑5%				
Gtr	**Infrastructure-related costs (risk-adjusted)**		**$21,000**	**$14,700**	**$6,300**	**$6,300**

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	($1,054,350)	($244,890)	($906,300)	($306,300)	($2,511,840)	($2,256,113)
Total benefits	$0	$698,300	$2,515,460	$1,116,300	$4,330,060	$3,552,403
Net benefits	($1,054,350)	$453,410	$1,609,160	$810,000	$1,818,220	$1,296,290
ROI						57%
Payback period						16 months

FORRESTER®

Imperva SecureSphere: Overview

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

Imperva SecureSphere is a comprehensive and scalable database audit and protection solution for a wide range of databases, including Oracle, Microsoft SQL Server, MySQL, Sybase, IBM DB2, IBM IMS, IBM Informix, IBM Netezza, MongoDB, PostgreSQL, Progress OpenEdge, and Teradata. It helps organizations discover and classify sensitive databases and identify excessive user rights and dormant users. The solution automates compliance tasks and can alert, quarantine, and block database attacks and unauthorized activities in real time.

Key capabilities include:

- **Flexible deployment options.** Imperva goes beyond the typical deployment scenario where agents are required on all database servers; SecureSphere supports multiple deployment methods, including a local agent, a network transparent bridge option, and a non-inline sniffer mode. By using a combination of deployment methods, the enterprise can meet a wide variety of needs without being locked into a one-size-fits-all model.
- **Cloud and big data support.** SecureSphere monitors and secures a broad range of cloud database and big data technologies, whether deployed on-premises or on infrastructure, such as Amazon AWS or Microsoft Azure. Hybrid deployment models are easily accommodated.
- **Discovery capabilities.** SecureSphere identifies databases, sensitive data, and system risks. Industry standards are utilized to create a prioritized risk score for each database. Combined with the automated data classification, organizations can accurately scope projects and prioritize risk mitigation efforts.
- **Real-time protection.** SecureSphere analyzes all database activity in real time, providing organizations with a proactive security enforcement layer and detailed audit trail that shows the “who, what, when, where, and how” of each transaction. SecureSphere addresses the compliance requirement for separation of duties and audits privileged users who directly access the database server, as well as users accessing the database through a browser, mobile, or desktop-based application. Stopping attacks in real time is the only effective way to prevent hackers from getting to your data. SecureSphere monitors all traffic for security policy violations looking for attacks on the protocol and operating system (OS) level, as well as unauthorized structured query language (SQL) activity. The highly efficient monitoring can quarantine activity pending user rights verification or block the activity — without disrupting business by disabling the entire account. Blocking is available both at the database agent and network levels, enabling the finetuning of the security profile to balance the need for absolute security with the need for maximum performance.
- **Efficient monitoring.** Even with a high volume of database traffic, SecureSphere simultaneously can monitor all traffic for security policy violations and only audit what is necessary for compliance policy purposes. The dual-channel monitoring for separate purposes allows companies to address both security and compliance requirements with a single unified solution. The efficiency also means companies can deploy monitoring that is more sophisticated and across more data sources than legacy solutions that must capture activity in audit logs before evaluation for policy violations. These legacy solutions can only monitor a fraction of the traffic before they affect performance and require additional appliances and more specialized resources to maintain the system.
- **Streamlined data compliance.** Unlike solutions that require DBA involvement and reliance on expensive professional services, SecureSphere provides the necessary management and centralization capabilities to manage thousands of databases, big data nodes, and file repositories. Predefined policies, remediation workflows, and hundreds of reports markedly reduce the need for SQL scripting and security or compliance matter expertise. Elimination of the need for ongoing DBA involvement ensures compliance with the separation of duties requirement. By utilizing the out-of-the-box process APIs, management console, workflows, reports, and analysis tools, existing personnel can deploy and manage the system.

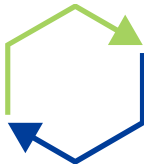
Appendix A: Total Economic Impact

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] Imperva SecureSphere is a comprehensive and scalable database audit and protection solution. It provides real-time monitoring, protection, and auditing capabilities for a wide range of databases. For more details about SecureSphere and its key capabilities, please refer to page 16.