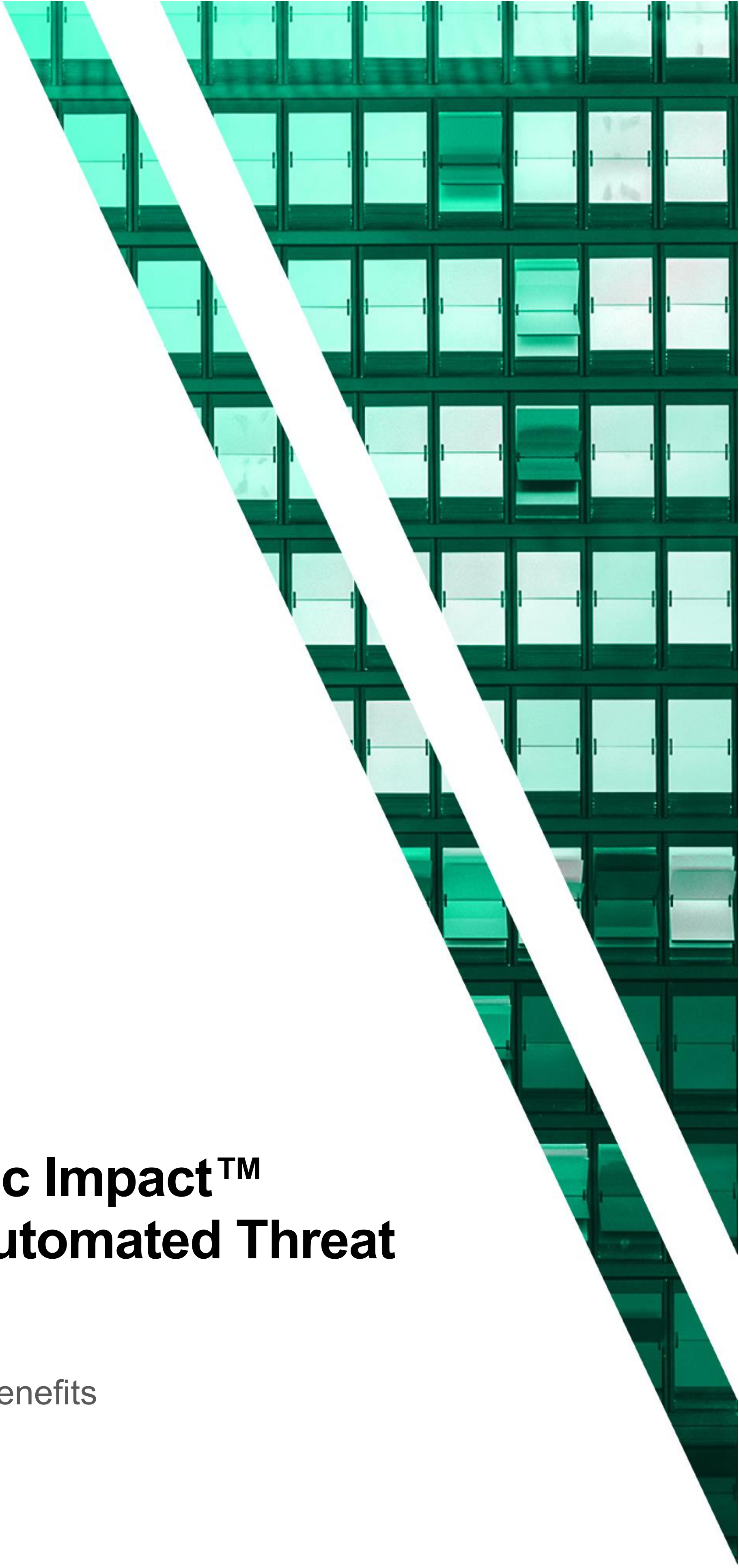


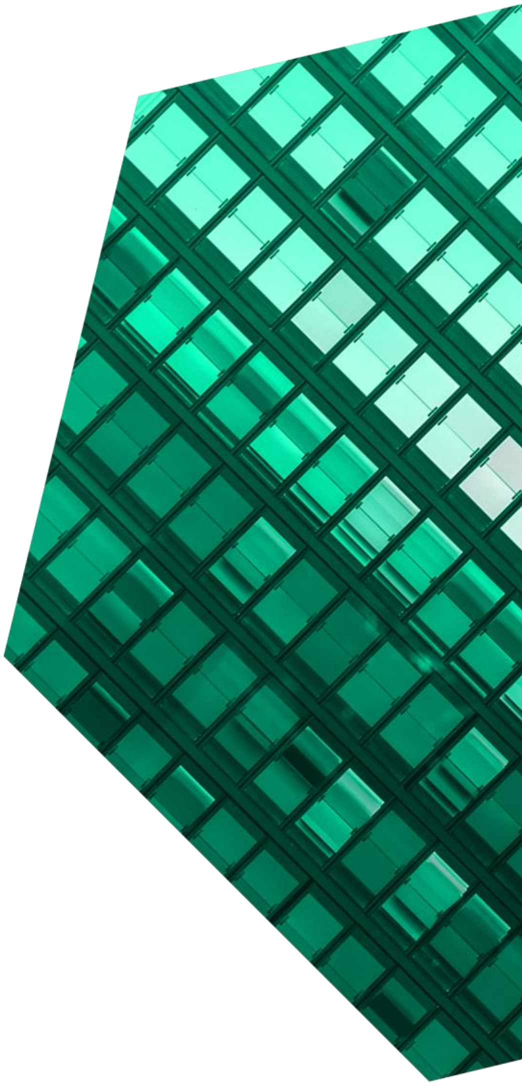
The Total Economic Impact™ Of The IriusRisk Automated Threat Modeling Platform

Cost Savings And Business Benefits
Enabled By IriusRisk

APRIL 2023

A FORRESTER TOTAL ECONOMIC IMPACT™ STUDY COMMISSIONED BY IRIUSRISK

Consulting Team: *Stefanie Vollmer*
Jan Sythoff



ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key transformation outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute on their priorities using a unique engagement model that tailors to diverse needs and ensures lasting impact. For more information, visit forrester.com/consulting.

Executive Summary

Organizations engage in threat modeling early in the software product lifecycle to reduce the number of security flaws introduced into their software systems. Manual threat modeling is common, but security teams struggle to scale it efficiently. IriusRisk helps organizations design secure systems by automating threat modeling and helping security and development collaborate at the earliest stages of the lifecycle. By automatically identifying threats and recommending countermeasures, IriusRisk helps teams secure products by design at scale.

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

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four representatives with experience using the IriusRisk Automated Threat Modeling Platform. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization.

Time to create a threat model:

From 80 hours to 8

Prior to using IriusRisk, these interviewees noted how their organizations carried out manual threat modeling on an ad hoc basis. Scalability is one of the common challenges with manual threat modeling, as security expertise remains scarce within organizations. As a result, only the most critical products are threat modeled prior to projects beginning. It leaves the majority of the product portfolio at risk of security flaws built into the design that are more difficult to remediate. Even threat modeled products could be vulnerable to security attacks.

KEY STATISTICS

Return on investment (ROI)

203%

Net present value (NPV)

$7.20M

After the investment in the IriusRisk Automated Threat Modeling Platform, the interviewees experienced efficiencies from automating threat modeling, cost savings from remediation avoidance, and efficiencies meeting and reporting on risk and compliance posture.

KEY FINDINGS

Quantified benefits. Three-year, risk-adjusted present value (PV) quantified benefits for the composite organization include:

- **Threat modeling automation efficiencies, worth $1.8 million over three years.** By implementing IriusRisk, the composite organization realizes a time savings of 72 hours per threat model. IriusRisk automates repetitive threat modeling tasks, so security teams can effectively focus on their resources.
- **Cost savings from remediation avoidance, worth $4.9 million over three years.** This is the biggest benefit for the composite organization, allowing it to avoid material time in remediating product vulnerabilities.
- **Increased productivity from compliance and reporting, worth $3.9 million over three years.** Prior to implementing IriusRisk, compliance and reporting was an intense and time-consuming process. By engaging IriusRisk, the composite organization gains access to the tool's extensive threat and countermeasure knowledge base, saving the security team hundreds of hours to review documents and match standards and requirements.
- **Increased productivity from integrating IriusRisk with issue trackers, worth $108,000 over three years.** Due to the lack of integration with issue trackers, manual threat modeling did not allow the validation of appropriate risk mitigation controls. After implementing IriusRisk, countermeasures are inserted directly into developer workflows, enabling a 50% productivity improvement for the composite organization.
- **Cost savings from avoidance of security incidents, worth $35,000 over three years.** IriusRisk allows cost savings from avoided security incidents due to identifying and remediating issues that would have otherwise led to incidents.

Unquantified benefits. Benefits that provide value for the composite organization but are not quantified in this study include:

- **Customization abilities.** Organizations can customize threat libraries, which allows them to map customized risk patterns to a component. Moreover, organizations benefit from IriusRisk's flexible out-of-the-box solution that can be used across their subsidiaries.
- **Fostering a threat modeling culture.** The introduction of IriusRisk helps to build a formal practice around threat modeling within organizations.

Costs. Three-year, risk-adjusted PV costs for the composite organization include:

- **Software license and support.** For the composite organization, a company with 1,000 products, the three-year present value of IriusRisk licenses comes to $2.3 million.
- **Implementation costs.** For the composite organization, initial implementation costs come to $46,000. This includes an initial configuration, testing of the platform, and rolling out the concept to the security team and development.
- **Onboarding and training.** On average, the composite organization's Software Security Group (SSG) employees and developers spends one full day on training sessions. There is initial training with a number of SSG employees, which is extended to the wider security team during the three-year period.
- **Ongoing management.** The composite organization has modest ongoing maintenance costs of $337,000 over three years.

The representative interviews and financial analysis found that a composite organization experiences benefits of $10.75 million over three years versus costs of $3.55 million, adding up to a net present value (NPV) of $7.20 million and an ROI of 203%.

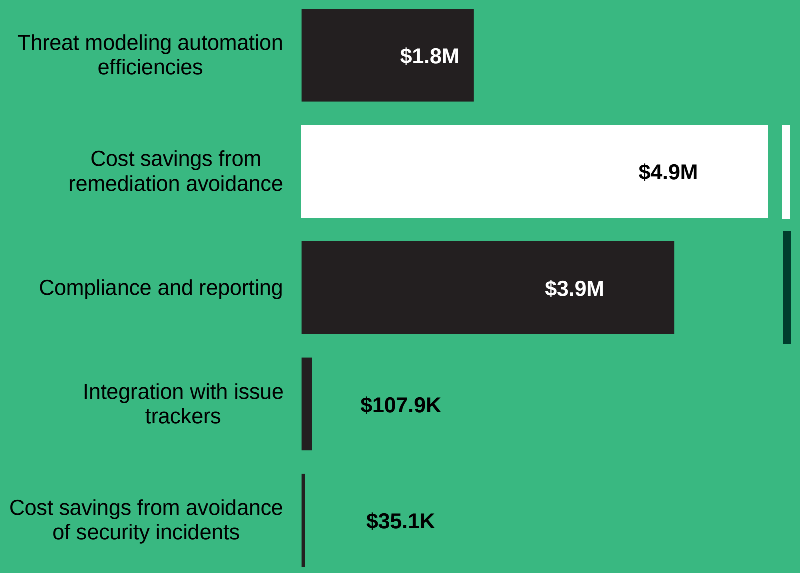
ROI
203%

BENEFITS PV
$10.75M

NPV
$7.20M

PAYBACK
<6 months

Benefits (Three-Year)



The biggest category represents the cost savings from remediation avoidance.

Firms also see increased productivity as security teams save hundreds of hours by leveraging IriusRisk's knowledge base.

> **"We have seen an increase in developers creating better architecture diagrams and documentation because of using IriusRisk. Previously, we had developers who worked on their very specific piece of code for this product. When they saw the whole picture, they had kind of an aha moment."**
>
> — Principal software architect, software sales

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 IriusRisk Automated Threat Modeling Platform.

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 IriusRisk can have on an organization.

Forrester Consulting conducted an online survey of 351 cybersecurity leaders at global enterprises in the US, the UK, Canada, Germany, and Australia. Survey participants included managers, directors, VPs, and C-level executives who are responsible for cybersecurity decision-making, operations, and reporting. Questions provided to the participants sought to evaluate leaders' cybersecurity strategies and any breaches that have occurred within their organizations. Respondents opted into the survey via a third-party research panel, which fielded the survey on behalf of Forrester in November 2020.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by IriusRisk and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the study to determine the appropriateness of an investment in IriusRisk Automated Threat Modeling Platform.

IriusRisk reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester’s findings or obscure the meaning of the study.

IriusRisk provided the customer names for the interviews but did not participate in the interviews.

DUE DILIGENCE

Interviewed IriusRisk stakeholders and Forrester analysts to gather data relative to IriusRisk Automated Threat Modeling Platform.

INTERVIEWS

Interviewed four representatives at organizations using IriusRisk 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 interviewees.

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 IriusRisk Automated Threat Modeling Platform Customer Journey

🟩 Drivers leading to the Automated Threat Modeling Platform investment

Interviews

Role	Industry	Region	Annual Revenue	Employees
Director of product security	Software sales	US	$6.9 billion	20,000
Principal software architect	Software sales	US and Europe	$313.5 million	1,700
Security domain expert	Financial services	Europe	$8.8 billion	46,000
Director of cloud security engineering	Financial services	Global	$75.3 billion	223,400

KEY CHALLENGES

Prior to investing in IriusRisk, the interviewees' organizations lacked a structural approach to threat modeling. Most organizations carried out manual threat modeling on an ad hoc basis, and it was done by the central security team. One organization didn't carry out threat modeling at all. The interviewees noted how their organizations struggled with common challenges, including:

- **Manual threat models that were difficult to scale.** All interviewees stated the time-consuming element of creating a manual threat model. It involved several repetitive tasks that needed to be carried out every time when setting up a new threat model. As the director of cloud security engineering at a financial service institution explained: "The architecture diagram had to be developed every single time. We were experiencing a lack of scalability and a lack of automation." The principal software architect at a software sales company added that manual threat modeling wasn't an activity that was done universally. As a result, only the most critical products were threat modeled, leaving the majority of the product portfolio at risk of security flaws built into the design that would be more difficult to remediate.
- **Bottlenecks with the security team.** Based on the 2022 Building Security In Maturity Model (BSIMM) survey, there are, on average, three Software Security Group (SSG) members for every 100 developers.[2] This shows the scarcity of employees with formal threat modeling knowledge within an organization, even though they have a formal software security team. All interviewees mentioned that the low product-security-to-developer ratio has hindered the organization from scaling its threat modeling operations across the organization and across its product portfolio.

> **"Manual threat modeling was not an activity that was done across the board. It was only possible for a handful of our key products."**
>
> *Principal software architect, software sales*

- **Inconsistencies in manual threat modeling.** The effectiveness of manual threat modeling depends on the judgment of those performing it. Different people building threat models have different views on what a threat is and how it should be ranked. These inconsistencies consequently have an impact on the way developers prioritize threats. As the director of product security at a software sales firm explained, "A lack of standardized processes led to inconsistent outputs." This means that threats and controls could be missed.

- **Difficulties in providing evidence of compliance.** Most of the interviewees reported that manual threat modeling made it difficult to provide regulators with an overview of the organization's security profile. The security domain expert at a financial services institution stated that the auditing process used to be a time-consuming exercise for the software security group, and it bogged down innovation.
- **Lack of control implementation.** After setting up a manual threat model, reports had to be generated with all the vulnerabilities that needed to be addressed by the developers. All interviewees shared that their organizations lacked integration with an incident tracker. As the principal software architect at a software sales firm explained, it was difficult to track and verify whether controls had been implemented.

SOLUTION REQUIREMENTS/INVESTMENT OBJECTIVES

The interviewees' organizations searched for a solution that allowed:

- **Automation of threat modeling.** According to interviewees, this was the top driver of the IriusRisk investment for several organizations. IriusRisk automates repetitive threat modeling tasks so security teams can effectively focus their resources, meaning that it alleviates any security team bottlenecks. IriusRisk Automated Threat Modeling Platform allows security teams to quickly define diagrams and threat models that can be scaled across the organization.
- **Integration with developers' workflow.** Due to the lack of integration with issue trackers, manual threat modeling did not allow to validate the appropriate risk mitigation controls implemented by the developers. IriusRisk seamlessly integrates with issue trackers, and it forms part of the developer's workflow. Additionally, the principal software architect at a software sales company explained that IriusRisk supports bidirectional communication when integrated with an issue tracker. They noted, "Not only the ticket is automatically generated — there is also an update on IriusRisk as soon as the ticket has been completed."
- **Flexibility and customization abilities.** IriusRisk's customization abilities were another key driver of investment. All interviewees mentioned that customization allowed them to use IriusRisk in the first place. It seamlessly integrates with their organizations' tools and workflows, and it allows them to import diagrams.

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 interviewees, and it 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 multinational financial organization with headquarters in North America and Europe, and it generates revenues of $10 billion to $20 billion each year. It has an employee base of 50,000 to 100,000; the software security group consists of 50 security architects and 150 security champions. There are a total of 1,000 developers. The composite organization has a portfolio of 1,000 products. IriusRisk is deployed on-premises.

Deployment characteristics. To support its business activities, the composite organization operates representative offices and service branches at selected locations in North America and Europe. As a large financial institution, the composite organization is subject to extensive governance and regulatory requirements. The security team is centralized and responsible for security across its network banks. Therefore, the composite organization is gradually scaling its threat modeling activities across its product portfolio and network banks. The composite organization invests in IriusRisk because it offers a comprehensive solution for threat modeling across the organization.

Key Assumptions

- **Financial institution**
- **Operating in North America and Europe**
- **$10B to $20B revenue**
- **50,000 to 100,000 employees**
- **1,000 products**

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	Threat modeling automation efficiencies	$324,000	$648,000	$1,296,000	$2,268,000	$1,803,787
Btr	Cost savings from remediation avoidance	$301,219	$1,204,875	$4,819,500	$6,325,594	$4,890,561
Ctr	Compliance and reporting	$432,000	$0	$4,680,000	$5,112,000	$3,908,881
Dtr	Integration with issue trackers	$23,400	$40,950	$70,200	$134,550	$107,858
Etr	Cost savings from avoidance of security incidents	$2,160	$8,640	$34,560	$45,360	$35,070
	Total benefits (risk-adjusted)	$1,082,779	$1,902,465	$10,900,260	$13,885,504	$10,746,157

THREAT MODELING AUTOMATION EFFICIENCIES

Evidence and data. Prior to implementing IriusRisk, the interviewees' organizations typically carried out manual threat modeling, which was time-consuming and difficult to execute as employees are geographically dispersed. Moreover, manual threat modeling was an activity that was done on an ad hoc basis, and it wasn't integrated into the software development lifecycle. Security expertise is scarce; hence, organizations lack the resources to devote senior security personnel for multiday exercises for each project or product. As a result, only a portion of the product portfolio was being threat modeled.

- The principal software architect at a software sales company stated: "Prior to starting our journey with IriusRisk, two to three individuals within the security team who had the relevant experience were doing manual threat modeling. It generally involved setting up a meeting with the software developers and then travelling to the development center site. We would then all get in a room for two or three days and discuss. Sometimes, the manual threat modeling exercise required traveling for multiple people going to a centralized location because we are a globally distributed company."
- The same interviewee noted: "A threat model wasn't set up unless we had a specific request to do it. … With IriusRisk, we're threat modeling all our product as we were able to reduce the cost from traveling."
- Prior to IriusRisk, manual threat modeling involved several repetitive tasks such as creating architecture diagrams. The director of cloud security engineering at a financial services organization noted efficiencies of reusing architectures and other content that is available in the IriusRisk library.
- Several interviewees explained that with IriusRisk, threat modeling is now integrated into their software development lifecycle, which includes an automated and continuous security review.
- All interviewees mentioned the lack of security expertise and the low product-security-to-developer ratio. The director of product security

at a software sales firm explained: “The latest BSIMM statistics stated that for every 100 developers, there were three application security people. We are still at around 1.6% or 1.7%.”

- IriusRisk enabled organizations to shift how they performed threat modeling: Security champions became each threat model's point of contact. The director of product security added: “It has helped from a scalability perspective to have security champions as a single point of contact. It used to be two or three individuals in our team just facilitating the whole threat modeling exercise. We’ve shifted that to having the security champions do that front-load work, and then we do the review.” The principal software architect at a software sales company echoed: “Security champions are the ones who are now required to do the threat models because they know their products. We don't know their products.”
- In multinational organizations, employees within the security group and software developers tended to be geographically dispersed, which complicated the collaboration when setting up a threat model and led to delays in the process. All interviewees stated that IriusRisk helped to break down silos between security and development teams. Furthermore, the interviewees found that using IriusRisk during the product design stage led to an increased security awareness due to greater communication and understanding across teams.

Modeling and assumptions. For the composite organization, Forrester assumes that:

- The composite organization has a portfolio of 1,000 products.
- Prior to using IriusRisk, manual threat modeling was carried out for 5% of the product portfolio in Year 1 (50 threat models), 10% in Year 2 (100 threat models) and 20% in Year 3 (200 threat models).
- A senior security architect takes an average of 80 hours to set up a manual threat model.
- With IriusRisk, it takes an average of 8 hours for a senior security architect to create an automated threat model.
- The average fully loaded hourly salary of a senior security architect is $100.

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

- The complexity and architecture of the products.
- The initial setup prior to automation. For example, the director of cloud security engineering at a financial services institution shared that their workflow needs improvement before it can be automated, which can take several weeks. This could therefore delay the automation of threat modeling with IriusRisk.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.8 million.

Threat Modeling Automation Efficiencies

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Products	Interviews	1,000	1,000	1,000
A2	Manual threat modeling: percentage of applications covered	Interviews	5%	10%	20%
A3	Manual threat models	A1*A2	50	100	200
A4	Time per manual threat model (setting it up, generating a report, and following up) (hours)	Interviews	80	80	80
A5	Fully loaded hourly rate of senior security architect	TEI standard	$100	$100	$100
A6	Time to create an automated threat model (hours)	Interviews	8	8	8
A7	Cost (per threat model) of automated threat modeling	A3*A5*A6	$40,000	$80,000	$160,000
At	Threat modeling automation efficiencies	(A3*A4*A5)-A7	$360,000	$720,000	$1,440,000
	Risk adjustment	↓10%			
Atr	Threat modeling automation efficiencies (risk-adjusted)		$324,000	$648,000	$1,296,000
	Three-year total: $2,268,000		**Three-year present value: $1,803,787**		

COST SAVINGS FROM REMEDIATION AVOIDANCE

Evidence and data. This was the biggest benefit identified by the interviewees. The deployment of IriusRisk was pivotal in allowing their organizations to avoid significant time and costs remediating product security flaws, including the time to find them. The interviewees shared that:

- Delays were drastically reduced because security requirements are known upfront. The security domain expert at a financial institution stated: “IriusRisk helped us to ensure go-live dates of [our] products by introducing a shift-left approach. If the left side is done well, the right side won't stress you.”

- By integrating IriusRisk during the design process, software security teams received a list of security tasks that they required before a line of code was written. The principal software architect at a software sales company explained: “As part of our secure software development lifecycle … one requirement is that teams must address all the required countermeasures in IriusRisk. They are required to hit the security bar right at the beginning. That shift-left has helped us to get the security as part of the design before hands ever touched the keyboard, saving us a lot of potential remediation time.”

- The principal software architect at a software sales company highlighted the cost savings by using IriusRisk at the design stage: “The main point of threat modeling is to highlight some of those issues that could occur and to put mitigating controls prior to them ever being an issue in the code. It's much cheaper to find those issues at the beginning. Developers may take 1 hour to have a conversation and to implement controls around an issue. It takes hundreds of hours if the product reaches production. So that was the saving that we wanted to avoid by having to go in and fix those issues later.”

Modeling and assumptions. For the composite organization, Forrester assumes that:

- Prior to deploying IriusRisk, manual threat modeling is carried out for 5% of the product portfolio in Year 1, which can be extended to 10% in Year 2 and 20% in Year 3. This totals 950 products with no manual threat model in Year 1, 900 products in Year 2, and 800 in Year 3.

- The composite organization invests in 100 IriusRisk licenses in Year 1, which increases to 300 in Year 2 and 1,000 in Year 3. Each license can be used for one threat model, which serves one product. Consequently, the composite organization can threat model its entire product portfolio by Year 3.

- Out of those products without a threat model, Forrester assumes that 50% will need preproduction remediation.

- The average preproduction remediation time per product with no threat model requires 75 hours of a software developer’s time.

- For products without a threat model, Forrester assumes that 50% will need postproduction remediation.

- The average postproduction remediation time per product with no threat model is 100 hours. It is more time-consuming than fixing flaws preproduction, as it requires conceptual changes. The average conceptual postproduction remediation time per product with no threat model is 80 hours, and it is performed by a security architect. Additionally, it requires an average remediation time of 20 hours by a software developer.

- Comparing the situation before and after investing in IriusRisk, the difference in products with no threat model that will either need pre- or postproduction remediation is 50 in Year 1, 200 in Year 2, and 800 in Year 3.

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

- The complexity and architecture of the products.
- A chance also exists that threat modeled products will also experience some type of deficiencies, such as source code flaws and open-source vulnerabilities.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $4.9 million.

COMPLIANCE AND REPORTING

Evidence and data. Many organizations — especially those in the financial industry — face extensive governance and regulatory requirements for their software products. During auditing processes, these organizations need to prove they complied with all security requirements. Prior to implementing IriusRisk Automated Threat Modeling Platform, this used to be an intense and time-consuming process for all employees within the security and development groups.

Cost Savings From Remediation Avoidance

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Number of products	Interviews	1,000	1,000	1,000
B2	Number of IriusRisk licenses	Interviews	100	300	1,000
B3	Before IriusRisk investment: products with no manual threat model (Y1: 95%; Y2: 90%; Y3: 80%)	Interviews	950	900	800
B4	After IriusRisk investment: products with no automated threat model	B1-B2	900	700	0
B5	Before IriusRisk investment: products with no threat model needing preproduction remediation	B3*0.5	475	450	400
B6	After IriusRisk investment: products with no threat model needing preproduction remediation	B4*0.5	450	350	0
B7	Average preproduction remediation time per product with no threat model (hours)	Interviews	75	75	75
B8	Fully loaded hourly rate of senior software developer	TEI standard	$65	$65	$65
B9	Avoided preproduction remediation time	(B5-B6)*B7*B8	$121,875	$487,500	$1,950,000
B10	Before IriusRisk investment: products with no threat model, needing postproduction remediation (50%)	B3*0.5	475	450	400
B11	After IriusRisk investment: products with no threat model, needing postproduction remediation (50%)	B4*0.5	450	350	0
B12	Average conceptual postproduction remediation time per product with no threat model (hours)	Interviews	80	80	80
B13	Fully loaded hourly rate of senior security architect	TEI standard	$100	$100	$100
B14	Average postproduction remediation time per product with no threat model (hours)	Interviews	20	20	20
B15	Avoided postproduction remediation time	(B10-B11)*B12*B13+ (B10-B11)*B14*B8)	$232,500	$930,000	$3,720,000
Bt	Cost savings from remediation avoidance	B9+B15	$354,375	$1,417,500	$5,670,000
	Risk adjustment	↓15%			
Btr	Cost savings from remediation avoidance (risk-adjusted)		$301,219	$1,204,875	$4,819,500
	Three-year total: $6,325,594		**Three-year present value: $4,890,561**		

- The security domain expert at a financial services institution provided an overview of the lengthy compliance process that took place biyearly: “Being compliant to the Center for Internet Security (CIS) and The Open Web Application Security Project (OWASP) means to go through hundreds of pages and to extract the relevant requirements for the products. It takes approximately 10 hours per standard. This is a huge effort for us. The total time to create a report for an average complex project is 40 to 50 hours per product. After implementing the recommended security requirements, we also must prove that we remain compliant. It’s a reoccurring effort and it takes an additional 10 to 20 hours per product.”

- Both interviewees in the financial sector stated the advantage of engaging IriusRisk during compliance operations, as the tool provides information about relevant countermeasures per standard. All of the interviewees’ organizations gained access to IriusRisk’s extensive and frequently updated threat and countermeasure knowledge base. This saved the security team hundreds of hours of reviewing documents and matching standards and requirements.

- This Another benefit of using IriusRisk Automated Threat Modeling Platform is the consistency in implementing security requirements. The security domain expert at a financial institution explained, “If 10 teams take the CIS and OWASP documents and extract requirements, we need to check every team individually because every team could have different interpretations, they could make different mistakes.”

- IriusRisk seamlessly integrates with customers’ tools by using an API, which proved helpful during auditing. The director of cloud security engineering at a financial services firm stated: “IriusRisk allows us to query flaws via API, meaning that we can query threats in our database. This is important for auditing processes. It's a lot easier to provide them with a list of vulnerabilities when compliance requests this. It saves us time.”

- The security domain expert at a financial services institution further explained that IriusRisk has had an impact on the risk posture of the organization: “With the way IriusRisk allows us to do the audit reporting, this pushes the people to implement more controls for compliance because it's tracked. That also reduces our risk for compromise or data loss to avoid reputational damage. This is basically the topic our top management has a big focus on right now.”

- When creating a compliance report with IriusRisk, the interviewees noted that, over time, it took significantly less time. The security domain expert at a financial services organization explained: “The first time you're doing a compliance report, you have a large front-load of work, especially if it's an existing application. Ongoingly though, software engineers just need to go into the model and make some updates.”

Modeling and assumptions. For the composite organization, Forrester assumes that:

- The auditing process takes place biannually in Year 1 and Year 3.

- For the composite organization, Forrester assumes that one security engineer manages compliance and reporting.
- Prior to implementing IriusRisk, it takes an average total of 50 hours to create a compliance report per threat model (product), and a total time of 20 hours to generate a report proving that the organization adhered to the security requirements throughout the year. This totals 70 hours to create a compliance report.
- In Year 1, compliance and reporting with IriusRisk takes on average 10 hours per license (product), which is reduced to 5 hours in Year 3.
- The average fully loaded hourly salary of a senior security engineer is $80.

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

- The complexity and architecture of the products.
- The number of compliance reports that need to be generated.

> **"IriusRisk allows [us] to make changes at the design stage. It reduces risk and the financial impact in case of breaches or downtime. In banking, reducing risk is enough argument to introduce a new tool."**
>
> *Director of cloud engineering, financial industry*

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $3.9 million.

Compliance And Reporting

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Number of licenses	Composite	100	300	1,000
C2	Time per threat model to create compliance report and to stay compliant (hours)	Interviews	70	0	70
C3	Fully loaded hourly rate of senior security engineer	TEI standard	$80	$80	$80
C4	Avoided time of manual compliance	C1*C2*C3	$560,000	$0	$5,600,000
C5	Time per threat model to create compliance report with IriusRisk (hours)	Interviews	10	0	5
C6	Compliance and reporting with IriusRisk	C1*C3*C5	$80,000	$0	$400,000
Ct	Compliance and reporting	C4-C6	$480,000	$0	$5,200,000
	Risk adjustment	↓10%			
Ctr	Compliance and reporting (risk-adjusted)		$432,000	$0	$4,680,000
	Three-year total: $5,112,000		**Three-year present value: $3,908,881**		

INTEGRATION WITH ISSUE TRACKERS

Evidence and data. All interviewees stated that manual threat modeling did not integrate well with issue trackers to streamline the assignment of recommended controls to the development teams. Manual reports had to be created, which was time-consuming. Moreover, there was a lack of options to verify that the development teams had implemented mitigations.

- The principal software architect at a software sales company explained, “After generating a manual threat model, it took the team one week to generate a report with all threats that needed to be addressed by the developers.” Moreover, the interviewee added: “The reports were done manually, which often ended up sitting in someone's inbox or on their desk or as a doorstop. Not a lot of activity got taken on the actual actions without continuous follow-up.”
- In terms of validating the appropriate risk controls, several interviewees mentioned the inconsistency of verifying controls using spreadsheets and shared documents. Updates by email were subject to misinterpretation, and they provided poor evidence of compliance with regulatory standards. Hence, the principal software architect at a software sales company noted: “Having IriusRisk tie into [our issue-tracking system] and have it go right into the developers’ backlog as part of their daily activity has been really helpful. What's particularly helpful is the two-way sync between IriusRisk and your issue tracker: You can generate the ticket from IriusRisk and once the developer has worked off the ticket in their workflow through [the issue-tracker], it automatically updates it at as being implemented at IriusRisk.”
- Prior to introducing IriusRisk, engineers would typically consult software developers on the implementation of the countermeasures to address a list of threats. Several interviewees stated that with IriusRisk, development teams receive a list of clear and descriptive countermeasures on their task management tools, rather than generic advice. The security domain expert at a financial services institution referred to it as a “clear recipe,” which contributes to a fluid workflow.
- The director of cloud security engineering at a financial services institution echoed: “IriusRisk can be integrated to our [issue-tracking] system. Tickets are automatically assigned. Automation really helps here. As you write the threats, you are writing it into the system, so everything is in IriusRisk. We then write it down in Gherkin Syntax so it’s clear what needs to happen next to tackle the threat. It’s clear and descriptive. Project management loves it as it is very predictable. We have logs available showing which risks have been worked off. Tickets flow end to end.”

Modeling and assumptions. For the composite organization, Forrester assumes that:

- Prior to IriusRisk, the average time for a software developer to implement countermeasures per threat model is 16 hours in Year 1. When implementing controls, developers tend to become efficient over time, and the average time to implement countermeasures decreases to 14 hours in Year 2 and 12 hours in Year 3.
- After implementing IriusRisk, developers get countermeasures inserted directly into their workflow and there is a two-way sync between IriusRisk and the issue tracker. This enables a real-time view of the progress and the risk ratings associated with the threat-modeled product. Therefore, Forrester assumes a 50% productivity improvement, which reduces the average time for a software developer to implement countermeasures per product to 8 hours in Year 1, 7 hours in Year 2, and 6 hours in Year 3.

> **“When you use a tool like IriusRisk and you can show the countermeasures overview on the dashboard to audit, the trust increases immediately.”**
>
> *Security domain expert, financial industry*

- The average annual fully loaded hourly salary for a senior security developer is $65.

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

- The complexity and architecture of the products.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $107,900.

Integration With Issue Trackers

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Number of products	Composite	1,000	1,000	1,000
D2	Manual threat modeling: percentage of applications covered	Composite	5%	10%	20%
D3	Number of manual threat models	D1*D2	50	100	200
D4	Time to implement countermeasures per threat model (hours)	Assumption	16	14	12
D5	Fully loaded hourly rate of a senior security developer	TEI standard	$65	$65	$65
D6	Productivity improvement by having countermeasures integrated with issue trackers	Assumption	8	7	6
Dt	Integration with issue trackers	D3*D5*D6	$26,000	$45,500	$78,000
	Risk adjustment	↓10%			
Dtr	Integration with issue trackers (risk-adjusted)		$23,400	$40,950	$70,200
	Three-year total: $134,550		**Three-year present value: $107,858**		

COST SAVINGS FROM AVOIDANCE OF SECURITY INCIDENTS

Evidence and data. Even though organizations have numerous security solutions in place to comply with regulatory and compliance requirements, security breaches occasionally happen, and sometimes go unnoticed.

Forrester defines a breach as an incident resulting in the loss or compromise of data, accompanied by material remediation costs. "Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q4 2020" was fielded to 351 cybersecurity leaders at global enterprises from organizations spanning a range of industries in the US, Europe, and Australia to evaluate their experience with cybersecurity threats and their ramifications within their organizations. To qualify, respondents had to work at companies with 500 or more employees.[3] The survey data indicates:

- Organizations were likely to see 2.5 material breaches per year, whereby organizations in the financial industry sector experienced an average of five material breaches per year.
- The average time to detect and to remediate a security incident is 7.5 hours. Organizations in the financial services sector reported an average time of 8.6 hours. Organizations with an employee base of more than 100,000 were likely to spend 12 hours to detect and remediate a security incident.

Modeling and assumptions. For the composite organization, Forrester assumes that:

- Uncovered products (i.e., those with no manual or automated threat model) have a 5% likelihood of being affected by a security incident, whereas covered products with a threat model in place have a 1% likelihood of being affected.
- Prior to investing in IriusRisk, the total number of uncovered products (no manual threat model) that are affected by a security breach is 48 in Year 1, 45 in Year 2, and 40 in Year 3. The total number of covered products that experience a security breach is 0.5 in Year 1, one in Year 2, and two in Year 3.
- With IriusRisk, the total number of uncovered products that are affected by a security incident is 45 in Year 1 and 35 in Year 2. In Year 3, there are no uncovered products, as the composite organization has 1,000 IriusRisk licenses to cover its entire portfolio. The total number of covered products that experience a security incident is 1 in Year 1, 3 in Year 2, and 10 in Year 3.
- Incidents require an average of 12 hours of a security architect's time to remediate. This is in line with data from "Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q4 2020."
- The average fully loaded hourly salary of a senior security architect is $100.

> **"We discover the weaknesses, threats, and countermeasures, and we can map our customized risk patterns to a new or to an existing component. We use that capability extensively."**
>
> *Director of product security, software sales*

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

- The baseline security strength, exposure, and posture of the organization.
- The organization's size, industry, and location.
- The cybersecurity systemic risk.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $35,100.

Cost Savings From Avoidance Of Security Incidents

Ref.	Metric	Source	Year 1	Year 2	Year 3
E1	Number of products	Composite	1,000	1,000	1,000
E2	Before IriusRisk investment: products with no manual threat model (Y1: 95%; Y2: 90%; Y3: 80%)	Interviews	950	900	800
E3	Total uncovered products (no manual threat model) that are affected by a security incident	Assumption: 5%	47.5	45.0	40.0
E4	Total covered products (manual threat model) that are affected by a security incident	Assumption: 1%	0.5	1.0	2.0
E5	After IriusRisk investment: products with no automated threat model (Y1: 100 licenses; Y2: 300 licenses; Y3: 1,000 licenses)	Composite	900	700	0
E6	Total uncovered products (no automated threat model) that are affected by a security incident	Assumption: 5%	45.0	35.0	0.0
E7	Total covered products (automated threat model) that are affected by a security incident	Assumption: 1%	1.0	3.0	10.0
E8	Average time per senior security architect to detect and to remediate a security incident (hours)	Forrester survey	12	12	12
E9	Fully loaded hourly rate of a senior security developer	TEI standard	$100	$100	$100
E10	Before IriusRisk investment: total time to remediate security incidents	(E3+E4)*E8*E9	$57,600	$55,200	$50,400
E11	After IriusRisk investment: total time to remediate a security incident	(E6+E7)*E8*E9	$55,200	$45,600	$12,000
Et	Cost savings from avoidance of security incidents	E10-E11	$2,400	$9,600	$38,400
	Risk adjustment	↓10%			
Etr	Cost savings from avoidance of security incidents (risk-adjusted)		$2,160	$8,640	$34,560
	Three-year total: $45,360		**Three-year present value: $35,070**		

UNQUANTIFIED BENEFITS

Additional benefits that customers experienced but were not able to quantify include IriusRisk's customization abilities when working with threat libraries and creating solutions that can be scaled throughout the organization. Moreover, IriusRisk helps to introduce formal practices around threat modeling within organizations.

- **Leveraging customization abilities.** All of the interviewees' organizations benefited from IriusRisk's customization abilities; for some, this was decisive when choosing IriusRisk during the vendor selection process. As the director of product security at a software sales firm explained, "IriusRisk is flexible enough that we can use it and customize it to how we need to, which is critically important for us."
  - **Customizing threat libraries.** Several interviewees explained how they leverage IriusRisk's threat libraries, which allows them to customize it and create their own software components. Moreover, the director of product security added the ability to map customized risk patterns to a new or existing component.
  - **Customizing scalable solutions.** The security domain expert at a financial services institution stated that the security team was able to customize IriusRisk to provide an out-of-the-box solution for its network banks to use, ensuring that they have recognizable components and libraries.
- **Fostering a threat modeling culture.** The introduction of IriusRisk helped to build a formal practice around threat modeling within organizations. The director of cloud security engineering at a financial services institution explained, "Organizations need to mature and adapt to a threat modeling culture." The director of product security at a software sales firm added: "We didn't do any threat modeling on the product side prior to IriusRisk. But now, we've got formal practice around it. It's documented on our website. We have an internal-facing product security site. And it has threat modeling front and center as one of the first things that development teams should do."

FLEXIBILITY

There are multiple scenarios in which a customer might implement IriusRisk and later realize additional uses and business opportunities, including:

- **Eliminating vendor dependency.** The director of cloud security engineering at a financial service institution noted: "With IriusRisk, nothing is static. The tool can be updated via APIs — it's a completely API-driven method. We can also save the code, meaning that we are not dependent on the vendor."

Analysis Of Costs

🟩 Quantified cost data as applied to the composite

Total Costs

Ref.	Cost	Initial	Year 1	Year 2	Year 3	Total	Present Value
Ftr	Software license and support	$0	$214,725	$644,175	$2,147,250	$3,006,150	$2,340,841
Gtr	Implementation costs	$45,540	$0	$0	$0	$45,540	$45,540
Htr	Onboarding and training	$145,200	$233,200	$501,600	$74,800	$954,800	$827,944
Itr	Ongoing management	$0	$60,500	$121,000	$242,000	$423,500	$336,818
	Total costs (risk-adjusted)	$190,740	$508,425	$1,266,775	$2,464,050	$4,429,990	$3,551,143

SOFTWARE LICENSE AND SUPPORT

Evidence and data. IriusRisk charged annual software license and support fees of nearly $215,000 for Year 1, increasing to just under $644,000 in Year 2 and then nearly $2.15 million in Year 3.

Modeling and assumptions. Forrester models this cost using data provided by IriusRisk. For the composite organization, Forrester assumes:

- One hundred licenses in Year 1, which increase to 300 in Year 2 and 1,000 in Year 3.
- The cost per license is $2,150, which includes support fees.

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

- Difference in customer size and industry.
- License fee changes over time.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $2.3 million. This comprises 70% of the total costs.

Software License And Support

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Number of licenses	Composite		100	300	1,000
F2	License fee	IriusRisk		$2,045	$2,045	$2,045
Ft	Software license and support	F1*F2	$0	$204,500	$613,500	$2,045,000
	Risk adjustment	↑5%				
Ftr	Software license and support (risk-adjusted)		$0	$214,725	$644,175	$2,147,250
	Three-year total: $3,006,150			**Three-year present value: $2,340,841**		

IMPLEMENTATION COSTS

Evidence and data. IriusRisk Automated Threat Modeling Platform can either be deployed as a SaaS product or on-premises; half of the interviewed organizations deployed it as a SaaS solution. Prior to implementing IriusRisk, customers typically tested the product and/or completed a proof of concept. The implementation included the initial configuration and the rollout to the rest of the teams. The implementation phase varied across interviewees' organizations, with resources ranging from teams of three to six security architects and teams of three to 50 developers.

- Several interviewees noted that when they first installed IriusRisk, a few members of the security group were selected to conduct a proof of concept. Afterward, the tool was rolled out to all security champions within the organization. The principal software architect at a software sales company added, "Rolling the proof of concept out to all the rest of the teams took three months."

- In terms of team involvement, the security domain expert at a financial services institution shared that a total of three software security resources were involved in the upfront testing of the IriusRisk platform, with support from IriusRisk's customer success specialists. The time involvement was 3 hours per week over a course of three months.

- The principal software architect also shared: "During the implementation phase, the security champions were responsible for using [IriusRisk] and creating the architecture diagram for triaging the list of countermeasures that were being provided from IriusRisk, and then acting on fixing those. Occasionally, they would pull in one or two developers to help triage the findings."

  Modeling and assumptions. For the composite organization, Forrester assumes:

- A team of five senior security architects and 10 senior software developers.

- An implementation period of three months, during which both the senior security architects and senior software developers spend 3 hours per week per resource on the initial configuration and rolling out the concept, which totals 540 hours of effort.

- The average fully loaded hourly rate of a senior security architect is $100.

- The average fully loaded hourly rate of a senior software developer is $65.

Risks. Risks that could impact the magnitude of this cost include:

- The level of implementation effort varies across organizations, depending on the size of the product portfolio requiring threat modeling.

- The security resources' skill sets and familiarity with threat modeling.

- The time and efficiency of the implementation phase depends on the decision-making strategy of introducing (automated) threat modeling in an organization. The principal software architect stated: "The implementation of IriusRisk wasn't a top-down driven initiative. This was an initiative from within our [security] group, so we essentially had more time to work on it. It wasn't being driven in the same way as a top-down strategy. Everything was carried out time-permitting. That's why it also took three to six months."

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $46,000.

Implementation Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	Senior software security architects to roll out the concept	Interviews	5			
G2	Time per senior software security architect (hours)	Interviews	36			
G3	Fully loaded hourly rate of senior security architect	TEI standard	$100			
G4	Senior software developers to roll out the concept	Interviews	10			
G5	Time per senior software developer (hours)	Interviews	36			
G6	Fully loaded hourly rate of senior software developer	TEI standard	$65			
Gt	Implementation costs	(G1*G2*G3)+(G4* G5*G6)	$41,400	$0	$0	$0
	Risk adjustment	↑10%				
Gtr	Implementation costs (risk-adjusted)		$45,540	$0	$0	$0
	Three-year total: $45,540		Three-year present value: $45,540			

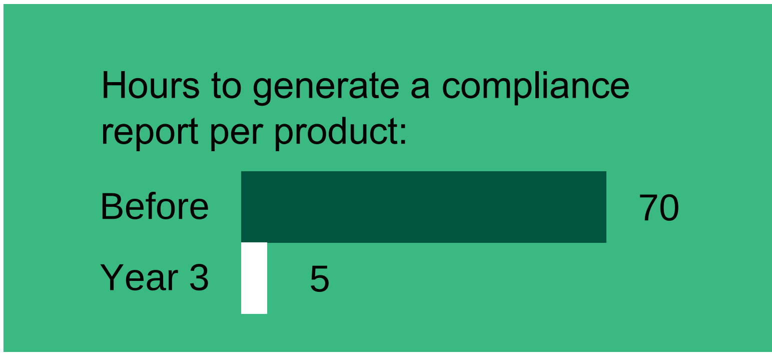
ONBOARDING AND TRAINING

Evidence and data. All interviewees noted the relevance of training and onboarding before starting to use IriusRisk Automated Threat Modeling Platform. Employees within the product security team attended an educational program, and software security architects learned how to customize the tool. The interviewees shared that:

- The training was deployed as a train-the-trainer type of education program, which usually took place virtually. SSG employees were the first users to receive the training, so they could train their colleagues and pass on their knowledge. The director of cloud security engineering at a financial services organization shared that during the initial training, around 25 to 30 employees were involved from the SSG. The session was a full one-day course.
- The director of cloud security engineering added that after the initial training of the SSG employees, they were able to train and onboard 1,000 developers over the course of the first year. This was a crucial step to scale their threat modeling activities across subsidiaries within the organization.
- All interviewees noted that IriusRisk's education program included training on the customization of the threat modeling platform based on each organization's needs. The director of product security at a software sales firm explained that this included customizing the workflow of a threat model, creating the custom fields, setting up initial security standards, and adding threats to the library.
- Moreover, the director of product security added, "There is also an ongoing security champion training in the form of a 60-minute workshop on how to threat model."
- During the onboarding phase, there are regular check-in calls with IriusRisk's customer success team. As the security domain expert at a financial institution stated, "Ten people from the security software group meet every second week for 60 minutes to discuss new features."

Hours to generate a compliance report per product:

Before IriusRisk	With IriusRisk (Y3)
70	**5**



Modeling and assumptions. For the composite organization, Forrester assumes that:

- Based on the train-the-trainer concept, a group of 100 security employees and 100 senior software developers attend the initial training. The duration of the initial training is 8 hours.
- In Year 1, the training is extended to 50 security employees and 200 senior software developers. In Year 2, an additional group of 30 security employees and 700 senior software developers are trained. The steep increase in the number of software developers who receive training in Year 2 is in line with the composite organization's extension in the number of IriusRisk licenses. To manage the implementation of countermeasures of 1,000 threat models in Year 3, a total of 1,000 trained senior software developers are needed.

- New employees within the SSG as well as software developers need to be onboarded; the duration of the training is 8 hours per employee.
- There are 10% new employees per year, which is a total of five security architects, 15 security champions, and 100 developers each year.

Risks. Risks that could affect the magnitude of this cost include:

- The product portfolio and the customization needs: Some organizations may need additional training sessions when initially setting up the tool.
- New employees requiring more than a full one-day course of training to become familiar enough with IriusRisk.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $828,000. This comprises 20% of the total costs.

Onboarding And Training

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
H1	Initial train-the-trainer training: senior software security architects and security champions	Interviews	100	50	30	
H2	Initial training time per software senior security architect (hours)	Interviews	8	8	8	
H3	Initial training: senior software developers	Interviews	100	200	700	
H4	Initial training time per senior software developer (hours)	Interviews	8	8	8	
H5	Total time for initial training	(H1*H2*H10)+ (H3*H4*H11)	$132,000	$144,000	$388,000	
H6	Onboarding: senior software security architects and senior security champions	Composite	0	20	20	20
H7	Onboarding time for senior software security architects and senior security champions (hours)	Interviews	0	8	8	8
H8	Onboarding: senior software developers	Composite	0	100	100	100
H9	Onboarding time for senior software developers (hours)	Composite	0	8	8	8
H10	Fully loaded hourly rate of senior security architect/senior security champion	TEI standard	$100	$100	$100	$100
H11	Fully loaded hourly rate of senior software developer	TEI standard	$65	$65	$65	$65
H12	Total time for onboarding	(H6*H7*H10)+ (H8*H9*H11)	$0	$68,000	$68,000	$68,000
Ht	Onboarding and training	H5+H12	$132,000	$212,000	$456,000	$68,000
	Risk adjustment	↑10%				
Htr	Onboarding and training (risk-adjusted)		$145,200	$233,200	$501,600	$74,800
	Three-year total: $954,800			Three-year present value: $827,944		

ONGOING MANAGEMENT

Evidence and data. All interviewees explained how the ongoing management and maintenance of the IriusRisk Automated Threat Modeling Platform was managed by a "tool champion" who typically had a software development background. The tool champion usually managed user and team access to the tool (i.e., integrated single sign-on) and to projects; the configuration and maintenance of integrations with DevOps tools; and the setup of custom dashboards. Additionally, the tool champion managed the standardization of libraries and the description of components. All interviewees noted that the number of dedicated resources managing the tool depended on the number of threat modeling licenses.

- The principal software architect at a software sales company noted: "There is half an FTE that handles the management and maintenance on an ongoing basis. It's generally one individual who is managing the tool as part of their responsibilities, because it isn't every day that the system needs to be updated or that new accounts must be created."

Modeling and assumptions. For the composite organization, Forrester assumes that:

- In Year 1, half an FTE is responsible for managing the IriusRisk platform, which increases to one FTE in Year 2 and two FTEs in Year 3.
- Tool champions manage the platform on a full-time basis.
- The average fully loaded annual salary for a software developer is $110,000.

Risks. Risks that could affect the magnitude of this cost include:

- Tool champions might require occasional guidance by SSG employees, especially in cases when an organization scales its threat modeling activities across its lines of business and subsidiaries.

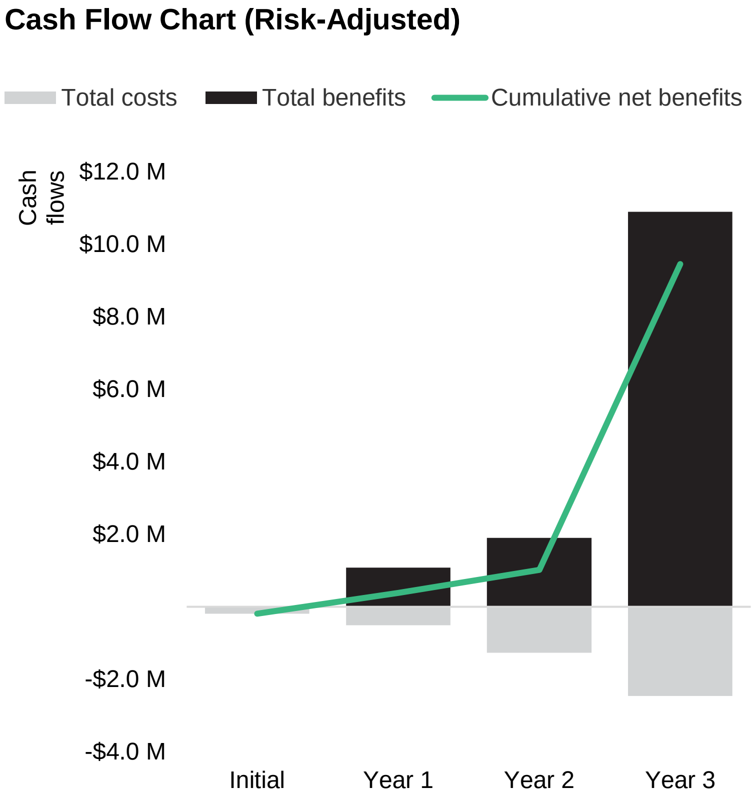
Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $337,000.

Ongoing Management

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
I1	Number of tool champions (FTEs)	Interviews	0	0.5	1.0	2.0
I2	Fully loaded annual salary for a software developer	TEI standard	0	$110,000	$110,000	$110,000
It	Ongoing management	I1*I2	$0	$55,000	$110,000	$220,000
	Risk adjustment	↑10%				
Itr	Ongoing management (risk-adjusted)		$0	$60,500	$121,000	$242,000
	Three-year total: $423,500		Three-year present value: $336,818			

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS



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	($190,740)	($508,425)	($1,266,775)	($2,464,050)	($4,429,990)	($3,551,143)
Total benefits	$0	$1,082,779	$1,902,465	$10,900,260	$13,885,504	$10,746,157
Net benefits	($190,740)	$574,354	$635,690	$8,436,210	$9,455,514	$7,195,014
ROI						203%
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: Supplemental Material

Related Forrester Research

"Optimize Your Security Tech Stack," Forrester Research, Inc., August 17, 2022

"Role Profile: Security Architect," Forrester Research, Inc., October 4, 2022

Appendix C: 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.

[2] Source: "BSIMM13 Trends & Insights Report 2022: Software Security Assessment Report," Synopsys.

[3] Source: Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q4 2020.

FORRESTER®