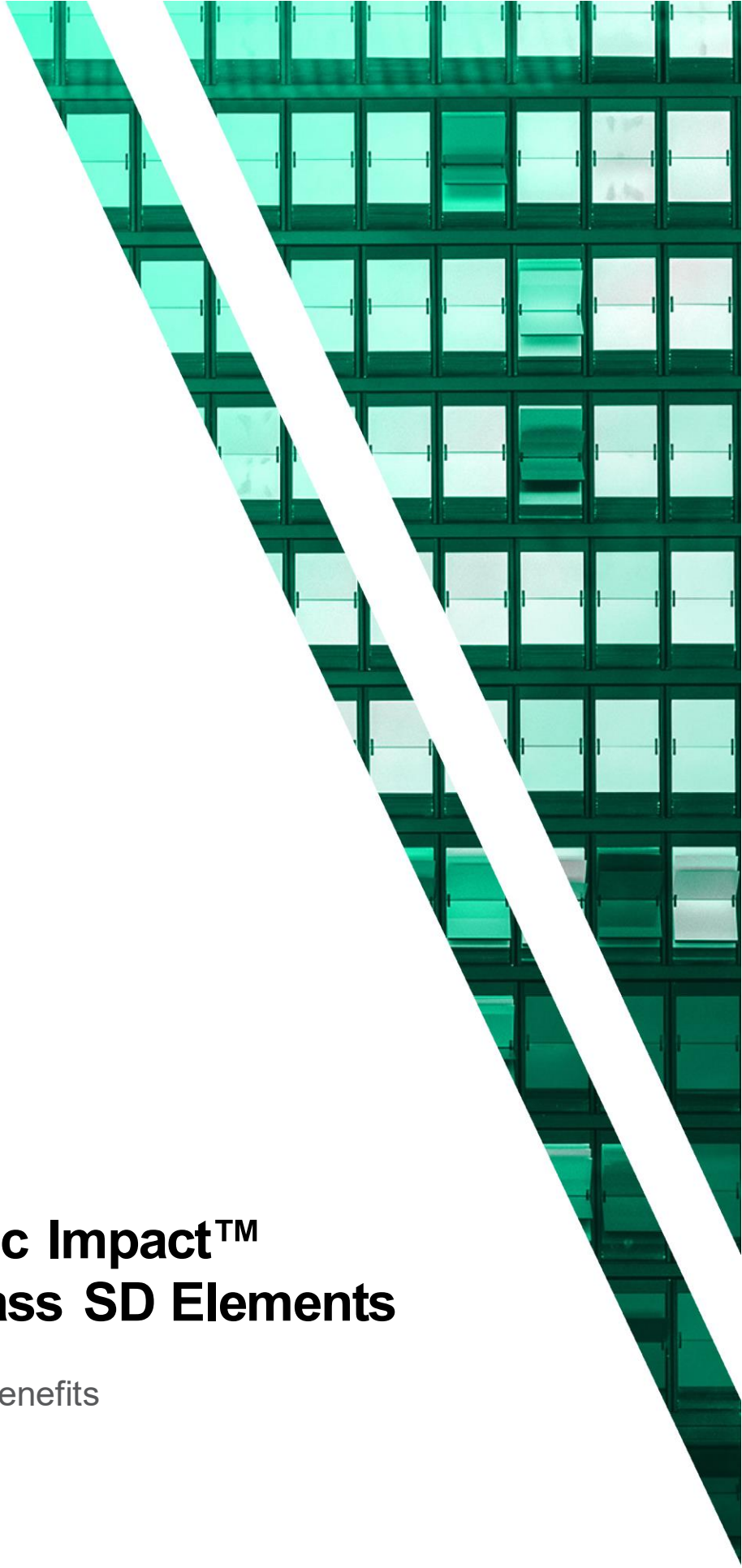
FORRESTER®



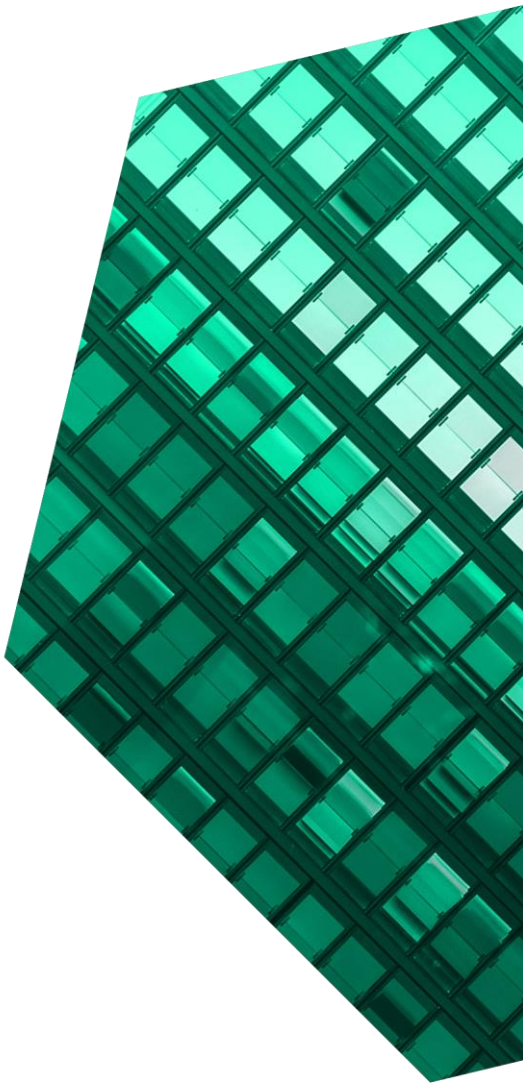
The Total Economic Impact™ Of Security Compass SD Elements

Cost Savings And Business Benefits Enabled By SD Elements

APRIL 2022

Table Of Contents

Consulting Team: Roger Nauth



Executive Summary

Development, security, and operations (DevSecOps) helps DevOps and agile teams increase speed-to-market by ensuring that fast and frequent deployments to production are secure by design. Teams need to shift security left in the software development cycle and identify compliance and regulatory standards, security requirements, and company policies that apply to applications before they are written. Automation saves time and money, enabling organizations to deliver secure code customers can rely on and trust.

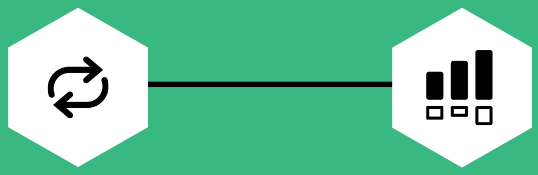
Security Compass is a leading provider of secure software development and developer-centric threat modeling solutions that enable organizations to build secure software faster. SD Elements helps software development teams continuously model software threats at scale, and then write code that significantly reduces cyber risk and remediation costs. SD Elements integrates security from the beginning of the development process and enables consistent, scalable secure coding and threat modeling across an entire software portfolio.

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

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four decision-makers with direct experience using SD Elements. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization.

Prior to using SD Elements, interviewees noted how their organizations used archaic, manually entered spreadsheets to create, track, and update security requirements, which often overlooked critical requirements, limited security control status visibility, and, most frustratingly, made it necessary to rewrite code. They lacked an automated solution that integrated security into the beginning of the development process. After the investment in SD Elements, the interviewees experienced a reduction in critical vulnerabilities and improved developer productivity.

KEY STATISTICS



Return on investment (ROI)
332%

Net present value (NPV)
$2.20M

KEY FINDINGS

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

- **Avoided vulnerability remediation, worth $396,000 over three years.** SD Elements allowed interviewees' organizations avoid material time in remediating application vulnerabilities. This included the time to investigate and validate vulnerabilities, as well as the actual remediation of vulnerabilities including testing fixes and reviewing fixes with development leads and security architects.

- **Reduced costs due to automation of manual security requirement tasks, worth $739,000 over three years.** Prior to implementing SD Elements, security architects had to understand requirements, utilize manual solutions such as spreadsheets, and provide training for security champions. For in-flight applications, security organizations had to review with the development teams where policies impacted their workflow, among other time-consuming steps.

"There are no other vendors providing a solution like this."
— Vice president and chief information security officer, IT and services for transportation and defense

- **Increased productivity due to reduction in product security requirements development time, worth $1.7 million over three years.** Interviewees noted their organizations' productivity increased significantly because of the solution, decreasing the time to develop security requirements for products by 90%. Prior to the implementation of SD Elements, multiple meetings and discussions were required to understand which requirements were applicable for a new product.
- **Decreased time spent on compliance certifications, worth $67,000 over three years.** Interviewees reported SD Elements decreased the time required to generate reports for auditing agencies. With the solution, it was easy to dive into the details and see what requirements were implemented. SD Elements enabled decision-makers to understand their application portfolio, including which products should be prioritized for certification in the near term and the future.

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

- **Increased ability to drive customers' speed-to-market.** Although the study did not capture quantified benefits related to speed-to-market, interviewees noted that SD Elements played a large role in their organizations increasing their ability to accelerate the secure development of their applications and solutions to meet market requirements.
- **Improved development team capabilities to focus on core responsibilities.** SD Elements enabled developers to utilize the solution's training library, allowing them to focus on value-added and critical priority tasks and quickly learn about specific and relevant security requirements.
- **Enhanced capability to prioritize and delegate tasks based on skill level and complexity.** Interviewees touted SD Elements as a platform that catalyzed their organizations' ability to prioritize and distribute workflow activities as a result of the platform's resource administrative capabilities.

Costs. Risk-adjusted PV costs include:

- **Annual software license and support.** After an initial cost of $110,000, Security Compass charged annual software license and support fees of $222,000 for Years 1 through 3. This cost was valued using data the interviewees and Security Compass provided.

The decision-maker interviews and financial analysis found that a composite organization experiences benefits of $2.86 million over three years versus costs of $663,000, adding up to a net present value (NPV) of $2.20 million and an ROI of 332%.

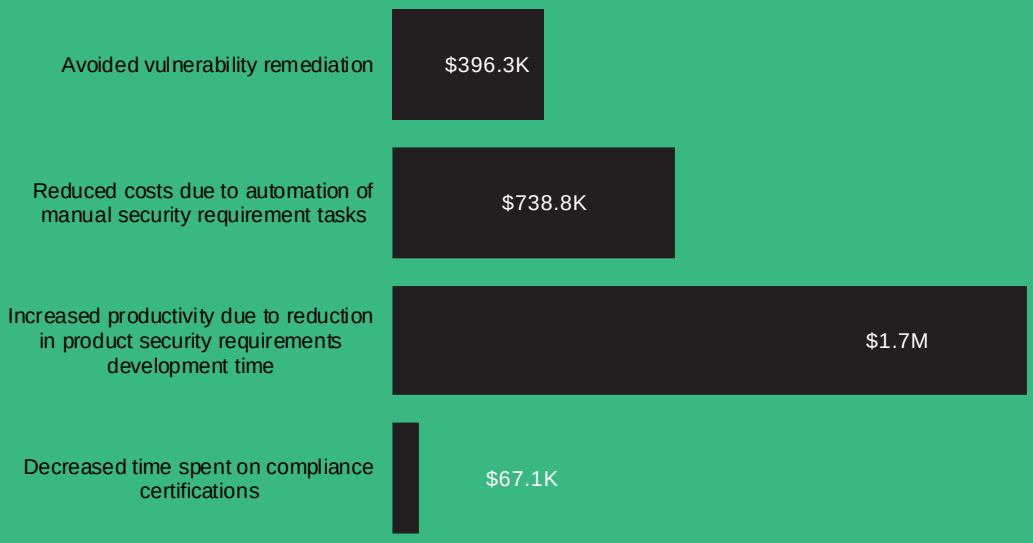
ROI
332%

BENEFITS PV
$2.86M

NPV
$2.20M

PAYBACK
<6 months

Benefits (Three-Year)



“SD Elements allows us to scale our security governance to meet the requirements of various jurisdictions. The automation it brings speeds up our process tremendously.”

— Chief product security officer, building equipment and controls

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 SD Elements.

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 SD Elements can have on an organization.

DUE DILIGENCE

Interviewed Security Compass stakeholders and Forrester analysts to gather data relative to SD Elements.

DECISION-MAKER INTERVIEWS

Interviewed four decision-makers at organizations using SD Elements 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 Security Compass SD Elements Customer Journey

Drivers leading to the SD Elements investment

Interviewed Decision-Makers

Interviewee	Industry	HQ	Geographic Market	Revenue	Size
Director and deputy chief product cybersecurity officer	HVAC, building controls, fire, and security	US	Global	$18 billion	56,000 employees
Vice president and chief information security officer	IT and services for transportation and defense	US	Global	$1.5 billion	6,200 employees
Vice president, cybersecurity	Financial services	US	Global	$17 billion	62,000 employees
Chief product security officer	Building equipment and controls	US	Global	$31 billion	28,000 employees

KEY CHALLENGES

The interviewees noted how their organizations could not efficiently develop and update comprehensive security requirements prior to SD Elements. They struggled with several common challenges contributing to this lack of ability to efficiently integrate security into the development process, including the following:

- **Prior automated solutions only provided generalized security requirements.** Interviewees' organizations that had automated security requirement solutions in place prior to implementing SD Elements discussed the difficulty they faced developing product-specific requirements and that their solution was only able to generate bare-minimum requirements.
- **Security requirements developed manually were difficult to track and update and failed to ensure product compliance.** Interviewees using manual spreadsheet-driven processes noted that their organizations lacked the ability to efficiently develop security requirements and track them across the development process. In some cases, this caused rewritten code, slower time-to-market, and frustration for developers who found themselves backtracking and spending significant time brainstorming relevant requirements.
- **A lack of visibility.** The consensus among interviewees, regardless of their organizations' prior environment, was that it was extremely difficult to accurately monitor the status of different products and their requirements. Interviewees noted that there was a significant lag in receiving status updates that slowed down development and both inter- and extradepartmental handoffs.

SOLUTION REQUIREMENTS

The interviewees' organizations searched for a solution that could:

- Establish product security as a practice.
- Improve security certification and compliance.
- Better identify security requirements during development activities.
- Improve security requirement development process efficiency.
- Improve their ability to track products' ongoing requirement development.
- Provide more application-specific security requirements.

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of the four 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:

Description of composite. The composite organization is a digital and SaaS technology-enabled business with revenues of $1.5B to $31B. It has 6,000 to 62,000 employees and more than 2,000 customers for B2B businesses and tens of thousands of customers for B2C companies. The organization could be in different industries with two key commonalities: 1) having extensive product lines and 2) being in an industry that is in the growth or maturity phases. The composite organization is a product-oriented business with operations spanning a wide geographic region with a unique set of security requirements for each product and region.

Deployment characteristics. The composite organization implements various tools and develops manual solutions to address gaps in the security requirement development and tracking processes. The organization is typically cloud-based and utilizes SaaS tools.

Key assumptions

- **$1.5 billion to $31 billion revenue**
- **Digital and SaaS technology-enabled business**
- **6,000 to 62,000 employees**
- **Numerous products**
- **Operating in various geographies**

“We needed something more dynamically driven and more application-specific.”
— Vice president, cybersecurity, financial services

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	Avoided vulnerability remediation	$159,375	$159,375	$159,375	$478,125	$396,342
Btr	Reduced costs due to automation of manual security requirement tasks	$297,075	$297,075	$297,075	$891,225	$738,782
Ctr	Increased productivity due to reduction in time developing security requirements for products	$668,100	$668,100	$668,100	$2,004,300	$1,661,466
Dtr	Decreased time spent on compliance certifications	$27,000	$27,000	$27,000	$81,000	$67,145
	Total benefits (risk-adjusted)	$1,151,550	$1,151,550	$1,151,550	$3,454,650	$2,863,735

AVOIDED VULNERABILITY REMEDIATION

Evidence and data. The deployment of SD Elements was pivotal in allowing interviewees' organizations to avoid significant time remediating application vulnerabilities, including the time to find vulnerabilities, and implement, test, and review fixes.

Modeling and assumptions. To calculate the value of this benefit, Forrester assumes the following:

- The model is based on a large enterprise organization where security architects are manually reviewing industry and regulatory guidelines, tracking these guidelines via spreadsheets, and then rolling out security requirements to hundreds of developers. Organizations that do not have a team of security architects doing this see an even greater return on vulnerabilities avoided.
- There are 250 applications on average for the composite organization.
- It takes an average of 10 hours of remediation time per application.
- The average fully burdened hourly salary of a senior security engineer is $75.

Risks. The value of this benefit can vary across organizations due to differences in complexity and architecture of the applications.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $396,000.

> **"When deploying SD Elements, we saw a huge decrease in the cost of critical vulnerabilities that were being produced and reworked."**
> *— Vice president, cybersecurity, financial services*

Avoided Vulnerability Remediation					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Number of applications	Interviews	250	250	250
A2	Remediation time avoided per application (hours)	Interviews	10	10	10
A3	Fully loaded hourly rate of senior security engineer	TEI standard	$75	$75	$75
At	Avoided vulnerability remediation	A1*A2*A3	$187,500	$187,500	$187,500
	Risk adjustment	↓15%			
Atr	Avoided vulnerability remediation (risk-adjusted)		$159,375	$159,375	$159,375
	Three-year total: $478,125		**Three-year present value: $396,342**		

REDUCED COSTS DUE TO AUTOMATION OF MANUAL SECURITY REQUIREMENT TASKS

Evidence and data. Without SD Elements, security architects had to understand new and updated requirements, update spreadsheets, and provide training for security champions. If an application release was in flight or about to be completed, the security organization had to review with the development teams where the policy impacted their workflow, which caused some friction and debate over what had to be changed to release the application. If there was a completely new policy, such General Data Protection Regulation (GDPR), security architects had to review the new policies, create a spreadsheet with all the requirements, and roll out new policies to each development team.

Interviewees told Forrester that, without SD Elements, security champions and development teams had to review any new or updated requirements to understand them based on their tech stack regarding how they impacted the application. Each requirement had to be reviewed whether relative decisions would impact the application or not. If decisions did have impact, then they had to indicate if the requirement had been implemented or not. If it had not been implemented, development had to create a ticket to implement. Security would have to track that development implemented the requirement.

With SD Elements, Forrester learned that one customer experienced going from seven standards based on their tech stack to 44 standards that were captured in the platform. One interviewee noted: "With SD Elements, requirements are automatically updated every six weeks. This saves my organization the time to understand requirements, create spreadsheets, and roll-out to security champions."

"The speed to complete the security requirements is significantly improved, probably by a factor of 10."
Chief product security officer, building equipment and controls

Forrester found that, after the SD Elements implementation at interviewees' organizations, the relationship between development and security was greatly improved. SD Elements let the development teams know where they were impacted and even created task tickets for them and provided updates when completed. Interviewees felt that security no longer needed to chase development to provide fixes and instead focused on being an advisor and partner to development.

Modeling and assumptions. To calculate the value of this benefit, Forrester assumes the following:

- There are 250 applications on average for the composite organization.
- The composite reduces the time to understand and integrate applicable requirements by 16 hours on average.
- The average fully burdened hourly salary of a senior security engineer is $75.
- The fully loaded annual salary of a senior security engineer is $150,000, one-third of which is for maintaining security requirements.

"[Before SD Elements], it was a struggle for engineers and the security team to create comprehensive requirements that made sense for each different product that we have."
Vice president and chief information security officer, IT and services for transportation and defense

Risks. The value of this benefit can vary across organizations due to differences in:

- The complexity and architecture of the applications, including how much organizations are able to automate.
- The maintenance of the catalog and relevant requirements.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $739,000.

"The complexity of keeping up with spreadsheets was a paramount problem."
Chief product security officer, building equipment and controls

Reduced Costs Due To Automation Of Manual Security Requirement Tasks					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Number of applications	Interviews	250	250	250
B2	Reduced hours to understand and integrate applicable requirements	Interviews	16	16	16
B3	Fully loaded hourly rate of senior security engineer	TEI standard	$75	$75	$75
B4	Subtotal: Reduced cost due to automation of manual security requirement tasks	B1*B2*B3	$300,000	$300,000	$300,000
B5	Fully loaded annual salary of senior security engineer	Interviews	$150,000	$150,000	$150,000
B6	Portion of FTE to maintain requirements for organization	Interviews	0.33	0.33	0.33
B7	Subtotal: Cost of one-third time of FTE	B5*B6	$49,500	$49,500	$49,500
Bt	Reduced costs due to automation of manual security requirement tasks	B4+B7	$349,500	$349,500	$349,500
	Risk adjustment	↓15%			
Btr	Total reduced costs due to automation of manual security requirement tasks (risk-adjusted)		$297,075	$297,075	$297,075
	Three-year total: $891,225		**Three-year present value: $738,782**		

INCREASED PRODUCTIVITY DUE TO REDUCTION IN PRODUCT SECURITY REQUIREMENTS DEVELOPMENT TIME

Evidence and data. Without SD Elements, interviewees required multiple meetings and discussions for a new product to understand the technology stack and what requirements were applicable. Interviewees' organizations' productivity increased significantly as a result of the platform, decreasing the time to develop security requirements for products by 90%.

Modeling and assumptions. To calculate the value of this benefit, Forrester assumes the following:

- There are 250 applications on average for the composite organization.
- The ratio of applications to products is 1:6.
- The composite requires 80 hours to develop security requirements prior to SD Elements.
- The composite requires 8 hours to develop security requirements after SD Elements.
- The average fully burdened hourly salary of a senior security engineer is $75.

Risks. The value of this benefit can vary across organizations due to differences in:

- The complexity and architecture of the products.
- The number of products.
- The complexity of developing security requirements.
- Efficiency in reducing the number of hours per product.
- FTEs salary across organizations and geographic locations.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of nearly $1.7 million.

Increased Productivity Due To Reduction In Product Security Requirements Development Time					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Number of applications	Interviews	250	250	250
C2	Ratio of applications to products	Interviews	1.6	1.6	1.6
C3	Number of products	C1/C2	156	156	156
C4	Number of hours per product to develop security requirements prior to SD Elements	Interviews	80	80	80
C5	Total number of hours required prior to SD Elements implementation	C3*C4	12,480	12,480	12,480
C6	Number of hours per product to develop security requirements with SD Elements	Interviews	8	8	8
C7	Total number of hours required after SD Elements implementation	C1*C6	2,000	2,000	2,000
C8	Reduction in total hours because of SD Elements	C5-C7	10,480	10,480	10,480
C9	Fully loaded hourly rate of senior security engineer	TEI standard	$75	$75	$75
Ct	Increased productivity due to reduction in product security requirements development time	C8*C9	$786,000	$786,000	$786,000
	Risk adjustment	↓15%			
Ctr	Increased productivity due to reduction in product security requirements development time (risk-adjusted)		$668,100	$668,100	$668,100
	Three-year total: $2,004,300		**Three-year present value: $1,661,466**		

DECREASED TIME SPENT ON COMPLIANCE CERTIFICATIONS

Evidence and data. Many interviewees required compliance security certifications. With SD Elements, the interviewees saved time because they could easily generate a report for the auditing agency. One interviewee stated, "If auditors have questions, it is easy with SD Elements to dive into the details and see what requirements were implemented."

SD Elements also gave executives an understanding of their application portfolios. One interview stated that their organization "can see which products need to move forward on product certification or may need to do so in the future." Security executives could prioritize what certifications were most important.

Modeling and assumptions. To calculate the value of this benefit, Forrester assumes the following:

- There are 10 certifications per year on average for the composite organization.
- The implementation of SD Elements saves 40 hours per certification.
- The average fully burdened hourly salary of a senior security engineer is $75.

Risks. The value of this benefit can vary across organizations due to differences in:

- The number of certifications.
- The complexity and architecture of the products.
- The rate of savings per certification.
- FTEs salary across organizations and geographic locations.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $67,000.

Decreased Time Spent On Compliance Certifications					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
D1	Certifications per year	Interviews	10	10	10
D2	Hours saved per certification	Interviews	40	40	40
D3	Total hours saved on compliance certifications because of SD Elements	D1*D2	400	400	400
D4	Fully loaded hourly rate of senior security engineer	TEI standard	$75	$75	$75
Dt	Decreased time spent on compliance certifications	D3*D4	$30,000	$30,000	$30,000
	Risk adjustment	↓10%			
Dtr	Decreased time spent on product security certifications (risk-adjusted)		$27,000	$27,000	$27,000
	Three-year total: $81,000		**Three-year present value: $67,145**		

"The SD Elements team keeps adding more functionality, including the ability to integrate with other components of the CI/CD pipeline and ticketing tools."

— VP of DevOps and cybersecurity

UNQUANTIFIED BENEFITS

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

- **Increased ability to drive customers' speed-to-market.** Interviewees reported that SD Elements catalyzed their organizations' ability to provide for the secure development of their applications and solutions, which in turn allowed them to accelerate their abilities to meet market requirements.
- **Improved development team capabilities to focus on core responsibilities.** Interviewees noted that SD Elements allowed their developers to concentrate on core operational tasks, particularly by utilizing the solution's training library. This allowed their developers to rapidly consume and learn specific, relevant security requirements.
- **Enhanced capability to prioritize and delegate tasks based on skill level and complexity.** Interviewees touted SD Elements as a solution that allowed their organizations to prioritize and distribute critical tasks.

FLEXIBILITY

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

- **Flexibility to address customer questions about how cybersecurity is integrated into the development process**. In addition to the pure automation functionality that SD Elements offered, its security library gave interviewees' customers the ability to get their DevSec-related questions answered, which in turn offered their teams options to be more aware and, thus, more market relevant.
- **Flexibility to enhance security and development relationship.** Interviewees reported that SD Elements allowed their organizations to showcase the value of secure development to development teams, thereby providing a unique but critical ability to enhance the symbiosis between the security and development teams.

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	Software license and support	$110,000	$222,200	$222,200	$222,200	$776,600	$662,579
	Total costs (risk-adjusted)	$110,000	$222,200	$222,200	$222,200	$776,600	$662,579

SOFTWARE LICENSE AND SUPPORT

Evidence and data. Security Compass charged annual software license and support fees of $222,000 for Years 1 through 3 after an initial cost of $110,000.

Modeling and assumptions. This cost is valued using data provided by interviewees and Security Compass.

Risks. The value of this cost can vary across organizations due to:

- Preferred pricing depending on customer size and industry.
- Changes in license pricing as customer organizations grow and require additional functionality.
- The initial support required at the onset of a client engagement and implementation.

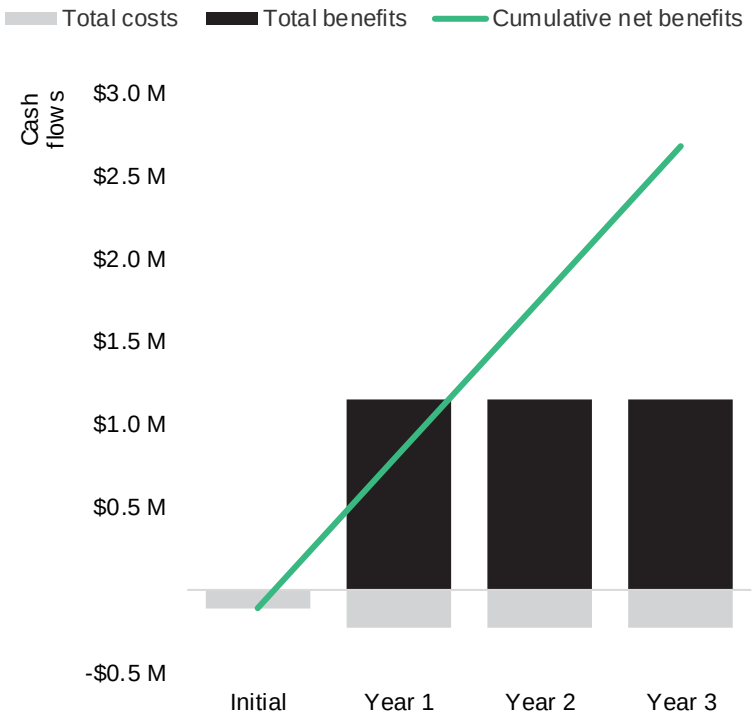
Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $663,000.

Software License And Support						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Software license and support	Interviews	$100,000	$202,000	$202,000	$202,000
Et	Software license and support	E1	$100,000	$202,000	$202,000	$202,000
	Risk adjustment	↑10%				
Etr	Software license and support (risk-adjusted)		$110,000	$222,200	$222,200	$222,200
	Three-year total: $776,600			**Three-year present value: $662,579**		

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	($110,000)	($222,200)	($222,200)	($222,200)	($776,600)	($662,579)
Total benefits	$0	$1,151,550	$1,151,550	$1,151,550	$3,454,650	$2,863,735
Net benefits	($110,000)	$929,350	$929,350	$929,350	$2,678,050	$2,201,156
ROI						332%
Payback period (months)						<6

Appendix A: Total Economic Impact

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

TOTAL ECONOMIC IMPACT APPROACH

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

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

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

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

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®