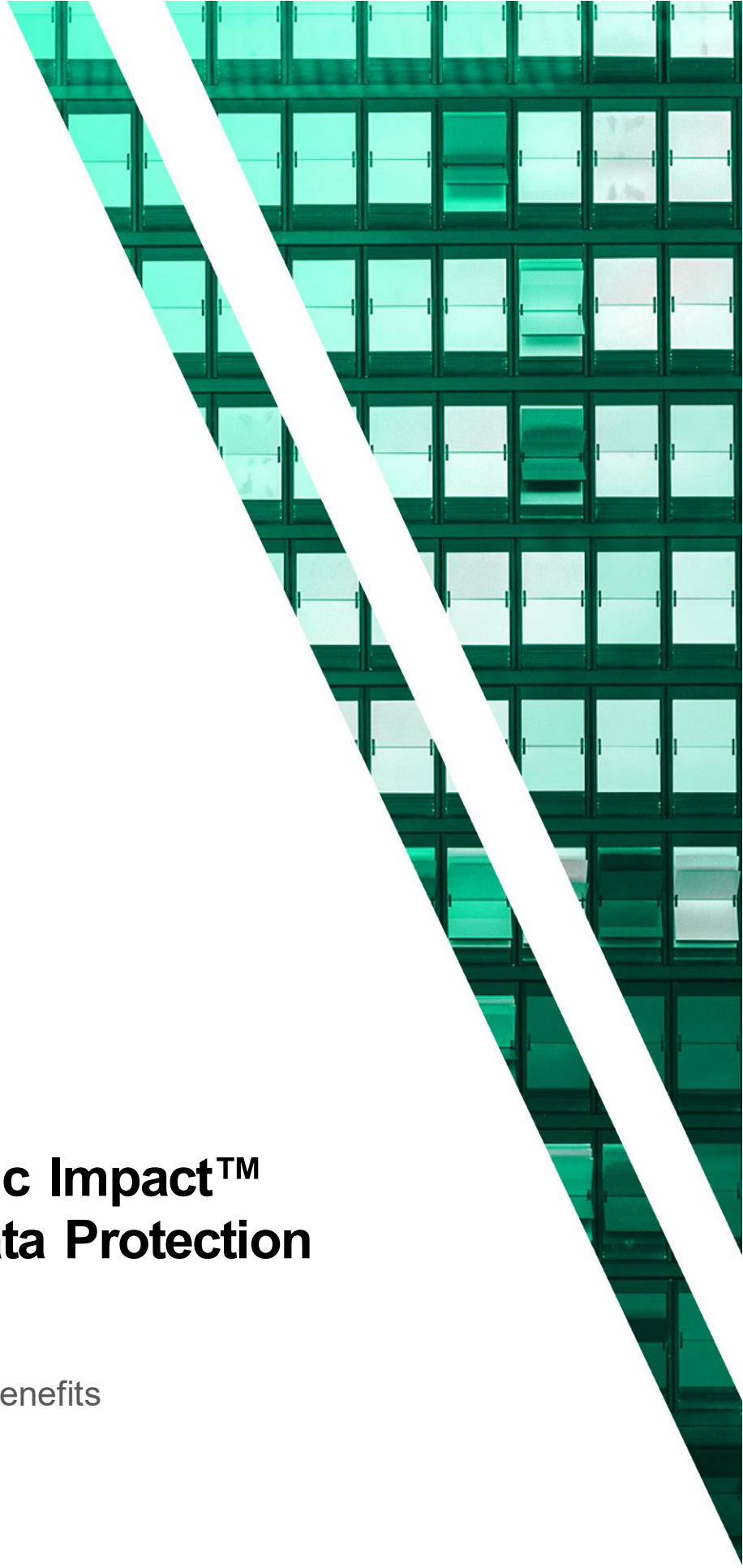
FORRESTER®



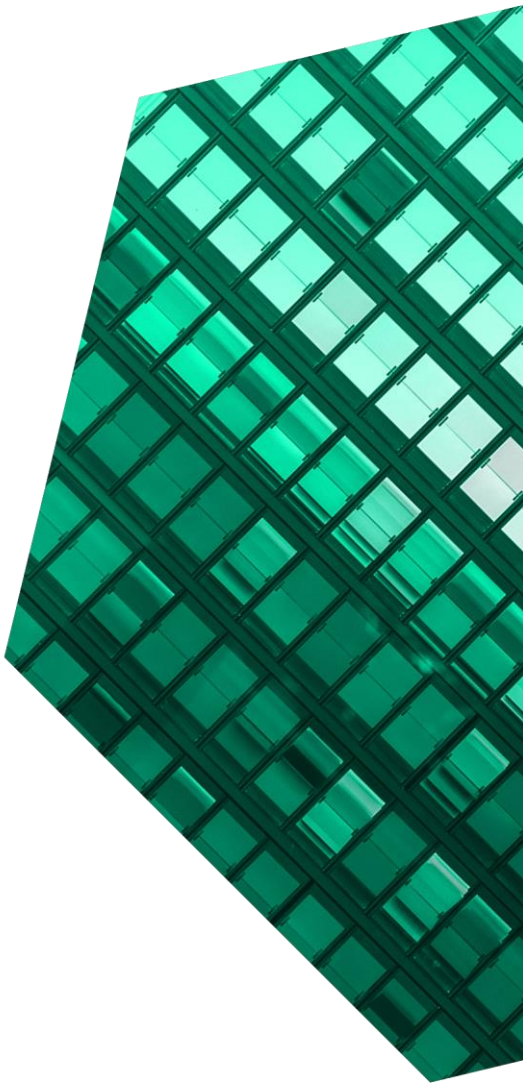
The Total Economic Impact™ Of The Imperva Data Protection Solution

Cost Savings And Business Benefits Enabled By Imperva

OCTOBER 2021

Table Of Contents

Consultant: *Rachel Ballard*



ABOUT FORRESTER CONSULTING

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

Executive Summary

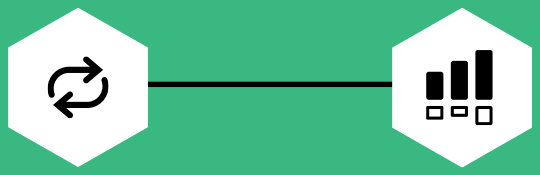
As today's enterprises become increasingly dispersed and dynamic, the technology that protects and powers their data must be scalable and agile. Beyond protection, a solution needs to have the capacity to store, retrieve, and analyze ever-increasing quantities of information, while complementing other necessary tools in an organization's data management arsenal. Imperva delivers a multi-layer data protection and threat defense system while providing potent analytic capabilities.

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 Imperva Sonar for Data Protection. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Imperva on their organizations.

Imperva Sonar for Data Protection is a database monitoring and security management solution that protects data by continuously analyzing the access behaviors of users, processes, and applications.[1] Risks to sensitive data are efficiently identified and remedied, minimizing the time and resources traditionally needed to investigate suspicious events and policy violations. The practical analytic capabilities simplify the database audit processes and allow organizations to maintain necessary compliance with industry regulators as well as other stakeholders. With notable compression rates and noise reduction, Imperva can process large quantities of log data in less time and store it for longer durations for security and compliance investigations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed five decision-makers with experience using Imperva to augment their existing database activity monitoring (DAM) and security incident and event management (SIEM) solutions. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization.

KEY STATISTICS



Return on investment (ROI)
152%

Net present value (NPV)
$4.05M

Prior to using Imperva, the customers relied on a combination of native logging, DAM, and SIEM solutions. Data protection through these solutions was not as efficient and comprehensive as the customers' organizations required, and audit data retention periods did not meet regulatory requirements. Reporting and incident analysis and resolution were cumbersome processes, making it difficult to access information that was necessary to a proactive line of analytics, compliance, and defense.

With Imperva deployed, the customers can efficiently manage a multi–data center environment across on-premises and cloud data repositories on a single platform with significantly reduced query times, multi-year audit data retention, and greater protection of sensitive data leading to improved internal and external outcomes.

Imperva has their web application firewall [WAF], runtime application, self-protection [RASP], and DAM all integrated in the data tracking which allows us to see what is happening at both the web and application level. It's embedded in the query, and then we see that information displayed within Imperva when we look at database activity monitoring events. There are no other products that do this — there just aren't. With Imperva's entire solution, we can stitch the three tiers together and paint the picture.

— Data security manager, financial services

KEY FINDINGS

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

- **Security and compliance staff time saved.** With its centralized console and streamlined data management and retrieval processes, Imperva enables the user to investigate, research, and resolve data protection events in near real time. The data security and compliance teams can quickly and interactively produce meaningful activity reports in order to efficiently track and resolve policy violations and facilitate internal and external audits. The efficiencies gained in resolving data protection events total $1.3 million per year, generating a three-year, risk-adjusted PV of $2.9 million.
- **Reduction of infrastructure and storage costs.** Imperva allows its users to reduce their infrastructure footprint through the elimination of legacy servers while simultaneously eliminating archive requirements by gaining multi-year access to live audit data. The composite organization eliminates 25 servers in Year 1, 70

servers in Year 2, and 100 servers in Year 3 at a cost savings of $12,000 per server. The resulting three-year, risk-adjusted PV savings is nearly $1.7 million.

Security and compliance staff time saved:

$2.9 million

- **Reduction of SIEM costs.** Through automation and advanced preprocessing of information, Imperva allows data teams to efficiently monitor, search, detect, and manage security and compliance incidents. Interviewees noted that with Imperva, they have greater visibility into all business unit data activity to which they can respond more quickly and with fewer SIEM resources. The reduction of SIEM license costs saves an organization $600,000 per year, resulting in a three-year, risk-adjusted PV of nearly $1.4 million.
- **Reassignment of FTE resources.** With Imperva's robust toolset for reporting, analytics, orchestration, and automation, the database security and compliance teams are able to accomplish more in less time, allowing for the reassignment of 2.5 team members to more strategic roles and projects within the organization. This reallocation of resources results in a three-year, risk-adjusted value of almost $722,000.

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

- **Increased long-term data retention.** Imperva allows organizations to store data without the need for aggregators, enabling them to retain and access relevant data for longer periods of time and eliminating the need to archive historical data to meet regulatory protocols, which can be costly and difficult to access.
- **Improved compliance and security outcomes.** With better understanding of exactly who is accessing data, organizations can compare configuration management database (CMDB) information to the production database servers and audit for anomalies impacting personal information (PII), personal health information (PHI), and other data. With enhanced information, teams can determine the extent of their current coverage, access permissions and data redundancies, and refine their security strategies in a timely manner, leading to better compliance and audit outcomes and fewer fines and penalties.
- **Increased visibility and reduced risk of data loss.** Imperva provides greater insight into activities occurring, whether by users or entities, in an organization's database environments. Defining who is using what company data through access permissions allows organizations to develop more effective strategies for preventing policy violations and minimizing potential exposures. Additionally, Imperva integrates the monitoring function with its upstream blocking capabilities, including RASP and WAF, reducing the risk of data loss.
- **Improved employee experience.** Imperva Sonar for Data Protection has centralized analytics, automation, and orchestration capabilities that allow the data security and compliance team to accomplish more in less time. Employees are, therefore, doing fewer manual tasks and more strategic work, both

enhancing their personal job experience as well as offering the company higher-value output.

- **Enhanced collaboration.** Imperva's streamlined processes make collaboration with both internal stakeholders and external business partners more efficient and effective. For example, one interviewee mentioned that their organization's data security and compliance team is working more closely with the extended cybersecurity department as the tool's advanced analytics become more relevant to the company's overall security posture and strategy.

Costs. Risk-adjusted PV costs include:

- **Total licensing costs.** The composite organization incurs a license fee of $800 per server in Year 1, $1,050 in Year 2, and $1,300 in Year 3. With 938 servers, the total annual licensing costs result in a three-year, risk-adjusted PV of $2.4 million.
- **Initial and ongoing costs.** Initial costs include internal FTE hours required for implementation, new hardware, and professional services. Ongoing costs include internal FTE hours required to maintain the solution and the Imperva relationship, as well as recurring professional services fees. The three-year, risk-adjusted PV of initial and ongoing costs total $263,000.

The customer interviews and financial analysis found that a composite organization experiences benefits of $6.73 million over three years versus costs of $2.68 million, adding up to a net present value (NPV) of $4.05 million and an ROI of 152%.

Reduction of infrastructure and storage costs:

$1.7 million

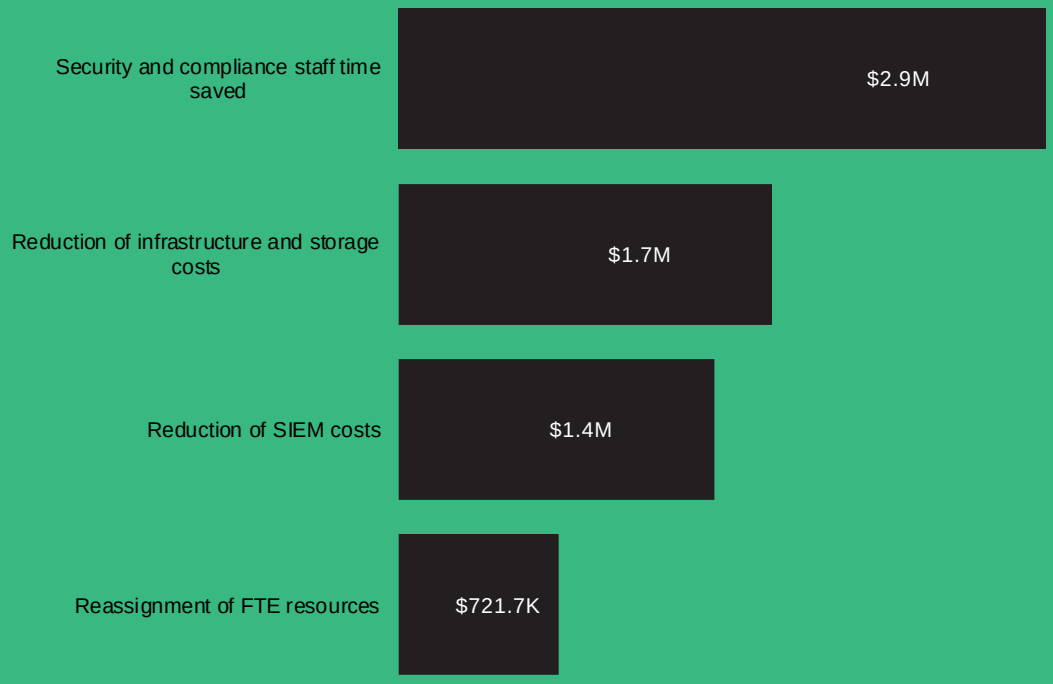
ROI
152%

BENEFITS PV
$6.73M

NPV
$4.05M

PAYBACK
<6 months

Benefits (Three-Year)



A cybersecurity engineer commented, "We increased our audit data retention from one week to five and a half years which significantly improved our regulatory compliance and audit results."

TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in Imperva.

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 can have on an organization.

DUE DILIGENCE

Interviewed Imperva stakeholders and Forrester analysts to gather data relative to the database security solution.

DECISION-MAKER INTERVIEWS

Interviewed five decision-makers at organizations using Imperva to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewees' 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 decision-makers.

CASE STUDY

Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

The Imperva Customer Journey

Drivers leading to the Imperva investment

Interviewed Decision-Makers

Interviewee	Industry	Organization description
Cybersecurity engineer	Financial services	Operates 780 branches
Data security architect	Insurance	Over 2,000 employees
Data protection team manager	Insurance	Fortune 500 investment and insurance provider
Lead, access management team	Insurance	Over 13 million policies in force
Data security manager	Financial services	Over $20 billion in annual revenue

KEY CHALLENGES

The interviewees' organizations previously managed their database monitoring and protection activities with a combination of solutions. This not only required excessive storage capacity, but it also meant they lacked sufficient, centralized access, analysis, visibility, and the agility to quickly identify and resolve data protection events. Interviewees noted that their organizations sought expanded coverage of data activity monitoring in cloud-based environments, i.e., database as a service (DBaaS), platform as a service (PaaS), etc., that also offered a hybrid on-premises option. They also looked to simplify their data protection protocols and permissions, reduce data redundancies, and improve compliance and audit results.

The interviewees struggled with common challenges, including:

- **Need for improved data protection.** The increasing amount of data brings with it the responsibility to make sure that protection against a wide variety of possible violations and breaches is adequate. In their legacy environments, the interviewees' organizations were unable to triage the growing amount of data access behaviors through anomaly detection, data classification, data entitlements, and vulnerability assessment.
- **Lack of readily available and constructive analytics.** The interviewees' organizations lacked the capacity to easily access historical data and view data access activity. This visibility would allow them to accurately assess their data security postures and fulfill regulatory requirements. Without quick access to accurate analytics, the organizations faced lengthy incident investigations, unresolved requests, and

> **"The level of detail that we are getting with Imperva is a vast improvement over our legacy environment. We were always covering all of our databases, but now we are able to review, follow up, and identify risks much faster."**
> *Data security architect, insurance*

inefficient auditing processes, often followed by penalties and fines.

- **Increasing costly licensing and storage needs.** While having to process a rapidly growing and daily inflow of log data, the interviewees' organizations faced increasingly expensive storage and licensing needs that collected, aggregated, and housed difficult-to-access and sometimes redundant data. They sought a platform that would offer an improved compression rate, allow for longer audit data retention periods, and eliminate costly storage fees and appliance requirements.

"Accessing data has decreased literally from days to seconds. Previously, we would start a query on a Monday morning, and hopefully by Tuesday night, it would finish. Being able to handle a multi–data center environment drastically reduced our query times."
Access management team lead, insurance

SOLUTION REQUIREMENTS/INVESTMENT OBJECTIVES

The interviewees' organizations searched for a solution that could:

- Allow their teams to efficiently assess, prioritize, and remediate risks and vulnerabilities through efficient database security management.
- Provide safe, accessible audit data for current needs as well as offer the ability to grow at a reasonable cost.
- Operate as a cloud-native or hybrid solution that integrates with other database protection tools.

COMPOSITE ORGANIZATION

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

- A financial services enterprise.
- Operations include the management of a large quantity of sensitive data, as well as meeting regulatory requirements.

Key assumptions

- **Financial organization**
- **40 data protection events per week**
- **Two days saved per data protection event**
- **Internal resource efficiencies realized after deployment**

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits

Ref.	Benefit	Year 1	Year 2	Year 3	Total	Present Value
Atr	Security and compliance staff time saved	$1,170,000	$1,170,000	$1,170,000	$3,510,000	$2,909,617
Btr	Reduction of infrastructure and data storage costs	$270,000	$756,000	$1,080,000	$2,106,000	$1,681,668
Ctr	Reduction of SIEM costs	$570,000	$570,000	$570,000	$1,710,000	$1,417,506
Dtr	Reassignment of FTE resources	$290,225	$290,225	$290,225	$870,675	$721,747
	Total benefits (risk-adjusted)	$2,300,225	$2,786,225	$3,110,225	$8,196,675	$6,730,538

SECURITY AND COMPLIANCE STAFF TIME SAVED

Evidence and data. The interviewees revealed the following about their organizations' use of Imperva:

- Before deploying Imperva, teams spent time manually loading archive files, identifying and resolving events, and composing reports of event details**.** Each of these processes could take several days. The cybersecurity engineer said: "With Imperva, our turnaround time has gone from a week to just minutes. Everything is readily accessible, either through Imperva directly or through an integrated solution working with Imperva."
- Imperva provided analytics that allow data security and compliance teams to see and mitigate anomalies in a proactive manner. Data is easily accessible, and reports are comprehensive, enabling teams to more efficiently assess data protection events. A data security manager commented: "With better analytics, account misuse is identified right away. I know who, when, and where the suspicious activity happens."
- Contributing to the efficiencies gained, Imperva allows customization and storage of queries to streamline routine data security maintenance. A data protection team manager said: "With Imperva, we are able to store previous query runs and customize reporting to focus on the delta from one run to the next. So, instead of spending a week or two every quarter, our resource is doing higher-value work. They are actually running the classification scans."

Modeling and assumptions. For the financial analysis, Forrester assumes that:

- The composite organization experiences 40 data protection events per week.
- Two days are saved per event.
- The fully loaded annual salary for a database analyst is $81,250.

Risks. The administration time saved will vary with:

- The frequency and size of data protection events and policy violations.
- The salary level of database analysts, depending on skill level and geographical location.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $2,909,617.

Security And Compliance Staff Time Saved					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Time saved managing data protection	Two days	2	2	2
A2	Number of data protection events requiring research and resolution	40 violations per week* 52 weeks	2,080	2,080	2,080
A3	Fully loaded annual security and compliance analyst salary	Assumption	$81,250	$81,250	$81,250
At	Security and compliance staff time saved	(A1/260)*A2* A3	$1,300,000	$1,300,000	$1,300,000
	Risk adjustment	↓10%			
Atr	Security and compliance staff time saved (risk-adjusted)		$1,170,000	$1,170,000	$1,170,000
	Three-year total: $3,510,000		**Three-year present value: $2,909,617**		

REDUCTION OF INFRASTRUCTURE AND STORAGE COSTS

Evidence and data. The interviewees revealed the following about their organizations' use of Imperva:

- By eliminating the need for aggregators that combine data from multiple sources into a more meaningful entity, Imperva reduced the need to store archive files with historical log data. The information needed for compliance reporting and auditing is gathered and compiled automatically, thereby saving organizations from having to store excess and redundant information for extended time periods. A data security manager noted: "With the introduction of Imperva, we're able to reduce the disk requirement because the data is not there anymore. We are reducing the number of management servers that we need."
- Imperva allowed the organizations to retain just the necessary, higher-quality data and isolate extraneous, redundant information. A data security manager reported: "Imperva allows for amazing data compression and retention. It looks at the database activity in more detail and stores what we need for compliance, reports, internal and external audits, data classification, and discovery."

Modeling and assumptions. For the financial analysis, Forrester assumes that:

- The composite organization eliminates 25 servers in Year 1, 70 servers in Year 2, and 100 servers in Year 3.
- The infrastructure and storage cost per server equals $12,000.

Cost reduction per server:

$12,000

Risks. Improved infrastructure and data storage efficiencies will vary with:

- The number of legacy servers.
- The quantity of data processed by the organization.
- Regulatory compliance and audit requirements.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $1,681,668.

Reduction Of Infrastructure And Storage Costs

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Number of legacy servers eliminated	Composite	25	70	100
B2	Infrastructure and data storage cost per server	Composite	$12,000	$12,000	$12,000
Bt	Reduction of infrastructure and storage costs	B1*B2	$300,000	$840,000	$1,200,000
	Risk adjustment	↓10%			
Btr	Reduction of infrastructure and storage costs (risk-adjusted)		$270,000	$756,000	$1,080,000
	Three-year total: $2,106,000			**Three-year present value: $1,681,668**	

REDUCTION OF SIEM COSTS

Evidence and data. The interviewees revealed the following about their organizations' use of Imperva:

- Organizations looked to complement their SIEM with a database security management platform.
- Imperva enabled organizations to optimize their SIEM investments for improved security visibility and data management while reducing costs.
- Through both the preprocessing of database log activity and the consolidation of capabilities into a single console, organizations eliminated 40% of their SIEM license costs and pushed the most relevant data into their SIEM for further investigation.

Modeling and assumptions. For the financial analysis, Forrester assumes that:

- The legacy SIEM costs totaled $1.5 million per year.

"With the Imperva solution, we have a good compression rate [and] a good cost. In addition to being able to ingest and store, we get anomaly detections, vulnerability assessments, data enrichment, and integration with our other products."

Data security manager, financial services

- Interviewees' organizations saved 40% of SIEM licensing costs.

Risks. The reduction of SIEM costs will vary with:

- An organization's specific security strategy and needs.
- The amount and nature of incoming data, including adopting broader security policies.
- An organization's legacy license costs.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1,417,506.

Reduction Of SIEM Costs

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Reduction in SIEM costs	Assumption	$1,500,000	$1,500,000	$1,500,000
C2	Percent reduction in SIEM costs	Assumption	40%	40%	40%
Ct	Reduction of SIEM costs	C1*C2	$600,000	$600,000	$600,000
	Risk adjustment	↓5%			
Ctr	Reduction of SIEM costs (risk-adjusted)		$570,000	$570,000	$570,000
	Three-year total: $1,710,000		**Three-year present value: $1,417,506**		

REASSIGNMENT OF FTE RESOURCES

Evidence and data. The interviewees revealed the following about their organizations' use of Imperva:

- From lacking both automation and a centralized platform, data security and compliance teams performed most tasks manually using multiple solutions.
- With the automation provided by Imperva, research, forensics, and reporting tasks are accomplished at a fraction of the time, enabling teams to reassign their resources. A data security manager noted: "Our data classification and discovery used to require four to five people. Since implementing Imperva, I am able to do it by myself." They added: "The automation is making my job a lot easier. I am continuously able to free up more time."

Modeling and assumptions. For the financial analysis, Forrester assumes that:

- The composite organization reassigns 2.5 data security and compliance analysts. Data security and compliance analyst earns a fully loaded annual salary of $122,200.

Risks. The reassignment of security and compliance resources to higher-level tasks will vary with:

"We have Imperva matching a lot of activity for ticket approval. That has been a big lift in terms of economic impact to the team. I was actually able to reduce my offshore resource overhead by doing that."

Data protection team manager, insurance

- The size of the organization and the quantity of data processed and monitored.
- The salary level of a data security and compliance analyst, depending on skill level and geographical location.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $721,747.

Reassignment Of FTE Resources

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Number of security and compliance staff reassigned	Interview	2.5	2.5	2.5
D2	Fully loaded salary of a security and compliance analyst	Assumption	$122,200	$122,200	$122,200
Dt	Reassignment of FTE resources	D1*D2	$305,500	$305,500	$305,500
	Risk adjustment	↓5%			
Dtr	Reassignment of FTE resources (risk-adjusted)		$290,225	$290,225	$290,225
	Three-year total: $870,675		**Three-year present value: $721,747**		

UNQUANTIFIED BENEFITS

Additional benefits that customers experienced but were not able to quantify include:

- **Increased long-term data retention.** Interviewees reported that their legacy environments did not allow for the long-term storage of audit data that is necessary to meet compliance and regulatory requirements. Imperva's pre-analytic filtering allows organizations to minimize the quantity of information that needs to be retained. The favorable compression rates enable more information to be stored with less hardware. A data security architect mentioned: "In our legacy environment, I could keep three months of data at most. Now, I am keeping three and one-half years and still have room on my original purchase."
- **Improved compliance and security outcomes.** Users report increased control and ease of monitoring after deploying Imperva. A data security architect said: "Imperva offers us enriched data so that we can quickly find the fallout. That has closed a big audit gap for us." Additionally, users can import data from other solutions and create reports to show coverage and vulnerabilities. A data protection manager noted, "With Imperva, we can import various data feeds together in order to run reports and create dashboards to show our executive leaders."
- **Increased visibility and reduced risk of data loss.** The analytic capabilities of Imperva help prevent costly data violations by giving security and compliance managers complete and focused insights on data activity throughout their organization. A data security manager mentioned: "In the end, Imperva helps to stop a threat in its tracks before it gets all the way to the data. There are millions of what would be considered attack-type events per day on our web applications. If any one of those manages to get through and get all the way to the data, then that's a disaster."

- **Improved employee experience.** Data security and compliance teams perform more efficiently with Imperva's consolidated, automated toolset, leading to an improved employee experience. A data protection team manager commented: "Our team is doing less manual work and doing higher-value work. It's a true lift to the program and the organization, and our employees are happier for it."
- **Enhanced collaboration.** Imperva's advanced data monitoring and security management capabilities encourage collaboration across departments within the organization and provide seamless integration with various complementary solutions. A data security manager stated: "We've seen tighter integration with our partners and our security architecture department. We're interacting with them in all facets of our data protection program. Imperva fosters that type of collaboration, and we expect that to continue and grow."

FLEXIBILITY

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

- **Customization of security procedures.** Imperva's flexible, cloud-native structure allows the user to continuously update and enhance security features. A data security architect noted: "Imperva allows us to not only import, but enrich data collected. We are now developing a real-time alerting mechanism that will allow us to catch outlier behavior before it's too late." A data protection team manager added: "We were able to build out the workflow process to allow platform access to other departments, such as internal auditors and database administrators [DBAs]. They can't change anything, but they can look at it and run reports on their own, adding efficiencies to my team. This has been very helpful, a side benefit that we were not intending."
- **Cloud-supported scalability.** As organizations continue to grow, their corresponding data loads also increase. Imperva accommodates this growth and enables continuity without the need for installing an agent. A data protection manager noted, "We're looking at using Imperva to manage our steadily increasing data load because of the ability to go agentless," and added, "Since we can scale with the cloud, we can start to push data across the organization, so any application user can do their own investigation, thereby streamlining the queries that do not require a higher-level security response."

"With Imperva, we see data right away. Before, we could see it, but we would have to go to multiple locations. Now everything is in one place. Information retrieval has gone from a few days to a few hours. In addition, the automation process in Imperva shows us all the information for any individual in one report instead of us having to pull everything together. Now I can actually collate that information in a few minutes."
Data security architect, insurance

- **Elimination of outsourced resources.** A data security manager commented: "With Imperva, we can do data classification on our own, while doing all other data security tasks as well. The one product does the classification, discovery, and the reporting. I know other companies are outsourcing these tasks, and it is taking them much longer than us."

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

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Etr	Total licensing costs	$0	$750,400	$984,900	$1,219,400	$2,954,700	$2,412,302
Ftr	Initial and ongoing costs	$179,463	$33,684	$33,684	$33,684	$280,515	$263,230
	Total costs (risk-adjusted)	$179,463	$784,084	$1,018,584	$1,253,084	$3,235,215	$2,675,532

TOTAL LICENSING COSTS

Evidence and data. The interviewees revealed the following about their organizations' use of Imperva:

- The annual licensing fee per server is $800 in Year 1, $1,050 in Year 2, and $1,300 in Year 3. The increase is based on Imperva's enterprise pricing structure, which accounts for organizations displacing their legacy systems.
- The composite organization monitors and manages 938 servers.

Results. Given Imperva's straightforward pricing structure, Forrester did not risk-adjust this cost, which yielded a three-year, risk-adjusted total PV (discounted at 10%) of $2,412,302.

Total Licensing Costs						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Cost per server	Composite		$800	$1,050	$1,300
E2	Number of servers	Composite		938	938	938
Et	Total licensing costs	E1*E2	$0	$750,400	$984,900	$1,219,400
	Risk adjustment	0%				
Etr	Total licensing costs (risk-adjusted)		$0	$750,400	$984,900	$1,219,400
	Three-year total: $2,954,700			**Three-year present value: $2,412,302**		

INITIAL AND ONGOING COSTS

Evidence and data. The interviewees revealed the following about their organizations' use of Imperva:

- Initial implementation required internal labor of up to four security engineers to set up and configure the new platform.
- New servers were necessary to support the deployment of the Imperva solution.
- The composite organization hired a third-party professional services provider for the automation buildout and to assist with the ongoing management of the solution.
- Ongoing management required a commitment of 10 hours per month performed by an internal security engineer.

Modeling and assumptions. For the financial analysis, Forrester assumes that:

- Implementation requires 50% of the time of four security engineers for 2.5 months at a fully loaded annual salary of $122,200.
- Two new servers are needed to support Imperva, at a cost of $30,000 each.
- Professional services, handling cloud and on-premises infrastructure changes, include 240 hours at $250 per hour for the initial implementation. The ongoing professional services fees are $25,000 per year.
- Ongoing internal management involves 10 hours per month of one security engineer at $59 per hour.

Risks. Initial and ongoing costs will vary with:

- The complexity of the database environment being protected and managed.
- The skill level and experience of the security and compliance team.
- Salary levels, depending on skillset and geographical location.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $263,230.

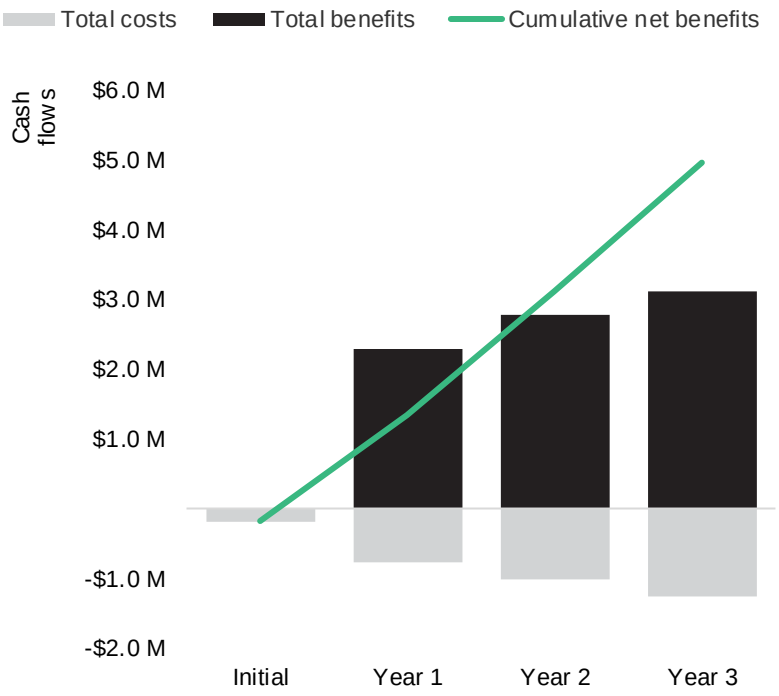
Initial And Ongoing Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Internal implementation labor costs	(2.5 months/12 months)*4 security engineers* $122,200 salary*50% time	$50,917			
F2	New hardware required	2 servers*$30,000 per server	$60,000			
F3	Initial professional services	240 hours*$250 per hour	$60,000			
F4	Ongoing management	10 hours per month*12 months*1 security engineer *$59 per hour		$7,080	$7,080	$7,080
F5	Ongoing professional services	Assumption		$25,000	$25,000	$25,000
Ft	Initial and ongoing costs	F1+F2+F3+ F4+F5	$170,917	$32,080	$32,080	$32,080
	Risk adjustment	↑5%				
Ftr	Initial and ongoing costs (risk-adjusted)		$179,463	$33,684	$33,684	$33,684
	Three-year total: $280,515		**Three-year present value: $263,230**			

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI, NPV, and payback period values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($179,463)	($784,084)	($1,018,584)	($1,253,084)	($3,235,215)	($2,675,532)
Total benefits	$0	$2,300,225	$2,786,225	$3,110,225	$8,196,675	$6,730,538
Net benefits	($179,463)	$1,516,141	$1,767,641	$1,857,141	$4,961,461	$4,055,006
ROI						152%
Payback						<6 months

Appendix A: Total Economic Impact

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

TOTAL ECONOMIC IMPACT APPROACH

Benefits represent the value delivered to the business by the product. The TEI methodology places equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization.

Costs consider all expenses necessary to deliver the proposed value, or benefits, of the product. The cost category within TEI captures incremental costs over the existing environment for ongoing costs associated with the solution.

Flexibility represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. Having the ability to capture that benefit has a PV that can be estimated.

Risks measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

PRESENT VALUE (PV)

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

NET PRESENT VALUE (NPV)

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

RETURN ON INVESTMENT (ROI)

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

DISCOUNT RATE

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

PAYBACK PERIOD

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

Appendix B: Endnotes

[1] Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.


FORRESTER®