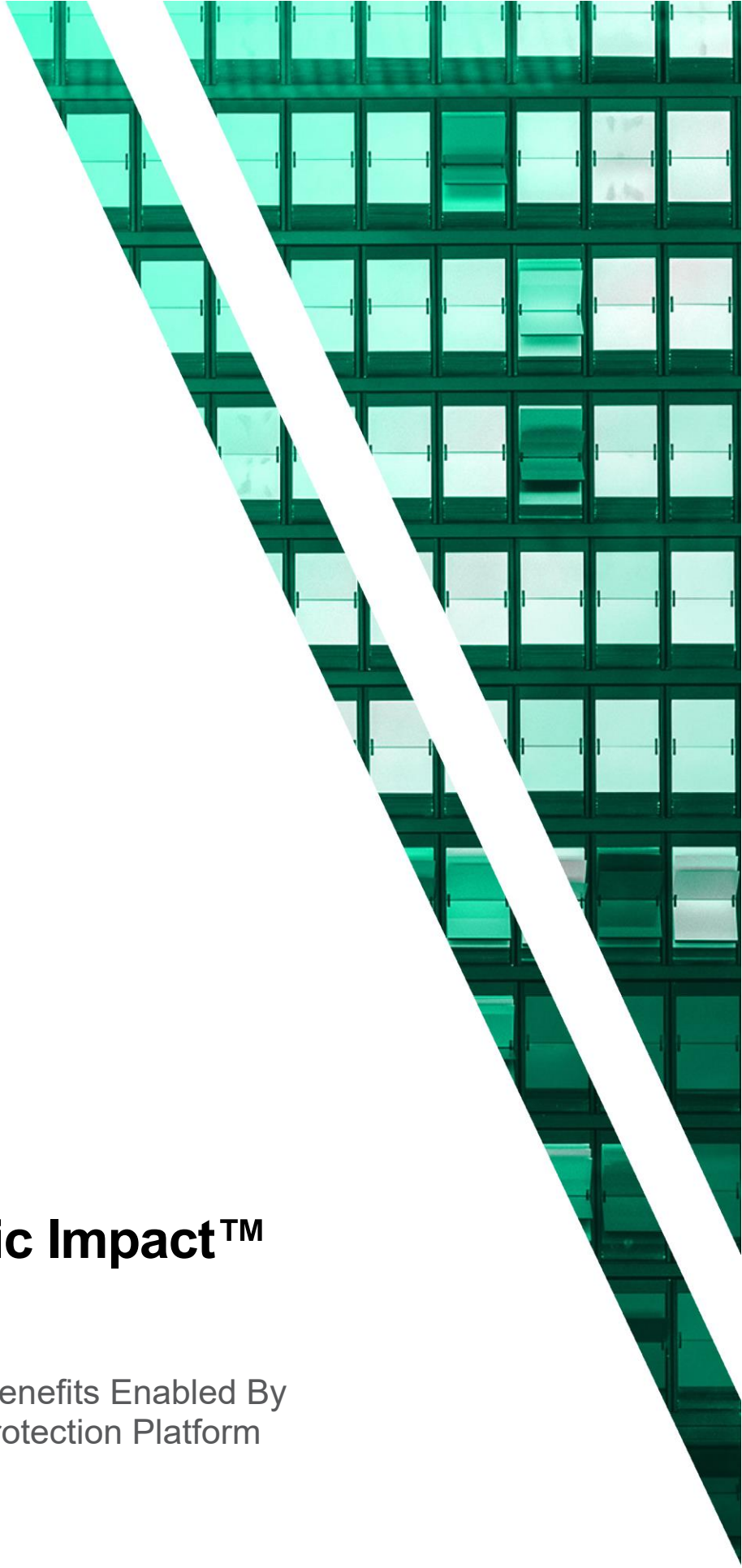
FORRESTER®



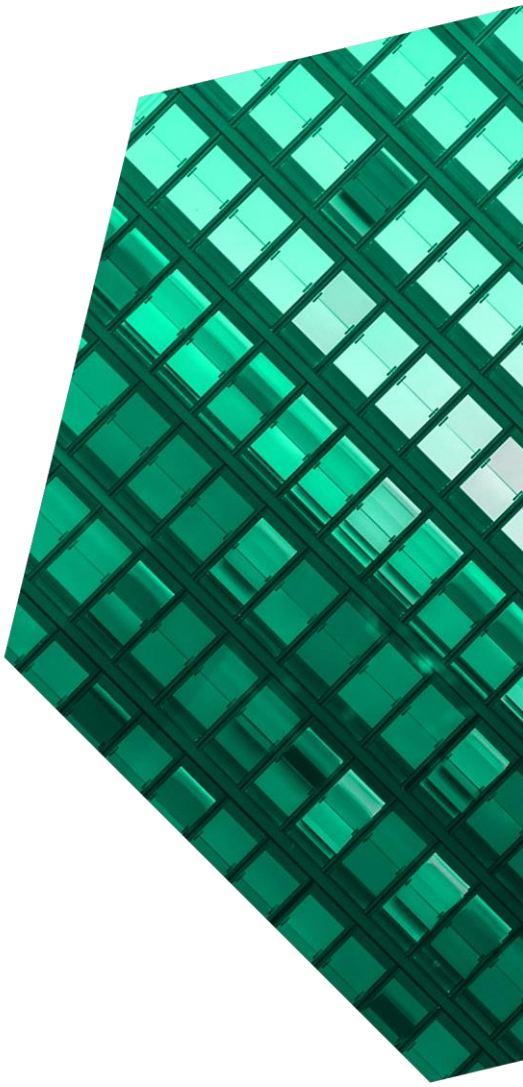
The Total Economic Impact™ Of CybelAngel

Cost Savings And Business Benefits Enabled By CybelAngel's External Risk Protection Platform

June 2022

Table Of Contents

Consulting Team: Diane Deng
Consultant



ABOUT FORRESTER CONSULTING

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

Executive Summary

The amount, type, nature, and sources of data that require a company's attention and intervention have transformed radically in the past five years, and cyberthreats will only continue to evolve and expand. Under this circumstance, the jobs of CISOs and cybersecurity teams have to evolve beyond their companies' perimeters to monitor, detect, and remediate risks that are exposed by individuals, partners, and the broader ecosystem.

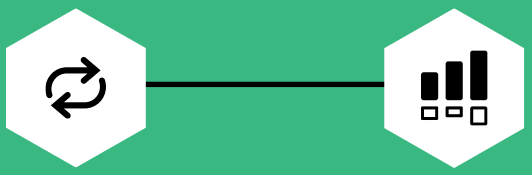
CybelAngel is a global cybersecurity provider focused on external risk protection. It detects exposed data, devices, and services outside the enterprise's perimeter, enabling remediation before the exposure is weaponized. It uses augmented intelligence from the start, where machine-learning algorithms combine with human expertise to eliminate all false positives.

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

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four representatives with experience using CybelAngel. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that is a global conglomerate with 50,000 employees and revenue of $20 billion per year.

Prior to using CybelAngel, these interviewees noted how their organizations faced increasing risks of information leakage and regulatory fines. They also lacked control over third-party vendors and partners' security practices, and they faced surging cybersecurity operational expenses. These limitations led to the adoption of CybelAngel.

KEY STATISTICS



Return on investment (ROI)
359%

Net present value (NPV)
$2.66M

After the investment in CybelAngel, the interviewees managed to gain better control over their organizations' external digital risks. Key results from the investment include avoiding the need to hire additional security analysts, saving on cyber insurance premiums, and avoiding costs from data breaches.

KEY FINDINGS

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

- **Avoids two potential major data breaches per year, which saves more than $2.1 million over three years.** CybelAngel's detection and remediation capabilities help the composite reduce different severities of external digital risks. The true-positive alerts detect risks early and

prevent further exploits. As a result, the composite avoids investigations and fines from regulatory bodies, customer lawsuits, incident response and remediation costs, lost revenue, costs of brand rebuilding, and costs of customer reacquisition.

Major data breaches in a year

Before **2**

After **0**

- **Avoids hiring at least two security analysts, which saves about $860,000 over three years.** By using CybelAngel, the composite organization avoids hiring at least two security analysts who detect incidents, filter through the false-positive alerts, classify incident severity, and initiate remediation. The capabilities of CybelAngel are also more robust than what the composite can develop in-house.
- **Saves 10% on cyber insurance premiums over three years, which worth $437,000.** In the composite's third year of using CybelAngel, it limits its cyber insurance premium increase rate by 10% lower than the average increase rate. This is because the company doesn't make any claims and improves its cybersecurity practices.

In Year 3, the cyber insurance premium increase rate is reduced by

10%

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

- **Improved global cybersecurity governance from incident discovery to remediation.** CybelAngel's ability to scan continually for external digital risks provide the composite's headquarters with visibility and centralized control. It allows the composite to formalize incident remediation processes.
- **Improved partner security practice and reduced partner cyber risks.** CybelAngel is able to trace the source of each data exposure. This allows the composite organization to better regulate and guide partners by updating cybersecurity requirements in partner contracts.

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

- **The annual platform and services fee costs about $494,000 over three years.** The composite determines to invest in CybelAngel based on several factors: product modules used, number of FTEs, number of keywords applied, and remediation services.
- **The internal management of CybelAngel costs about $248,000 over three years.** Before using CybelAngel, the composite organization did not have any in-house or outsourced resource to cover external risk management. The composite organization needs 50% of one analyst's time to read and scan the reports, manage true-positive incidents, and initiate remediation.

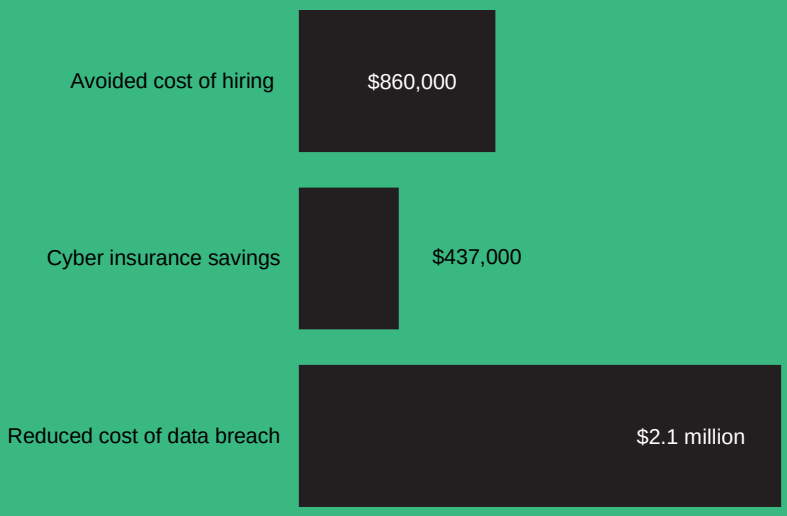
The representative interviews and financial analysis found that a composite organization experiences benefits of $3.40 million over three years versus costs of $741,000, adding up to a net present value (NPV) of $2.66 million and an ROI of 359%.

ROI
359%

BENEFITS PV
$3.40M

NPV
$2.66M

Benefits (Three-Year)



“No business can claim they have the same ability to scan the global internet as well as CybelAngel. It’s not something a company develops. It’s too sophisticated.”

— Global head of cybersecurity, healthcare

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 CybelAngel.

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 CybelAngel 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 CybelAngel 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 CybelAngel.

CybelAngel 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.

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

DUE DILIGENCE
Interviewed CybelAngel stakeholders and Forrester analysts to gather data relative to CybelAngel.

INTERVIEWS
Interviewed four representatives at organizations using CybelAngel 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 CybelAngel Customer Journey

Drivers leading to the CybelAngel external digital risk protection platform investment

Interviews			
Role	**Industry**	**Headquarters**	**CybelAngel Start Date**
CISO	Commercial real estate services	United States	2019
Global head of cybersecurity	Healthcare	France	2015
CISO	Media and retail	France	2017
Group information security officer	Energy and utilities	France	2019

KEY CHALLENGES

Interviewees said security and risk professionals realized their organizations face increasingly distributed digital footprints without the right tools to provide them direct control or ownership.

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

- **Increasing risks of information leakage and regulatory fines.** Interviewees' organizations were vulnerable to various external digital risks since they did not have visibility over what had been exposed. The commercial real estate services interviewee said the high cost of investigation for severe incidents drove their organization to look for a solution.
- **Lacking control over broad partner networks.** The media and retail interviewee shared that over 80% of their organization's data breaches were due to leakage of partners and third parties. However, most companies neither have a solution to trace leakage, nor a process to guide partner cybersecurity practices.
- **Surging cybersecurity operational expenses, including cyber insurance premiums and deductibles.** Research shows that cyber insurance premiums have increased significantly

"A large part of our business depends on the condition of our suppliers. If a supplier goes down, we may have a critical business function going down."

Global head of cybersecurity, healthcare

"We made this investment in order to keep stability and potentially avoid larger-scale incidents. This space is constantly evolving. Cybersecurity three years ago wasn't the same as it is today."

CISO, commercial real estate services

across the board.[2] Companies need ways to slow down the pace of insurance premium increases.

SOLUTION REQUIREMENTS/INVESTMENT OBJECTIVES

The interviewees' organizations searched for a solution that could:

- Be easy to deploy and integrate.
- Monitor all digital risks on the internet.
- Provide best incident detection capability in proof of concept (POC).

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 global conglomerate organization is headquartered in the United States and operates globally. The composite organization has a strong brand and online and offline presences. The composite organization has 50,000 employees globally and 30 security analysts across all operating regions. The revenue of the organization globally is $20 billion. The CISO has a $12 million budget dedicated to cybersecurity.

Deployment characteristics. Before using CybelAngel, the company did not have any tools to monitor external digital risks, and it had very limited cybersecurity capability in-house. The company now uses five modules of CybelAngel: Data Breach Prevention, Account Takeover Prevention, Dark Web Monitoring, Domain Protection, and Asset Discovery and Monitoring.

Key Assumptions

- **$20 billion in revenue**
- **50,000 employees**
- **Didn't have any digital risk management tools before CybelAngel**

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits						
Ref.	**Benefit**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Atr	Avoided cost of hiring	$345,600	$345,600	$345,600	$1,036,800	$859,456
Btr	Cyber insurance savings	$0	$120,000	$450,000	$570,000	$437,265
Ctr	Avoided cost of data breach	$847,384	$847,384	$847,384	$2,542,151	$2,107,318
	Total benefits (risk-adjusted)	$1,192,984	$1,312,984	$1,642,984	$4,148,951	$3,404,039

AVOIDED COST OF HIRING

Evidence and data. Before adopting CybelAngel, the interviewees' organizations had no visibility into their digital risks on the internet. However, increasing cybersecurity risks compelled large organizations to level up their security practices, including adopting new tools, standardizing security practices, and/or hiring more talent. Several interviewees mentioned that the capability of CybelAngel helped their organizations avoid hiring and training additional security analysts.

- CybelAngel took on the workload of a healthcare company's security team and helped it avoid hiring three FTEs. The organization's global head of cybersecurity shared, "If I would have to build the capability in-house, it would require three FTEs to do the work, and this would not match the detection capabilities of CybelAngel."
- The CISO of a media and retail company claimed the value of CybelAngel cannot be replaced by a security operations center (SOC). They said: "My SOC is able to send me thousands of small alerts of malware detections, but the value is not there. I get value from my 300 CybelAngel cases where I see real things that potentially can be exploited directly."

Modeling and assumptions. Forrester modeled the impact for the composite organization assuming:

- The composite organization needs at least two security analysts to conduct the tasks that are done by CybelAngel which include detecting incidents and filtering through the false-positive alerts. CybelAngel also made it easier for analysts to classify incident severity and initiate remediation, which could be time-consuming.
- The annual fully burdened salary for a security analyst is $180,000.
- The cost to onboard a new security analyst is 20% of the annual salary.

Risks. The expected financial impact is subject to risks and variation based on several factors:

- CybelAngel's ability to replace additional hiring will depend on the cybersecurity capability and requirements of each organization.
- The salary of security analyst differs based on the industry, location, and seniority of employees.

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 $860,000.

Avoided Cost Of Hiring					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Number of FTEs required to do detections in-house	Composite	2	2	2
A2	Fully burdened annual salary for security analyst	TEI standard	$180,000	$180,000	$180,000
A3	Avoided onboarding cost	Composite	$36,000	$36,000	$36,000
At	Avoided cost of hiring	A1*(A2+A3)	$432,000	$432,000	$432,000
	Risk adjustment	↓ 20%			
Atr	Avoided cost of hiring (risk-adjusted)		$345,600	$345,600	$345,600
	Three-year total: $1,036,800			**Three-year present value: $859,456**	

CYBER INSURANCE SAVINGS

Evidence and data. Interviewees said cyber insurance premiums have increased significantly during the past few years. Several interviewees valued CybelAngel's contribution to a less steep increase of cyber insurance rate.

- The CISO of a commercial real estate services company acknowledged that CybelAngel contributed to a slower pace of the increment of cyber insurance premium. They said: "We never made a claim after using CybelAngel. If we have made claims, the premium would be even higher."
- The group information security officer for an energy and utilities company also shared the same view. They said: "All insurance premiums are increasing. CybelAngel might have limited the spike. We probably saved about €100,000 per year on insurance premium."

Modeling and assumptions. Forrester modeled the impact for the composite organization assuming:

- The insurance premium is at $10 million for $100 million coverage.[3]
- The cyber insurance premium increment over three years pre-CybelAngel was 15%, 25%, and 35%.
- In Year 3 of using CybelAngel, the composite organization manages to limit the increase rate by 10% lower. The cyber insurance premium increment over three years post-CybelAngel is 15%, 20%, and 30%.

"All insurance premiums are increasing. CybelAngel might have limited the spike."

Group information security officer, energy and utilities

- Forrester attributes 30% cyber insurance savings to CybelAngel since initiatives such as adopting other tools and improving cybersecurity governance and capability also play important roles.

Risks. The expected financial impact is subject to risks and variation based on several factors:

- Insurance coverage and premium can be affected by the type of assets, company size, industry, etc.
- The annual cyber insurance premium increase rate varies by specific locations and cybersecurity practices of specific organizations.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $437,000.

Cyber Insurance Savings

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Pre CybelAngel annual insurance premium	Assumption	$8,696,000	$8,696,000	$8,696,000
B2	Rate increase without CybelAngel	Assumption	15%	25%	35%
B3	Premium increase without CybelAngel	B1*(1+B2)	$10,000,000	$12,500,000	$16,875,000
B4	Rate increase with CybelAngel	Composite	15%	20%	25%
B5	Premium increase with CybelAngel	B1*(1+B4)	$10,000,000	$12,000,000	$15,000,000
B6	Avoided cyber insurance premium increase	B3-B5	$0	$500,000	$1,875,000
B7	Attribution to CybelAngel	Assumption	30%	30%	30%
Bt	Cyber insurance savings	B6*B7	$0	$150,000	$562,500
	Risk adjustment	↓20%			
Btr	Cyber insurance savings (risk-adjusted)		$0	$120,000	$450,000
	Three-year total: $570,000			**Three-year present value: $437,265**	

AVOIDED COST OF DATA BREACH

Evidence and data. Forrester research shows that 63% of organizations were breached in 2021, and that enterprises take an average of 37 days to recover from a breach.[4]

Interviewees' organizations have managed to prevent data breaches by leveraging five modules of CybelAngel: Data Breach Prevention, Account Takeover Prevention, Dark Web Monitoring, Domain Protection, and Asset Discovery and Monitoring.

"Using CybelAngel prevented us from losing money. Some leaks we found were liable to heavy fines or trials."

Global head of cybersecurity, healthcare

In general, incidents in these five modules can be categorized into four levels:

- Level 4 incidents are those that have the potential to trigger major disruptive events, and they have severe impacts on customers and businesses. For example, customer or employee personal information leakage could expose an organization to GDPR fines that could be 4% of worldwide turnover for the preceding financial year for global large organizations.
- Level 3 incidents include critical data openly available but not yet stolen. These types of incidents can have an impact to a given business unit, but they do not pose severe impact on the group entirely.
- Level 2 and level 1 incidents are incomplete credential or data leaks with limited risks of an attack.

Interviewees said CybelAngel's detection and remediation capabilities helped their companies reduce different levels of severities of digital risks. The true-positive alerts managed to detect risks early and prevented further exploits.

- The CISO of the media and retail company said their organization could detect cases within 24 hours.
- The group information security officer with the energy and utilities company said that with CybelAngel, it took three to four days between leak and alert. They said: "We were going to get GDPR fines if the customer data leaks were not remediated. CybelAngel was able to find out the hard disk was badly configured by the individual so we could contact that person and take that down in time."

Modeling and assumptions. Forrester modeled the impact for the composite organization assuming:

- The composite organization receives 400 alerts from CybelAngel in a year, and 20 of them are level 4 detections that could result in severe regulatory fines and sensitive competitive information leakage and exploitation.
- Forrester estimates the average internal and external cost of a breach for an organization of 50,000 employees is $3,026,370 per incident.[5] This includes fines to regulatory bodies, customer reimbursement lawsuits, incident response and remediation, lost revenues, brand equity rebuild costs, and cost of customer reacquisition.
- Forrester attributed 20% of these cost savings to CybelAngel, since improved internal and partner cybersecurity practices and higher organizational awareness are critical to data breach prevention.

Risks. The expected financial impact is subject to risks and variation based on several factors:

- The specific type of data breach.
- The size of the organization.
- The location of the organization.

Results. To account for these risks, Forrester adjusted this benefit downward by 30%, yielding a three-year, risk-adjusted total PV of $2.1 million.

"If there is a detection in the dark web linked to a keyword of an entity, the local manager will be informed directly."

CISO, media and retail

Avoided Cost Of Data Breach					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Number of data breaches per year that become major incidents	Composite	2	2	2
C2	Data breach cost per incident	Forrester research	$3,026,370	$3,026,370	$3,026,370
C3	Attribution to CybelAngel	Assumption	20%	20%	20%
Ct	Avoided cost of data breach	C1*C2*C3	$1,210,548	$1,210,548	$1,210,548
	Risk adjustment	↓30%			
Ctr	Reduced cost of data breach (risk-adjusted)		$847,384	$847,384	$847,384
	Three-year total: $2,542,151		**Three-year present value: $2,107,318**		

UNQUANTIFIED BENEFITS

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

- **Improved global cybersecurity governance.**
  - **Discovery:** Interviewees' organizations have security operations spread across different business units and regions, and CybelAngel can scan globally for external digital risks. It provides the headquarters with visibility and centralized control over the entire company and partner network's cybersecurity practices.
  - **Remediation:** The group information security officer with the energy and utilities company said their organization has formalized incident remediation process with CybelAngel's ability to detect and remediate.
- **Improved partner security practice and reduced partner risks.**
  - Interviewees mentioned that most of their organizations' data breaches came from third parties, such as sellers, potential suppliers, customers, etc.
  - CybelAngel can trace down the source of each leakage, which has allowed interviewees' organizations to better regulate and guide partners by updating cyberpolicy in partner contracts.

FLEXIBILITY

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

- **More streamlined detection to remediation processes in the long run.** One of the key differentiators of CybelAngel is its ability to provide zero false positives with machine learning and analyst intervention. However, the definition of incident severity needs to be customized to each organization. Dedicated in-house analysts and CybelAngel develop a more aligned view on the severity of different types of incidents and the best approach to remediation, which leads to a more mature and streamlined process in the long run.

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

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Dtr	Annual platform and services fee	$0	$198,450	$198,450	$198,450	$595,350	$493,516
Etr	Internal cost	$0	$99,528	$99,528	$99,528	$298,584	$247,511
	Total costs (risk-adjusted)	$0	$297,978	$297,978	$297,978	$893,934	$741,027

ANNUAL PLATFORM AND SERVICES FEE

Evidence and data. Interviewees said the investment in CybelAngel was determined by several factors: product modules used, number of FTEs, number of keywords applied, and remediation services. CybelAngel also provides a free three-week POC to showcase the potential impact of its services.

Modeling and assumptions. The platform cost and services fee are calculated based on the following metrics of the composite organization:

- The number of FTEs is 50,000.
- The number of keywords used in detection is 3,000.
- The company requests five takedown services from CybelAngel in a year.

Risks. The expected financial impact is subject to risks and variation based on several factors:

- Listed price adjustment.
- Currency exchange.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $494,000.

Annual Platform And Services Fee					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
D1	Number of FTE	Composite	50,000	50,000	50,000
D2	Number of keywords	Composite	3,000	3,000	3,000
D3	Platform fee	Composite	$180,000	$180,000	$180,000
D4	Remediation services (5 takedowns)	Composite	$9,000	$9,000	$9,000
Dt	Annual platform and services fee	D3+D4	$189,000	$189,000	$189,000
	Risk adjustment	↑5%			
Dtr	Annual platform and services fee (risk-adjusted)		$198,450	$198,450	$198,450
	Three-year total: $595,350			**Three-year present value: $493,516**	

INTERNAL COST

Evidence and data. Each interviewee said that before using CybelAngel, their organization did not have any in-house or outsourced resource to cover external risk management. Compared to the prior state, the tasks to manage CybelAngel is a new job scope for most organizations.

Modeling and assumptions. The composite organization needs 50% of one analyst's time to read and scan the reports, manage true-positive incidents, and initiate remediation.

Risks. The expected financial impact is subject to risks and variation based on several factors:

- The workload to manage CybelAngel varies depending on the size of the organization, the number of incidents, and the approach to remediation.
- The salary of security analysts, which could vary.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $248,000.

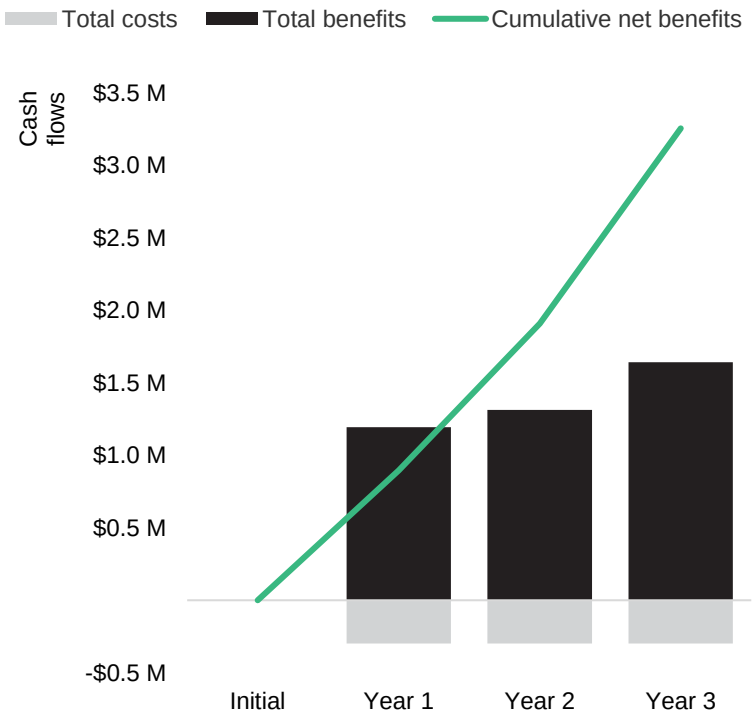
Internal Cost

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
E1	Management time required	Composite		1040	1040	1040
E2	Security analyst hourly rate	A2/2,080		$87	$87	$87
Et	Internal cost	E1*E2	$0	$90,480	$90,480	$90,480
	Risk adjustment	↑10%				
Etr	Internal cost (risk-adjusted)		$0	$99,528	$99,528	$99,528
	Three-year total: $298,584			**Three-year present value: $247,511**		

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 and NPV for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI and NPV 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	$0	($297,978)	($297,978)	($297,978)	($893,934)	($741,027)
Total benefits	$0	$1,192,984	$1,312,984	$1,642,984	$4,148,951	$3,404,039
Net benefits	$0	$895,006	$1,015,006	$1,345,006	$3,255,017	$2,663,012
ROI						359%

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%.

Appendix B: Supplemental Material

Related Forrester Research

"Estimate Breach Impact And Costs To Drive Investments," Forrester Research, Inc., December 3, 2018

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: "The Cyber Insurance Market Struggles With Continued Hardening Market Conditions," Gallagher, January 2022.

[3] Source: "Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market," U.S. Government Accountability Office, May 20, 2021 (https://www.gao.gov/assets/gao-21-477.pdf).

[4] Source: "The 2021 State Of Enterprise Breaches," Forrester Research, April 8, 2022.

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


FORRESTER®