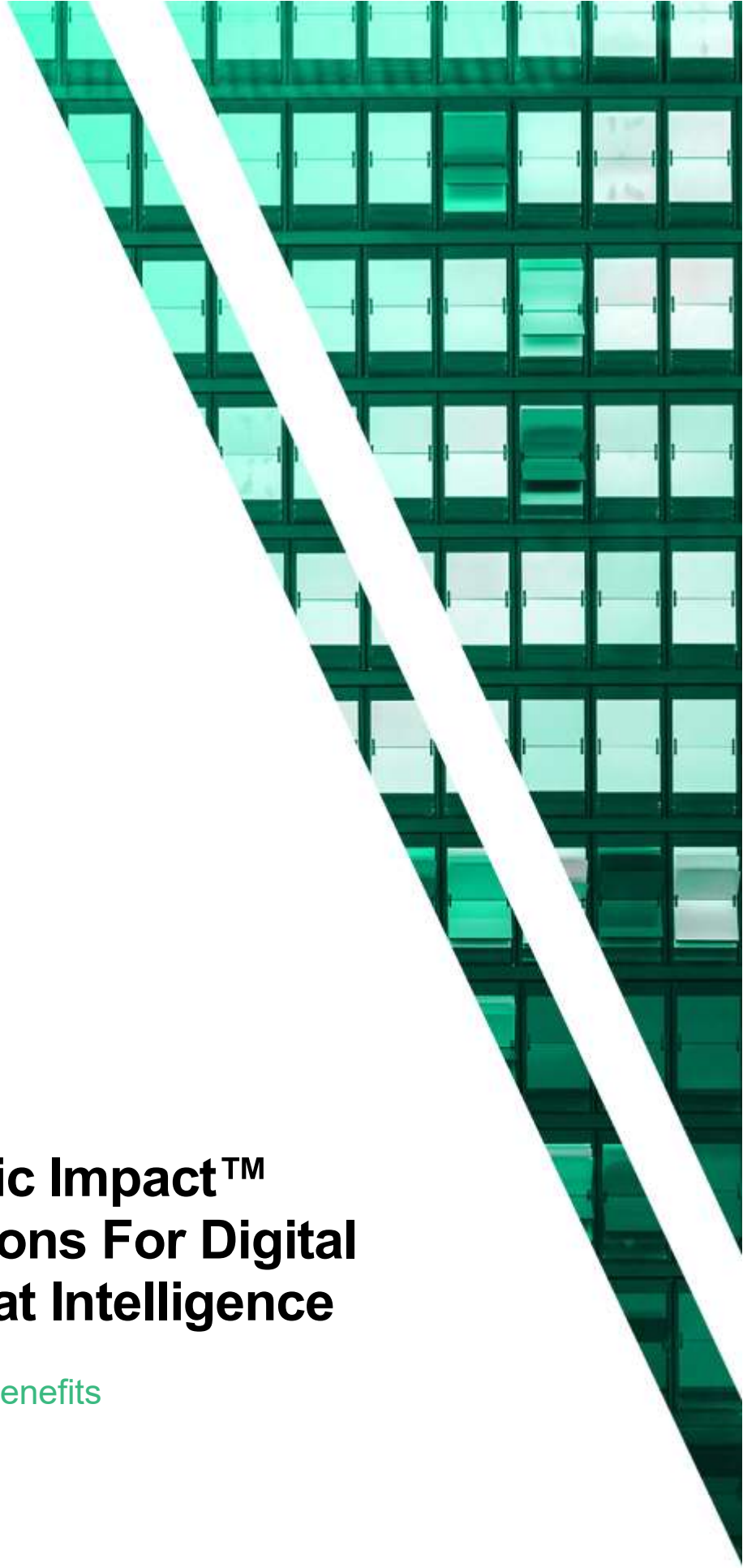
FORRESTER®



The Total Economic Impact™ Of ZeroFOX Solutions For Digital Security And Threat Intelligence

Cost Savings And Business Benefits Enabled By ZeroFOX

SEPTEMBER 2020

Table Of Contents

Executive Summary 1

The ZeroFOX Customer Journey..... 6

Interviewed Organization 6

Key Challenges 6

Solution Requirements And Investment Objectives 6

Use Case Description..... 6

Analysis Of Benefits 8

Reduced Risk Of Executive Impersonation 8

Reduced Cost Of Taking Down Imitation Entity Accounts 9

Unquantified Benefits.....11

Flexibility 11

Analysis Of Costs 12

Annual Subscription Fees.....12

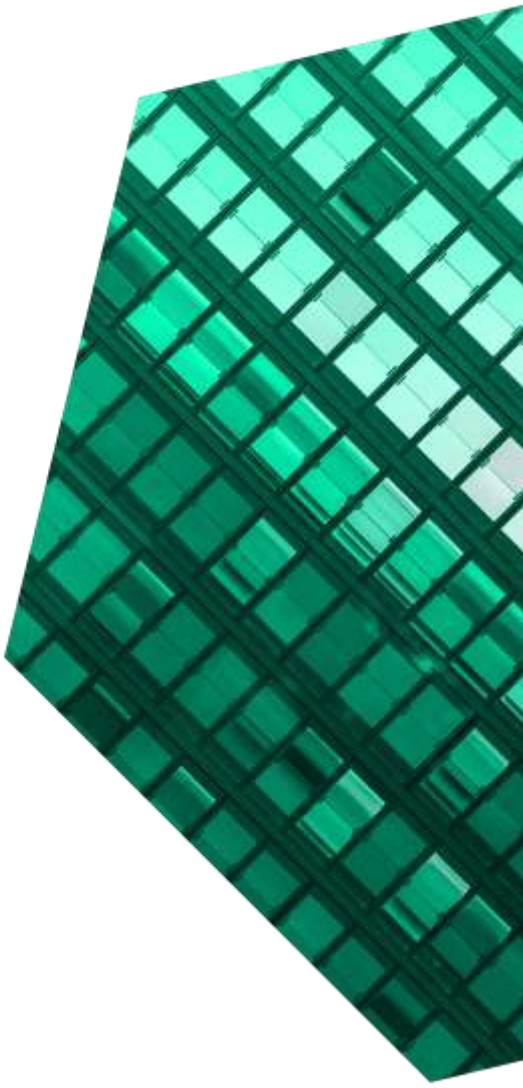
Initial And Ongoing Costs 13

Financial Summary 14

Appendix A: Total Economic Impact.....15

Appendix B: Endnotes.....16

Consultant: *Rachel Ballard*



Executive Summary

While the digital environment creates unprecedented efficiencies, it also provides a myriad of social engineering and cyberattack opportunities. Quickly identifying, remediating, and eliminating digital security risks have become a priority for most enterprise organizations. And by minimizing identity, data, and financial theft scenarios, organizations are able to preserve their brand, reputation, and customer base.

ZeroFOX commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying ZeroFOX. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of ZeroFOX on their organizations. ZeroFOX is a digital risk protection provider that delivers a comprehensive solution that includes an AI-powered software-as-a-service (SaaS) cloud platform, managed services, and automated remediation that identifies and eliminates risk across public attack surfaces. ZeroFOX enables organizations to identify and take down potential security threats, which, if not immediately addressed, can lead to breaches that directly affects employees, customers, and the organization.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed two members of the risk governance team at a global financial services organization with experience using the ZeroFOX solution. Forrester used this experience to project a three-year financial analysis.

Prior to using ZeroFOX, the customer was using a less robust threat intelligence platform to address security issues that are specific to social media impersonations, digital risk, and social engineering. The system yielded limited success and required significant internal, manual searches; the customer was concerned that it did not have the necessary coverage for the organization's size and level of public exposure. The interviewees sought a solution that could proactively analyze large amounts of data and effectively take down verified executive impersonations and imitation entity (company or people) account threats.

KEY STATISTICS

Return on investment (ROI)
267%

Net present value (NPV)
$2.40M

After the investment in ZeroFOX, the customer immediately realized a significant uptick in the number of identified real threats. And through automated remediation, it was able to reduce the potential exposure with fewer FTE hours committed to the manual task of threat hunting and threat elimination.

Reduced risk of executive impersonation:

$1.9 million

KEY FINDINGS

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

- **Reduced risk of executive impersonation.** ZeroFOX allows organizations to continuously monitor executives' presence on all digital platforms by cross-referencing suspicious, flagged material with genuine accounts. They can quickly note false accounts and take mitigating actions. Upon adoption of ZeroFOX, the organization identified an increase of 300 executive impersonations, specifically "whaling" attacks, requiring commensurate takedowns per year, with an average potential cost of $44,000 per threat. Over three years, and adjusting for success rates and risks, this benefit is worth over $1.9 million to the organization.
- **Reduced cost of taking down imitation entity accounts.** ZeroFOX enables organizations to increase their ability to identify imitation entity accounts, such as spoofed domains, fake mobile apps, or false social media accounts, and resolve them. With ZeroFOX, the organization can automate necessary remediation, avoiding the labor cost of manually taking offending accounts down, as in its previous environment. The annual savings of $695K results in a three-year, risk-adjusted present value (PV) of $1.43 million.

> "We can't give any oxygen to these fake accounts. We have to find and take them down immediately because they threaten our customers. ZeroFOX helps us do that."
>
> Global marketing manager, financial services

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

- **Reduced training time by 75%.** The organization reported that their risk governance employees could fully realize the benefits of the ZeroFOX platform in two weeks, down from the two-month training period required with the legacy platform. This reduction in training time allows employees to be fully competent in their roles sooner, resulting in improved digital security coverage.
- **Protected brand reputation.** ZeroFOX enables organizations to identify and remediate potential threats before they become breaches, avoiding possible reputational damage. The interviewed organization reported that it now receives trusted alerts on potential attacks that can be handled before they are launched.
- **Reduced employee burnout.** In its previous environment, the security staff experienced high turnover due to the stressful nature of manual threat hunting and takedowns. With ZeroFOX, both searches and takedowns are completed automatically, significantly reducing the need for employee intervention. One interviewee mentioned: "The stress of finding and remediating threats wasn't getting any better, it was getting worse. I could feel the burnout. We lost employees that could not stand the stress of it."
- **Improved UI and customer service.** Users at the organization report that the ZeroFOX interface is easy to navigate, and they also report that its platform provides comprehensive functionality without being clunky or complicated. Additionally, the organization enjoys the responsive, efficient customer service experience provided by ZeroFOX. The interviewees mentioned that ZeroFOX is a competent, responsive partner concerning their organization's security needs.

Costs. Risk-adjusted PV costs include:

- **Annual subscription fees.** The organization pays a yearly subscription fee of $255,000, resulting in a three-year, risk-adjusted PV of $634,147.
- **Initial and ongoing costs.** The risk-adjusted initial costs incurred were $267,884 over three years. These costs included internal labor required for implementation as well as the expense of maintaining the legacy system during the transitional period. The ongoing costs represent the internal labor necessary to maintain the platform, performing updates as needed, as well as the new cost per imitation entity account takedown.

Reduced cost of taking down imitation entity accounts:

$1.4 million

The interview and financial analysis found that this customer experiences benefits of $3.31M over three years versus costs of $902.0K, adding up to a net present value (NPV) of $2.40M and an ROI of 267%.

ROI
267%

BENEFITS PV
$3.31M

NPV
$2.40M

PAYBACK
<3 months

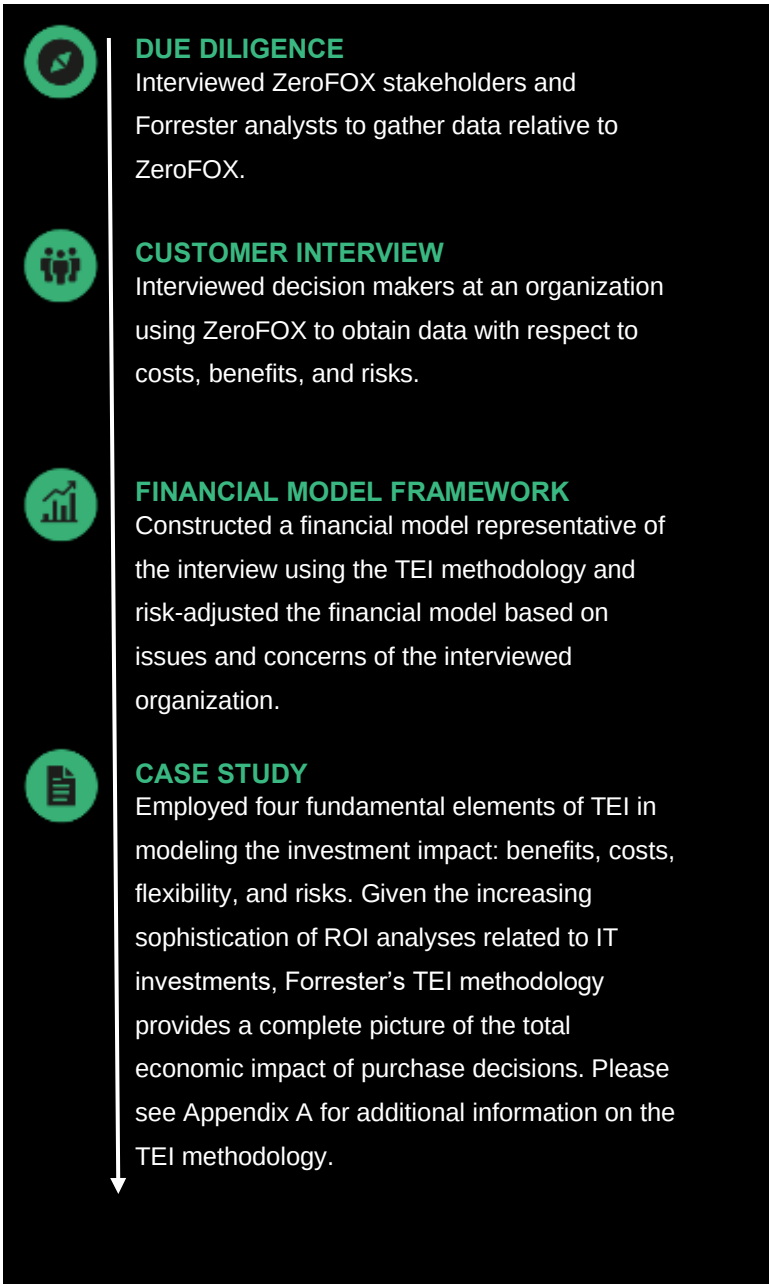
Benefits (Three-Year)

Training time reduced by 75%

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 ZeroFOX.

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 ZeroFOX can have on an organization.



The ZeroFOX Customer Journey

Drivers leading to the ZeroFOX investment

INTERVIEWED ORGANIZATION

Forrester interviewed a ZeroFOX customer with the following characteristics:

- A large global financial services company.
- Risk governance team that monitors over 90 in-house executive accounts for impersonations.
- Strong focus on digital risk protection, social engineering, and the organization's digital footprint.

KEY CHALLENGES

The interviewed organization experienced limitations with its previous solution for monitoring executive impersonations and other external security threats. The risk governance team internally identified an increasing number of social media threats, therefore realizing that its manual approach to detection and resolution was insufficient.

The interviewed organization struggled with common challenges, including:

- **Lack of automated threat detection.** The organization's risk governance team manually found security issues that its legacy solution did not detect. Social engineering threats were pervasive, and the lack of coverage offered by the prior solution resulted in the high risk of a successful digital attack.
- **Delayed reporting.** The lack of accurate and timely threat reporting led to an increased risk to the organization's security, reputation, and privacy. Impersonation and imitation entity accounts went undetected, leaving the organization susceptible to attack. The team needed to efficiently remediate potential risks to avoid large, costly breaches.
- **Need for a user-friendly interface.** The legacy security solution was clunky, cumbersome, and inefficient, forcing the team to primarily rely on its manual threat detection and takedowns. This challenge resulted in an increased potential for human error and employee burnout.

> **"With ZeroFOX, the onboarding was very good, and the user interface is very easy to navigate."**
>
> *Risk governance manager, financial services*

SOLUTION REQUIREMENTS AND INVESTMENT OBJECTIVES

The interviewed organization searched for a solution that could:

- Provide a broad scope of protection for its digital assets, including executive protection, allowing for efficient monitoring.
- Produce useful, timely alerts for detected threats on which management can decisively act and perform automatic takedowns as needed.
- Offer a user-friendly, straightforward interface with the ability to customize performance and provide responsive customer service, ensuring the organization's security needs are met.

USE CASE DESCRIPTION

The interviewed organization sought a comprehensive tool to address increasing exposure to digital threats. Upon adoption, ZeroFOX in concert with the organization's governance team reviewed the company's digital channels and flagged executive impersonation accounts going back several years, uncovering the organization's exposure that necessitated immediate, corrective action. During this

exercise, ZeroFOX also discovered and took down a significant number of dark web threats on pastebin sites that revealed customer data and account information.

In the organization's current environment, ZeroFOX captures relevant information, sends timely alerts regarding malicious threats aimed to exploit customers and external users, and then quickly remediates those risks. The solution liberates the team to focus on higher-level risk and security strategies that preserve its corporate reputation and the integrity of its customers. The team's manager stated: "We rely on ZeroFOX's relationships with public platforms to help to manage our expectations of what's out there. They help us better manage our social media and digital risk footprint efficiently and protect it."

For this use case, Forrester has modeled benefits and costs over three years.

Key assumptions

- **Global financial services organization**
- **Team focused on risk governance**
- **Annual increase in executive impersonation takedowns = 300**
- **Annual increase in imitation entity account takedowns = 8,500**
- **Annual subscription fees = $255K**
- **Implementation time = 2 months**

Analysis Of Benefits

Quantified benefit data

Total Benefits						
Ref.	**Benefit**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Atr	Reduced risk of executive impersonation	$772,200	$772,200	$772,200	$2,316,600	$1,920,347
Btr	Reduced cost of taking down imitation entity accounts	$557,600	$557,600	$557,600	$1,672,800	$1,386,669
	Total benefits (risk-adjusted)	$1,329,800	$1,329,800	$1,329,800	$3,989,400	$3,307,016

REDUCED RISK OF EXECUTIVE IMPERSONATION

Evidence and data. The team realized a substantial increase in the number of executive accounts that required monitoring for irregularities.

- Executive impersonation scammers use social engineering to assume online or email identities of an organization's C-suite to target and persuade innocent employees, vendors, or customers to send wire payments to a criminal's account. This type of cyberfraud is called whaling. One team member mentioned, "ZeroFOX has expanded our coverage of key executives, enabling us to monitor more personnel and therefore reduce our exposure to an impersonation attack."
- In collaboration with the organization, ZeroFOX thoroughly reviewed all existing accounts, flagging executive impersonation accounts, alerting the organization, and resolving those threats which were determined to be real. Searches are now continuously refined and refreshed with up-to-date, customized keywords, enabling the team to stay ahead of digital attackers.
- By providing a solution to track executive account threats and remediate automatically, ZeroFOX eliminated the organization's need for manual threat searches and resolution, which led to better results requiring less team labor.

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

- The increase in executive impersonation account takedowns totals 300 per year.
- Of these takedowns, 10% are dedicated to a whaling attack.
- According to a report from the City of London Police's National Fraud Intelligence Bureau (NFIB), a successful whaling attack costs an organization, on average, $44,000.[1]
- The success rate of a whaling attack is 65%.

> **"Thanks to ZeroFOX, we have our list of nearly 100 top executives that we monitor regularly to make sure there are no account irregularities."**
>
> *Risk governance manager, financial services*

Risks. There are risks, both quantitative and qualitative, that can impact the level of this benefit. Therefore, the reduced risk of executive impersonation will vary with:

- The increasing sophistication of cybercriminals and digital threat technology.
- Strength of executive social media presence.
- Size, industry, and geographical location.
- Internal staff's awareness of digital attack strategies.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.9 million.

Reduced Risk Of Executive Impersonation

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
A1	Total annual increase in executive impersonation takedowns		300	300	300
A2	Percentage of executive impersonation accounts dedicated to whaling attacks		10%	10%	10%
A3	Cost per potential executive impersonation whaling attack	City of London Police NFIB	$44,000	$44,000	$44,000
A4	Average success rate of an executive impersonation whaling attack		65%	65%	65%
At	Reduced risk of executive impersonation	A1*A2*A3*A4	$858,000	$858,000	$858,000
	Risk adjustment	↓10%			
Atr	Reduced risk of executive impersonation (risk-adjusted)		$772,200	$772,200	$772,200
	Three-year total: $2,316,600		**Three-year present value: $1,920,347**		

REDUCED COST OF TAKING DOWN IMITATION ENTITY ACCOUNTS

Evidence and data. The interviewed organization realized the need to cast a wider net with broader threat coverage to adequately identify and take down fake accounts and mitigate potential data breaches.

- The organization defined imitation entity accounts to include location threats, dark web pastebin sites containing private account information, fake URLs misdirecting traffic with the nefarious intention of gathering information, and general phishing attacks using altered email addresses. A successful imitation entity account attack can result in costly reputational and financial damage to the company and its customers.
- The adoption of ZeroFOX allowed the organization to automate threat detection and remediation, significantly increasing the number of successful takedowns of imitation entity accounts. ZeroFOX evaluates potentially threatening phrases, keywords, and logos in its searches to help determine if a threat is either real or a false positive.
- ZeroFOX allows the organization to take down 8,500 more entity account threats per year, up from 1,000, and it requires significantly fewer internal resources. The risk governance manager noted: "My colleague who predominantly handles the fake account takedowns was spending 3 hours per day on this task, before knowing the true breadth of fake accounts. And while we have so much more coverage now, she is now only spending 30 to 45 minutes on this. ZeroFOX is a

big time saver in terms of overseeing the alerts and managing the takedown process."

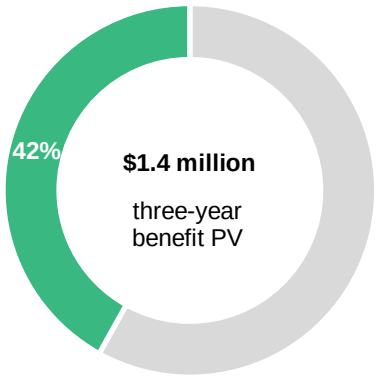
Modeling and assumptions. For the financial analysis, Forrester assumes that:

- The increase in imitation entity account takedowns totals 8,500 per year.
- Based on the organization's previous environment, the cost per manual takedown is $82.

Risks. The reduced cost of taking down imitation entity accounts will vary with:

- The efficiency and skill level of the risk governance security team.
- The salaries of the risk governance security team, which can vary by location or skill set.
- The value of both the organization's and its customers' data.

To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of nearly $1.4 million.



Reduced cost of taking down imitation entity accounts

Reduced Cost Of Taking Down Imitation Entity Accounts					
Ref.	**Metric**	**Calculation**	**Year 1**	**Year 2**	**Year 3**
B1	Increase in takedowns of imitation entity accounts		8,500	8,500	8,500
B2	Previous cost per manual takedown per imitation entity account		$82	$82	$82
Bt	Reduced cost of taking down imitation entity accounts	B1*B2	$697,000	$697,000	$697,000
	Risk adjustment	↓20%			
Btr	Reduced cost of taking down imitation entity accounts (risk-adjusted)		$557,600	$557,600	$557,600
	Three-year total: $1,672,800		**Three-year present value: $1,386,669**		

UNQUANTIFIED BENEFITS

Additional benefits that the customer experienced but was not able to quantify include:

- **Reduced training time.** The plug-and-play nature of ZeroFOX reduced the team's training time for new employees by 75%, allowing them to focus on more strategic projects involving social engineering.
- **Protected brand reputation.** By seeking and taking down possible impersonation and other entity account threats, the organization is better able to control both its overall exposure and the customers' exposure. For example, customer account information could be located on pastebin sites. The successful use of this information would result in financial damage to the customer, and it would have reputational, and thereby financial, repercussions to the organization.
- **Reduced employee burnout.** ZeroFOX automated many team tasks that were previously handled manually. The legacy platform could not manage the scale of the required searches. The risk governance team was spending most of its time on threat hunting and time-consuming, manual takedowns, which led to a high-stress environment, resulting in high turnover.
- **Improved UI and customer service.** The organization appreciated the ability of ZeroFOX to adapt and customize to meet its specific needs. Having experienced the limitations of the previous solution's interface and its related customer service, the team required improvements in these areas.

FLEXIBILITY

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

- **Customized service.** The interviewees noted the responsiveness of ZeroFOX and its willingness to fashion both managed services and updates to meet the organization's goals, allowing the team to perform higher-level tasks.

The global marketing manager mentioned: "ZeroFOX knows that we are really focused on our digital footprint, and they are very supportive of that fact. They work with us directly toward that goal, helping us to be even more productive . . . taking a huge burden off our plate and giving us the flexibility to work more strategically."

Flexibility is described in more detail in Appendix A.

Analysis Of Costs

Quantified cost data

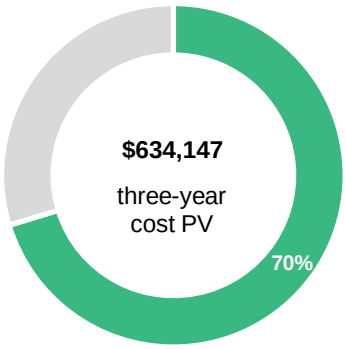
Total Costs

Ref.	Cost	Initial	Year 1	Year 2	Year 3	Total	Present Value
Ctr	Annual subscription fees	$0	$255,000	$255,000	$255,000	$765,000	$634,147
Dtr	Initial and ongoing costs	$61,351	$83,050	$83,050	$83,050	$310,501	$267,884
	Total costs (risk-adjusted)	$61,351	$338,050	$338,050	$338,050	$1,075,501	$902,031

ANNUAL SUBSCRIPTION FEES

Evidence and data. For a social media and digital risk protection application that is working within a global financial services organization of this size, ZeroFOX charges an annual subscription fee of $255,000.

Risks. Given ZeroFOX's pricing structure, Forrester did not risk-adjust this cost, which yielded a three-year total PV of $634,147.



Annual Subscription Fees

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
C1	Subscription fees			$255,000	$255,000	$255,000
Ct	Annual subscription fees	C1	$0	$255,000	$255,000	$255,000
	Risk adjustment	0%				
Ctr	Annual subscription fees (risk-adjusted)		$0	$255,000	$255,000	$255,000
	Three-year total: $765,000			**Three-year present value: $634,147**		

INITIAL AND ONGOING COSTS

Evidence and data. Customers reported initial costs, which include internal labor required for implementation and the cost to maintain the legacy solution for two months.

- Ongoing maintenance costs related to the ZeroFOX investment include internal management and the new cost per takedown of imitation entity accounts.

> **"Any time we have an issue or a gap, ZeroFOX is very easy to contact. They respond remarkably quickly, and there's always a solution."**
>
> *Risk governance manager, financial services*

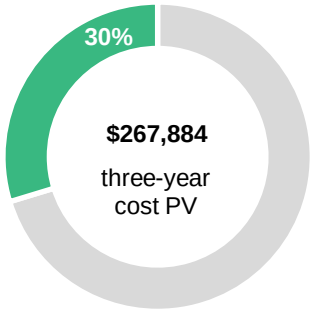
Modeling and assumptions. For the financial analysis, Forrester assumes that:

- Two FTEs are fully dedicated for two months to the implementation of ZeroFOX.
- Maintaining the legacy solution for two months is necessary for continuity of operations.
- The ongoing management and maintenance of ZeroFOX require one FTE for 1.5 hours per day in addition to the new cost per takedown of $8.
- The fully loaded FTE cost is $40,000 per year.

Risks. The risks of this cost category will vary with:

- The experience and sophistication of the risk governance staff.
- The salaries of the risk governance security team, which can vary by location or skill set.
- An organization's previous cost per manual takedown of imitation entity accounts.

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $267,884.



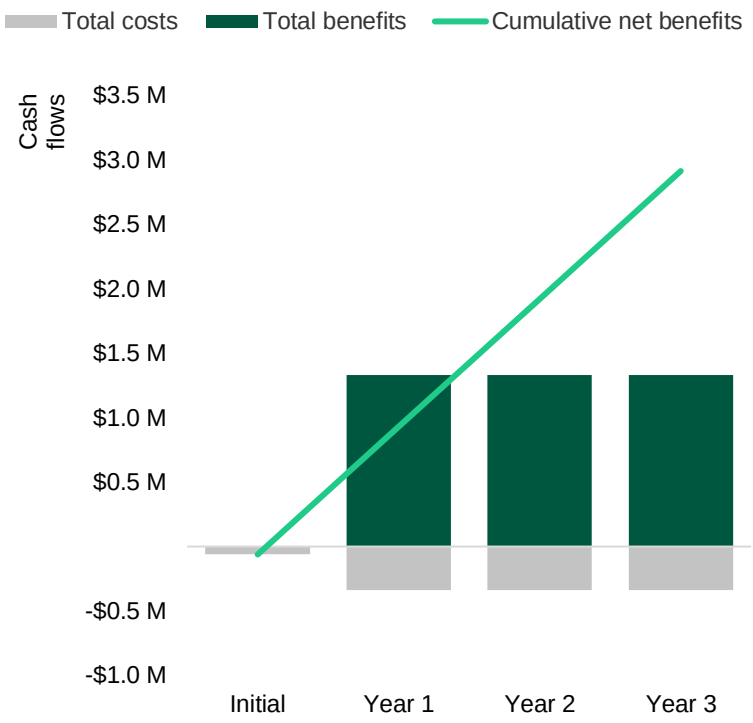
Initial and ongoing costs

Initial And Ongoing Costs						
Ref.	**Metric**	**Calculation**	**Initial**	**Year 1**	**Year 2**	**Year 3**
D1	Initial internal labor cost for implementation	(2 FTEs combined annual salaries/12 months)* 2 months	$13,333			
D2	Cost to maintain previous legacy solution	2 months*$21,220	$42,440			
D3	Ongoing management of solution	(1 FTE*1.5 hours/day) + ($8/takedown*8,500 takedowns)		$75,500	$75,500	$75,500
Dt	Initial and ongoing costs	D1+D2+D3	$55,773	$75,500	$75,500	$75,500
	Risk adjustment	↑10%				
Dtr	Initial and ongoing costs (risk-adjusted)		$61,351	$83,050	$83,050	$83,050
	Three-year total: $310,501			**Three-year present value: $267,884**		

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



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

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

Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($61,351)	($338,050)	($338,050)	($338,050)	($1,075,501)	($902,031)
Total benefits	$0	$1,329,800	$1,329,800	$1,329,800	$3,989,400	$3,307,016
Net benefits	($61,351)	$991,750	$991,750	$991,750	$2,913,899	$2,404,985
ROI						267%
Payback period						<3 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.

Appendix B: Endnotes

[1] Source: “Action Fraud warning after serious rise in CEO fraud,” ActionFraud, May 2, 2016 (actionfraud.police.uk/alert/action-fraud-warning-after-serious-rise-in-ceo-fraud).

FORRESTER®