FORRESTER®

The Total Economic Impact™ Of The Securonix SIEM Platform

Cost Savings And Risk Mitigation Enabled By The Securonix SIEM Platform

A FORRESTER TOTAL ECONOMIC IMPACT STUDY
COMMISSIONED BY SECURONIX, JULY 2025

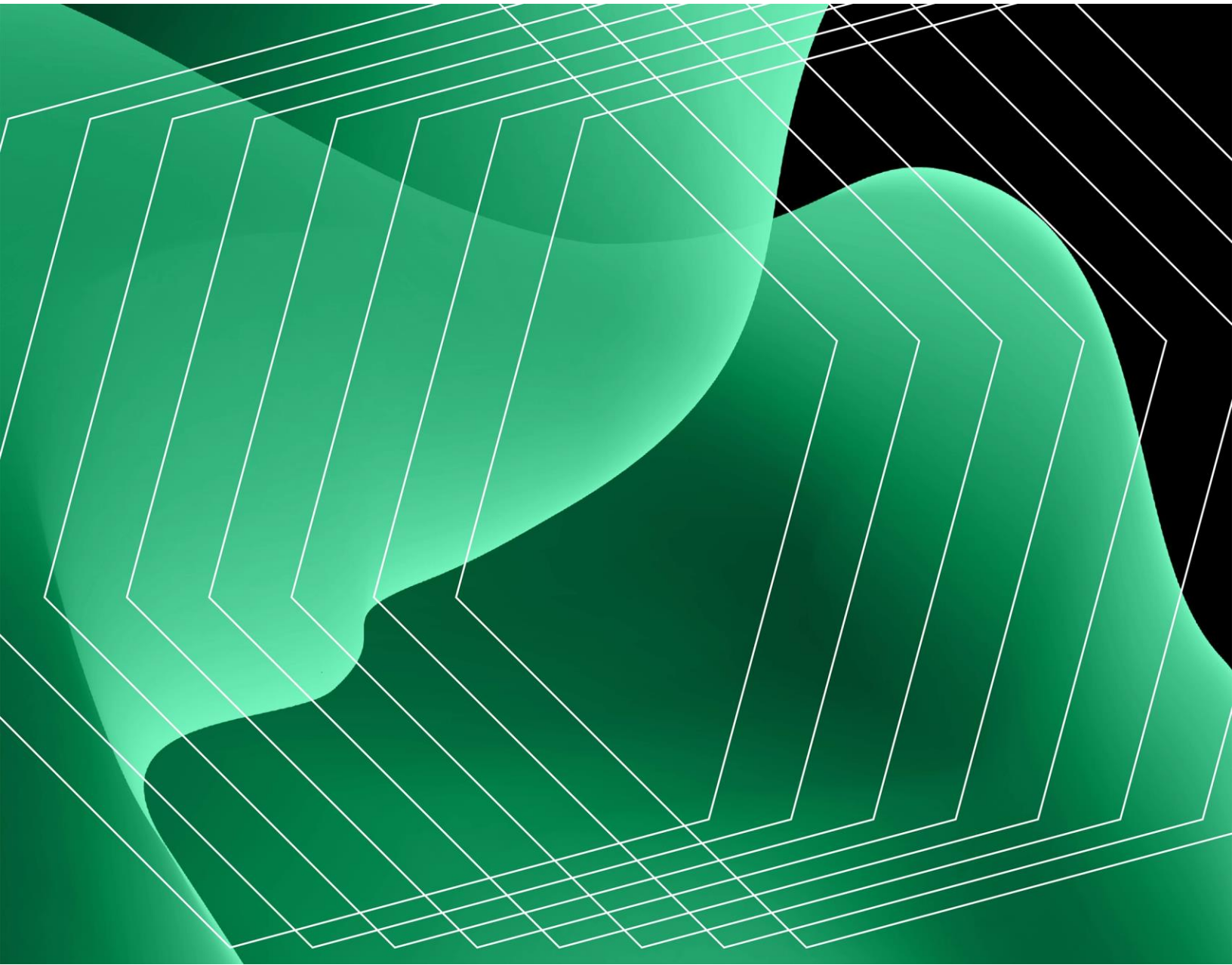


Table Of Contents

Consulting Team:

Nick Mayberry

ABOUT FORRESTER CONSULTING

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

Executive Summary

Security information and event management (SIEM) solutions provide security operations teams with a place to centralize security-relevant business data for several use cases, including providing visibility and sufficient data analysis to develop security insights; tracking and reporting on security posture for regulatory compliance; continuously building new detections on increasingly large datasets (sometimes with the help of machine learning); and alerting, investigating, and responding to incidents.

The Securonix SIEM platform offers all of the above while also providing important data features like federated search and data pipeline management, which serve to improve analysts' experience. These data features are joined by additional integrations including user entity and behavior analytics (UEBA) for protection against insider threats and security orchestration, automation, and response (SOAR) to automate threat detection, investigation, and response (TDIR) workflows. Securonix offers multiple iterations of these pairings for flexibility, all from a single interface.

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

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed five decision-makers with experience using the Securonix SIEM platform. For the purposes of this study, Forrester aggregated the experiences of the interviewees and combined the results into a single composite organization, which is a growing, regulated organization with 4,500 employees and $3 billion in annual revenue.

Return on investment (ROI)
193%

Net present value
$2.28M

Interviewees said that prior to using the Securonix SIEM platform, their organizations faced climbing security operations center (SOC) costs from team and technology expansion in

response to increasing security attacks and attack vectors. Prior SIEM solutions suffered from performance issues and incomplete functionality, limiting the ability to search security data effectively and to detect and respond to insider threats. These solutions also had more rigid deployment requirements, running only on-premises or in the cloud.

After the investment in the Securonix SIEM platform, the interviewees lowered their overall cost of operating a SOC. They avoided additional hires, up-leveled junior security analysts to the effectiveness of midtier security analysts, and reduced the time it took to run TDIR and generate use cases via federated search capabilities. They lowered their security-related risk costs by reducing cyber insurance premiums and the likelihood of security incidents, while benefiting from regulatory savings in the form of avoided penalties and increased audit process efficiency.

KEY FINDINGS

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

- **SOC efficiency increase of 58%.** The Securonix SIEM platform leverages several tools that reduce the composite's false positives by 80%, allowing it to avoid increasing its SOC team size, and the associated costs, by 60%. The platform's ease of use enables the composite to leverage Level 1 security analysts to do the work of Level 2 analysts, providing higher value at a 45% cost reduction. It also reduces search query times by 60% and use-case development times by 40%. When combined with technology savings, these provide the composite with a three-year present value of $1.8 million.
- **Risk savings of 19%.** The Securonix SIEM platform enables the composite to better secure its environment from attacks and to prove it with data. This contributes to the composite's ability to lower its cyber insurance premium rates by 10% and, especially thanks to the addition of UEBA, reduce its risk of security incidents by 80%. Combined, these savings provide the composite with a three-year present value of $1 million.
- **Compliance savings of 15%.** The Securonix SIEM platform helps the composite to better track, search, and analyze its security incident data. With these capabilities, the composite can better prove its compliance to regulators and avoid 15% of penalties while also shortening audit log collection time by 40%. Combined, these savings provide the composite with a three-year present value of $622,000.

> "We chose Securonix because of its scalability, its ease of use, and its help in avoiding further SOC costs. We ended up investing 70% of the budget we had planned for SIEM and got UEBA as well. The solution was implemented in 45 days instead of the usual six months."
>
> **VICE PRESIDENT OF INFORMATION SECURITY, HEALTHCARE**

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

- **Improved analyst experience.** By reducing the number of false positives, enabling junior employees to provide the value of midtier employees, improving the time spent running TDIR processes, and reducing the time to build use cases, the Securonix SIEM platform improves analysts' experience, efficiency, and productivity, enabling them to work on higher value tasks and make more strategic decisions.
- **Skilled implementation and support.** Securonix provides the composite with a high level of service during implementation and demonstrates its skill in complex deployments and ongoing support, so the composite's SOC team and security engineers feel well-attended to.

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

- **Securonix fees.** Based on the volume of data ingested by the Securonix SIEM platform as well as specific features and add-ons, the composite pays $60,000 for up-front implementation services and $170,000 annually for licensing.
- **Implementation and management effort.** Similarly, the composite incurs implementation effort costs for one security engineer over six months. On an ongoing basis, the composite needs one Level 3 security analyst to manage the platform full-time. Training takes each team member 40 hours, and there is an attrition rate of one team member per year.

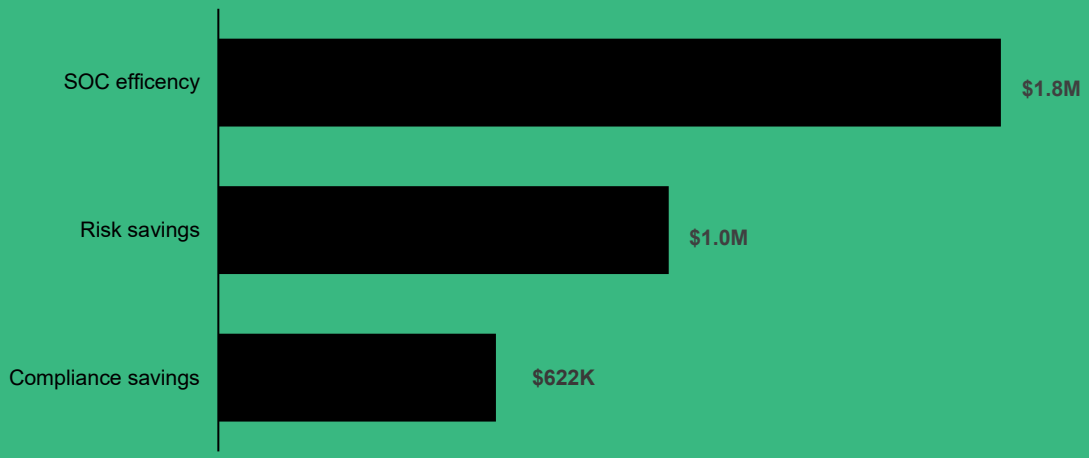
The financial analysis that is based on the interviews found that a composite organization experiences benefits of $3.47 million over three years versus costs of $1.18 million, adding up to a net present value (NPV) of $2.28 million and an ROI of 193%.

Total reduced SOC cost from efficiency gains and avoided costs

58%

ROI	BENEFITS PV	NPV	PAYBACK
193	$3.47M	2.28M	< 6 months

Benefits (Three-Year)



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 the Securonix SIEM 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 the Securonix SIEM platform can have on an organization.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Securonix 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 the Securonix SIEM platform.

Securonix 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.

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

1. **Due Dilligence**
   Interviewed Securonix stakeholders and Forrester analysts to gather data relative to the Securonix SIEM platform.
2. **Interviews**
   Interviewed five representatives at organizations using the Securonix SIEM platform to obtain data about costs, benefits, and risks.
3. **Composite Organization**
   Designed a composite organization based on characteristics of the interviewees' organizations.
4. **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.
5. **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 Securonix SIEM Platform Customer Journey

Drivers leading to the SIEM Platform investment

Interviews			
Role	**Industry**	**Region**	**Total Employees**
Director of information security	Financial services	North America	100
Senior technical analyst Senior analyst	Healthcare	North America	10,000
VP of information security	Healthcare	EMEA	50,000
Senior manager of cybersecurity engineering	Pharmaceuticals	Global	100,000

KEY CHALLENGES

Before investing in the Securonix SIEM platform, the interviewees' organizations were either too immature in their security practices to require a SIEM or were using a legacy SIEM with functional shortcomings.

The interviewees noted how their organizations struggled with common challenges, including:

- **Increasing SOC costs.** Customers noted that as their organizations matured, the number of false positives and potential real threats increased. Maintaining 24/7 operations in the face of these threats required investment in the form of team expansion, managed services expansion, or additional technological investment with the added senior resources necessary for managing these technologies. Customers viewed Securonix as one means to manage these increasing costs by reducing false positives while being easy for junior security teams members to use effectively.
- **Missing or broken functionality.** Customers with prior SIEM solutions noted that they suffered from missing or broken functionality. For example, the director of information security in the financial services industry noted that his organization's prior SIEM lacked the necessary integrations to make UEBA effective. The senior manager of cybersecurity

engineering at the pharmaceuticals company noted that their prior SIEM solution's search was broken, with many attempts to investigate threats timing out as searches took too long.

- **Inflexible deployment.** Lastly, interviewees noted that their prior SIEM solutions had inflexible deployment. Customers had to choose between on-premises or cloud deployments, if regulations permitted such a choice, which would then limit their future options. On-premises deployments meant potentially higher resource costs to manage, limited or labor-intensive integrations, and a lack of cloud-application monitoring, while cloud-only deployments eased the burden of integrations but limited control over data and resource provisioning via quotas.

> "Securonix's flexibility was integral to our expansion. Scaling with on-premises deployments requires more labor, more hardware, and more network bandwidth. The Securonix SIEM platform's ability to work in hybrid environments enabled us to scale effectively while keeping costs low and meeting regulatory requirements."
>
> VP OF INFORMATION SECURITY, HEALTHCARE

> "Securonix was a great choice for us because it met all the on-premises capability we needed while providing us the flexibility to leverage cloud-based federated search to resolve the broken search of our legacy SIEM."
>
> SENIOR MANAGER OF CYBERSECURITY ENGINEERING, PHARMACEUTICALS

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 five 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 is a growing regional organization in a regulated industry and has global scaling ambitions. It currently employs 4,500 workers and generates $3 billion in revenue annually. Five of the company's workers are a part of a lean SOC team that, among other responsibilities, manages a legacy SIEM solution. However, this solution is too inflexible to meet the shifting platform demands of the business toward a hybrid environment.

Deployment characteristics. The composite begins using the Securonix SIEM platform after a six-month implementation period. The composite uses the platform's 90-day hot storage option, the standard-level SIEM option, basic threat modeling, and the built-in SOAR offering. Although the SIEM platform's ease of use benefits the organization, the composite still experiences an efficacy ramp-up during the first year as SOC team members become proficient.

MODEL ASSUMPTIONS

Ref.	Assumption	Source	Initial	Year 1	Year 2	Year 3
R1	Total SOC team size	Composite	5	5	5	5
R2	Total Level 1 security professionals	Composite	2	2	2	2
R3	Total Level 2 security professionals	Composite	2	2	2	2
R4	Total Level 3 security professionals	Composite	1	1	1	1
R5	Fully burdened annual salary for a Level 1 security professional	Composite	$110,000	$110,000	$110,000	$110,000
R6	Fully burdened annual salary for a Level 2 security professional	Composite	$160,000	$160,000	$160,000	$160,000
R7	Fully burdened annual salary for a Level 3 security professional	Composite	$190,000	$190,000	$190,000	$190,000
R8	Fully burdened annual salary for an average SOC team member	(R2*R5+R3*R6+R4*R7)/R1	$146,000	$146,000	$146,000	$146,000

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	SOC efficiency	$565,322	$824,643	$824,643	$2,214,608	$1,815,018
Btr	Risk savings	$262,730	$501,460	$501,460	$1,265,650	$1,030,029
Ctr	Compliance savings	$121,085	$290,171	$362,171	$773,427	$621,993
	Total benefits (risk-adjusted)	$949,137	$1,616,274	$1,688,274	$4,253,684	$3,467,040

SOC EFFICIENCY

Evidence and data. The interviewees shared that Securonix helped reduce the cost of their SOC with built-in functionality that reduced false positives, ease of use that up-leveled junior employees, and efficient federated search capabilities for TDIR.

The Securonix SIEM platform has built-in whitelisting capabilities, threat intelligence integration, UEBA, and SOAR capabilities. Interviewees noted that combined, these features reduced the number of false positives requiring investigation, which in turn helped their organizations avoid additional SOC hires. The VP of information security at the EMEA healthcare company said: “Securonix enabled us to whittle down 1.4 billion incidents generated monthly to between 200 and 250 incidents. This saves us from having to hire at least seven to eight additional team members.”

Interviewed customers also shared that Securonix was easy to use, with an intuitive user interface, customization capabilities, and streamlined workflows. This enabled junior team members to up-level their work and provide the same level of value as more experienced team members. The VP of information security at the EMEA healthcare company noted, “Securonix is so easy to use that our junior SOC team members can be quickly trained and ramped to do the

work of midtier resources, providing us the value of these more experienced resources at lower cost."

Interviewees reported further cost reduction due to Securonix's federated search capabilities, which dramatically improved the speed of their search queries and reduced the SOC's time spent investigating threats. The senior manager of cybersecurity engineering at the pharmaceuticals company shared: "On our prior SIEM, our queries would time out 80% of the time. This would then force the underlying infrastructure to go down multiple times, which would eventually bring the entire application down. With Securonix, our query time-out rate is down to less than 5%."

The VP of information security at the EMEA healthcare company also noted that cloud-based federated search improved their speed in building use cases. He said: "What matters to me is how quickly we're getting out logs and how quickly we can build and implement use cases to prevent future incidents. Our prior SIEM took a very long time to collate data to get to the necessary analysis for use cases. Securonix's cloud-based infrastructure enables this for us in at least half the time."

Additionally, interviewed customers with a prior SIEM technology found that the Securonix SIEM platform could replace it, removing the need to pay for and manage that solution while providing more capabilities and value to their organization

Modeling and assumptions. For the composite organization, Forrester models**:**

- A SOC team of four employees that includes:
    - Two Level 1 security analysts with an average fully burdened annual salary of $110,000 each.
    - Two Level 2 security analysts with an average fully burdened annual salary of $160,000 each.
- One Level 3 security analyst with an average fully burdened annual salary of $190,000.
- Compared to the organization's prior SIEM, Securonix reduces false positives by 80%.
- The reduction in false positives allows the composite to avoid 60% of its SOC team size in additional hires (three FTEs).
- Securonix's ease of use enables the composite's Level 1 security analysts to provide the value of Level 2 security analysts, saving the company the 45% higher wage it would have to pay new Level 2 hires for the same value-add.

- The SOC previously spent 1,800 hours annually on search queries and 84 hours annually on building use cases. With Securonix, the SOC's time spent searching decreases by 60%, and its spent time building use cases decreases by 40%.
- The composite achieves 50% of these benefits in Year 1 due to the SOC team ramping up. In Years 2 and 3, the composite receives 100% of the benefit.
- The composite decommissions its legacy SIEM in favor of Securonix, saving $150,000 annually on licensing costs and $190,000 annually on management costs.

Risks. The amount of SOC cost reduction will vary with:

- The current SOC team size and its projected growth due to security alert and incident increases.
- The number of Level 1 security analysts able to level up to Level 2 security analyst work.
- The prior time spent conducting search queries and building use cases.
- The average fully burdened annual salary for a SOC team member.

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.

Reduction in noise from false positives
80%

Avoided SOC headcount
60%

SOC Efficiency					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Total SOC team size	R1	5	5	5
A2	Reduction in false positives	Interviews	80%	80%	80%
A3	Avoided hires	Interviews	60%	60%	60%
A4	Fully burdened annual salary for a SOC team member	R8	$146,000	$146,000	$146,000
A5	**Subtotal: Avoided costs from reduced false positives**	**A1*A3*A4**	**$438,000**	**$438,000**	**$438,000**
A6	Level 1 security analysts	R2	2	2	2
A7	Added value from Securonix ease of use	Interviews	45%	45%	45%
A8	Fully burdened annual salary for a Level 1 security analyst	Composite	$110,000	$110,000	$110,000
A9	**Subtotal: Upskilling of security team**	**A6*A7*A8**	**$99,000**	**$99,000**	**$99,000**
A10	Prior annual hours spent on queries	Interviews	1,800	1,800	1,800
A11	Query time reduction from Securonix	Interviews	60%	60%	60%
A12	Prior annual hours spent building use cases	Interviews	84	84	84
A13	Use-case time reduction from Securonix	Interviews	50%	50%	50%
A14	Fully burdened hourly rate for a SOC team member	R8/2,080	$70	$70	$70
A15	Productivity recapture rate	Composite	50%	50%	50%
A16	**Subtotal: Productivity gain to threat detection, investigation, and response**	**(A10*A11+A12*A13)*A14*A15**	**$39,270**	**$39,270**	**$39,270**
A17	Benefit received due to ramp-up	Interviews	50%	100%	100%
A18	Reduced cost of prior SIEM	Composite	$150,000	$150,000	$150,000
A19	Reduced cost to manage prior SIEM	1*R7	$190,000	$190,000	$190,000
At	SOC efficiency	(A5+A9+A16)*A17 +A18+A19	$628,135	$916,270	$916,270
	Risk adjustment	↓10%			
Atr	SOC efficiency (risk-adjusted)		$565,322	$824,643	$824,643
	Three-year total: $2,214,608			**Three-year present value: $1,815,018**	

RISK SAVINGS

Evidence and data. Securonix helped interviewees save on security risk-related costs by reducing the cost of their cyber insurance policies and the risk of security incidents.

Regarding cyber insurance, customers noted that the ability to gather their organization's threat data in one place and easily access and search that data enabled them to demonstrate a detailed view of their security posture to potential insurance providers. They could also leverage Securonix's data ingestion, access, and search to build strategic plans for additional security improvements, which further assuaged insurance providers' concerns about cybersecurity incident risks. One customer reported saving 26% on their policy costs after implementing Securonix.

In security incident risk, interviewed customers noted that the additional information Securonix's SIEM platform contains out of the box, including built-in use cases, industry-specific use cases, threat intelligence data, UEBA, and SOAR, all helped to reduce the risk of a security incident by up to 80% compared to their prior environment.

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

- A prior annual cost of cyber insurance of $300,000.
- A conservative 10% reduction in policy costs due to the Securonix SIEM platform.
- An average unauthorized access incident cost of $1,147,740, composed of an average incident cost multiplied by the percentage of incidents involving external access.[1]
- A likelihood of an unauthorized access incident of 65%.[2]
- A reduction in unauthorized access incident risk of 80%, with much of this due to the inclusion of UEBA.
- A benefit ramp of 50% in Year 1, with 100% of benefits achieved by Year 2.

Risks. Risk savings may vary with:

- The difference in visibility into the customer's security environment and understanding of attack vectors before and after implementing Securonix.
- The ability of the customer to negotiate a better rate with their cyber insurance provider.
- The industry and size of the organization, which impact the cost of a security incident, annual breakdown of incident types, and the likelihood of any type of incident.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1 million.

Reduction in risk of an unauthorized access incident
80%

Risk Savings					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Prior cost of cyber insurance	Composite	$300,000	$300,000	$300,000
B2	Percentage savings with Securonix	Interviews	10%	10%	10%
B3	**Subtotal: Reduced insurance premium**	**B1*B2**	**$30,000**	**$30,000**	**$30,000**
B4	Average cost of unauthorized access incident	Forrester research	$1,147,740	$1,147,740	$1,147,740
B5	Likelihood of unauthorized access incident	Forrester research	65%	65%	65%
B6	Risk reduction from Securonix	Interviews	80%	80%	80%
B7	Benefit received due to ramp-up	A17	50%	100%	100%
B8	**Subtotal: Reduced risk of unauthorized access**	**B4*B5*B6*B7**	**$298,412**	**$596,825**	**$596,825**
Bt	Risk savings	B3+B8	$328,412	$626,825	$626,825
	Risk adjustment	↓20%			
Btr	Risk savings (risk-adjusted)		$262,730	$501,460	$501,460
	Three-year total: $153,900			**Three-year present value: $150,400**	

COMPLIANCE SAVINGS

Evidence and data. Securonix further benefited the interviewees' organizations by helping avoid or reduce costs associated with regulations and compliance. Customers reported that Securonix helped avoid regulatory penalties and improved their SOC team's efficiency in responding to audits and regulatory requests.

Regarding avoided regulatory penalties, the VP of information security at the EMEA healthcare company shared: "Securonix made it easy for us to have all our events and regulatory due diligence in one place, proving to auditors and regulators that we are acting in accordance with regulations. In the past couple of years, we protected ourselves against eight or nine incidents which could have easily resulted in $2 million in regulatory penalties if not for Securonix."

The same customer shared that Securonix reduced the time their SOC team spent on audits thanks again to Securonix's use of cloud-based federated search. He said: "As a healthcare provider, we undergo around 10 audits each year. Log collection for these audits was always burdensome, taking time from our team that could have been used on strengthening our security posture. Securonix has reduced the time the team spends on log collection for our audits by 70%, allowing them more time to advance our strategy."

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

- A $12 million potential annual cost of regulatory penalties.
- A 25% potential of receiving these regulatory penalties before Securonix.
- A 10% to 15% reduction in the potential for receiving these regulatory penalties due to Securonix.
- Four annual audits.
- Thirty-two hours to collect logs for each audit before Securonix.
- A conservative 40% reduction in log collection time with Securonix.
- The composite solely uses their Level 1 resources for audit log collection.
- A benefit ramp of 50% in Year 1, with 100% of benefits achieved by Year 2.

Risks. Total regulatory savings will vary with:

- The total potential annual penalties and the likelihood of receiving these penalties.

- The total number of hours required for audit log collection and the mix of resources used to conduct audit log collection.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $622,000.

Reduction in potential for regulatory penalty
15%

Reduction in time spent on audit log collection
40%

Compliance Savings					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Potential cost of regulatory penalty	Interviews	$12,000,000	$12,000,000	$12,000,000
C2	Potential for receiving regulatory penalty	Interviews	25%	25%	25%
C3	Reduction in potential for penalty	Interviews	10%	12%	15%
C4	**Subtotal: Reduced cost of penalties**	**C1*C2*C3**	**$300,000**	**$360,000**	**$450,000**
C5	Number of audits annually	Interviews	4	4	4
C6	Prior hours spent on log collection per audit	Composite	32	32	32
C7	Reduced log collection time per audit with Securonix	Interviews	40%	40%	40%
C8	Fully burdened hourly rate for a Level 1 security professional	R5/2,080	$53	$53	$53
C9	**Subtotal: Audit process efficiency**	**C5*C6*C7*C8**	**$2,714**	**$2,714**	**$2,714**

C10	Benefit received due to ramp-up	A17	50%	100%	100%
Ct	Compliance savings	(C4+C9)*C10	$151,357	$362,714	$452,714
	Risk adjustment	↓20%			
Ctr	Compliance savings (risk-adjusted)		$121,085	$290,171	$362,171
Three-year total: $773,427			**Three-year present value: $621,993**		

UNQUANTIFIED BENEFITS

Interviewees mentioned the following additional benefits that their organizations experienced but were not able to quantify:

- **Improved analyst experience.** Interviewed customers shared that Securonix improved their SOC teams' experience by reducing the number of false positives they had to investigate; improving the time spent running TDIR processes due to fast federated search, built-in use cases, and more efficient custom use-case building; and enabling junior employees to add more value than before. Combined, these benefits allowed SOC team members to think and act at a higher, strategic level rather than just triaging alerts.
- **Skilled implementation and support.** Interviewed customers praised Securonix for the support they received throughout their contract. Customers noted that Securonix's implementation team was very skilled and easily handled platform setup and deployment in a complex technological environment. They also shared feeling "spoiled" at the availability of Securonix's support team and that any issues were always resolved quickly.

> "Securonix helped reduce the number of false positives our SOC was investigating by 90%. Now, we only get those issues that make the most of our team's time, reducing alert fatigue and improving security analyst experience."
>
> **SENIOR TECHNICAL ANALYST, HEALTHCARE**

FLEXIBILITY

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

- **Improved visibility.** Customers noted that Securonix's platform improved visibility by ingesting more data thanks to its numerous cloud connectors and improving access to this data via fast federated search. This increased visibility led to an improved understanding of the organizations' security postures and bettered their leaderships' abilities to make effective, strategic security decisions.
- **Industry-specific use cases.** Customers also shared that Securonix has built-in use cases for responding to threats that are industry specific. Not only does this help to improve security posture and incident response from Day 1, but it also ensures that customers remain up to date with the shifting attack vectors and regulatory demands specific to their industries, while focusing on their daily work.

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

> "Before Securonix, we lacked visibility into our security posture and environment. The lack of visibility meant we were not able to draft a five-year strategic plan because we lacked understanding both at the industry level and at the organization-specific level. With Securonix, we understand our external threats, any internal threats (thanks to UEBA), and where there are gaps in our cybersecurity portfolio, enabling us to plan strategically for the first time."
>
> **VP OF INFORMATION SECURITY, HEALTHCARE**

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**
Dtr	Securonix fees	$66,000	$187,000	$187,000	$187,000	$627,000	$531,041
Etr	Implementation and management effort	$123,695	$212,080	$212,080	$212,080	$759,935	$651,107
	Total costs (risk-adjusted)	$189,695	$399,080	$399,080	$399,080	$1,386,935	$1,182,148

SECURONIX FEES

Evidence and data. Interviewed customers incurred fees associated with the Securonix SIEM platform implementation and ongoing platform use. Implementation fees depended on the complexity of the customer's IT environment and the particular options and add-ons for the platform as chosen by the customer.

The annual licensing fee is based on ingested gigabytes of data per day as well as any specific product configurations. The composite uses the platform's 90-day hot storage option, the standard-level SIEM option, basic threat modeling, and the built-in SOAR offering.

Modeling and assumptions. For the composite, Forrester models:

- Up-front implementation fees of $60,000.
- Annual licensing fees of $170,000.

Risks. The cost of Securonix fees may vary with:

- The amount of data ingested by the Securonix SIEM platform.
- The specific features and add-ons chosen by the customer.
- The complexity of the customer's IT environment.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $531,000.

Securonix Fees						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
D1	Implementation fees		$60,000	$0	$0	$0
D2	Licensing fees		$0	$170,000	$170,000	$170,000
Dt	Securonix fees	D1+D2	$60,000	$170,000	$170,000	$170,000
	Risk adjustment	↑10%				
Dtr	Securonix fees (risk-adjusted)		$66,000	$187,000	$187,000	$187,000
	Three-year total: $627,000			**Three-year present value: $531,041**		

IMPLEMENTATION AND MANAGEMENT EFFORT

Evidence and data. Interviewed customers incurred internal costs for implementation, management, and training related to the Securonix SIEM platform. Customers experienced implementation times between 45 days and one year, with the low end a greenfield deployment of the cloud-based solution and the high end an on-premises deployment with hybrid cloud storage into a very complex IT environment.

Customers also shared leveraging between one and two full-time, senior-level security analysts to manage the solution. All employees received an average of one week of training.

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

- The composite needs one security engineer to manage the Securonix implementation for six months at an average fully burdened annual salary of $202,500.
- The composite needs one Level 3 security analyst to manage the Securonix SIEM platform on an ongoing basis at an average fully burdened annual salary of $190,000.
- Each SOC team member receives 40 hours of training on the Securonix SIEM platform. There is an attrition rate of one team member each year, requiring new team member training for an additional 40 hours annually.

Risks. The cost of implementation and management effort will depend on:

- The complexity of the customer's security IT environment.
- The various features and add-ons selected by the customer.
- The total number of SOC team members requiring training and the ongoing attrition rate of the SOC team.

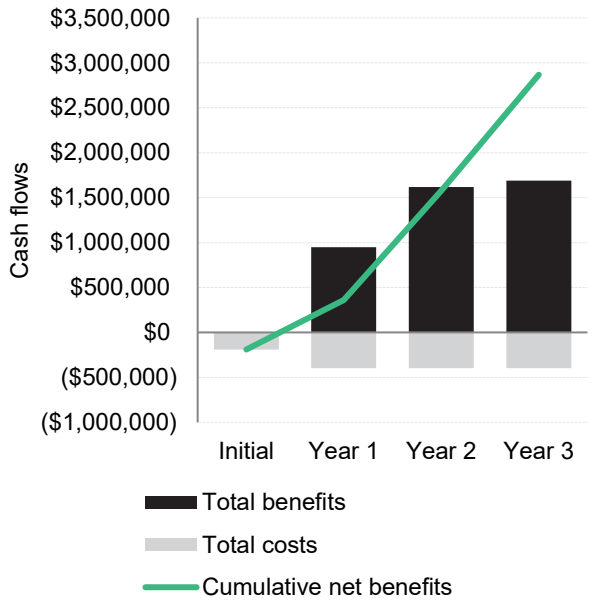
Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $651,000.

Implementation And Management Effort						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Security engineers assisting with implementation	Interviews	1	0	0	0
E2	Months spent on implementation	Interviews	6	0	0	0
E3	Fully burdened annual salary for a security engineer	Interviews	$202,500	$0	$0	$0
E4	Subtotal: Implementation effort cost	E1*E2/12*E3	$101,250	$0	$0	$0
E5	FTEs managing the solution	Interviews	0	1	1	1
E6	Subtotal: Management effort cost	E5*R7	$0	$190,000	$190,000	$190,000
E7	FTEs needing training	Composite	4	1	1	1
E8	Hours needed to train	Interviews	40	40	40	40
E9	Subtotal: Training effort cost	E7*E8*A14	$11,200	$2,800	$2,800	$2,800
Et	Implementation and management effort	E4+E6+E9	$112,450	$192,800	$192,800	$192,800
	Risk adjustment	↑10%				
Etr	Implementation and management effort (risk-adjusted)		$123,695	$212,080	$212,080	$212,080
	Three-year total: $759,935			**Three-year present value: $651,107**		

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)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($189,695)	($399,080)	($399,080)	($399,080)	($1,386,935)	($1,182,148)
Total benefits	$0	$949,137	$1,616,274	$1,688,274	$4,253,684	$3,467,040
Net benefits	($189,695)	$550,057	$1,217,194	$1,289,194	$2,866,749	$2,284,892
ROI						193%
Payback						<6 months

APPENDIX A: TOTAL ECONOMIC IMPACT

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

Total Economic Impact Approach

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

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

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

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

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.

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.

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 solution providers in communicating their value proposition to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of business and technology initiatives to both senior management and other key stakeholders.

[2] Regression analysis of the reported total cumulative costs of all breaches experienced by security decision-makers' organizations in the past 12 months. The composite organization's revenue is used as the input to the regression formula. Source: Forrester's Security Survey, 2024, "Using your best estimate, what was the total cumulative cost of all breaches experienced by your organization in the past 12 months?" Base: 1,660 global security decision-makers who have experienced a breach in the past 12 months.

FORRESTER®