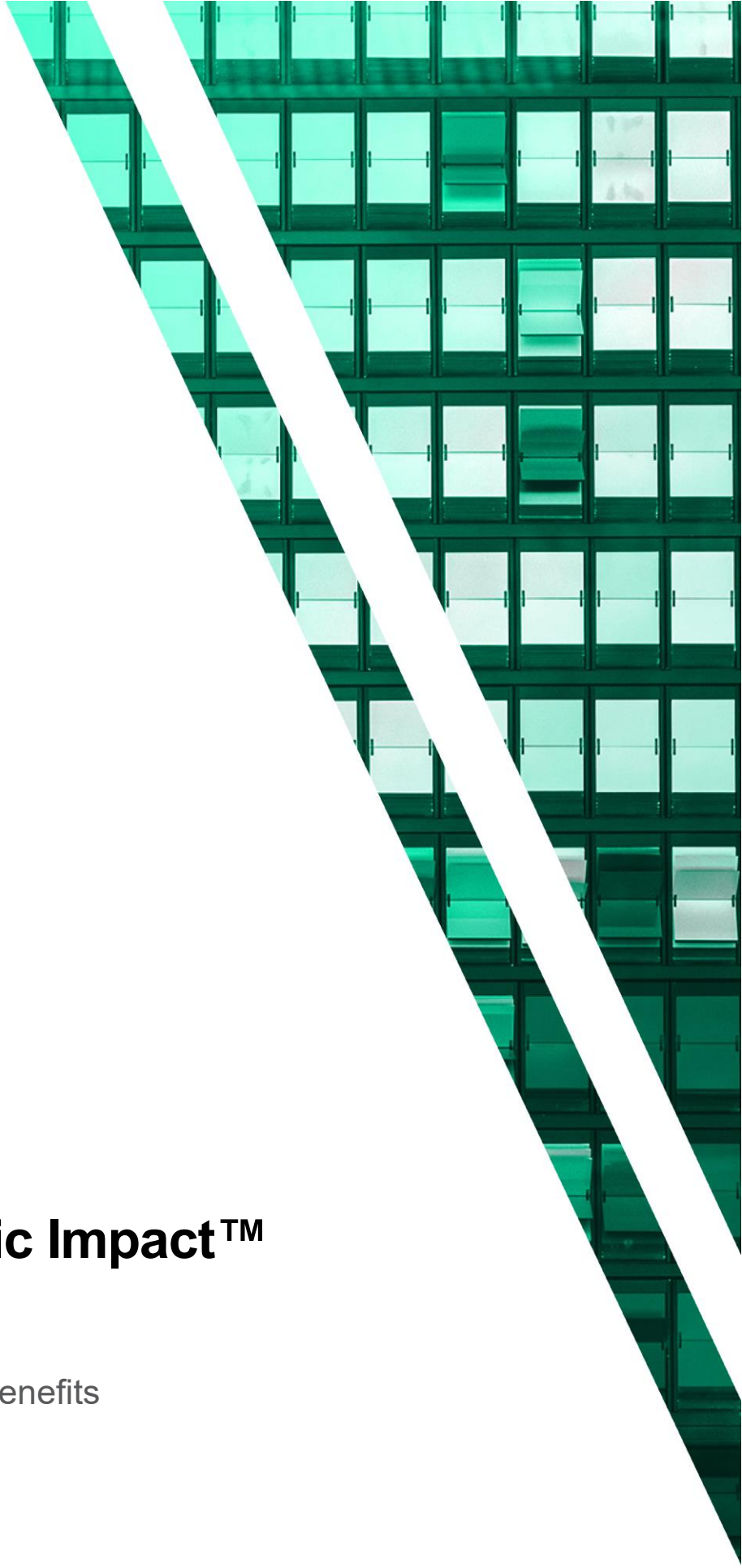
FORRESTER®



The Total Economic Impact™ Of Bolster

Cost Savings And Business Benefits Enabled By Bolster

DECEMBER 2022

Table Of Contents

Executive Summary 1

The Bolster Customer Journey 6

Interviewee's Organization 6

Key Challenges 6

Use Case Description 6

Analysis Of Benefits 7

Increased Productivity From Enhanced Domain Takedown Capacity And Management 7

Avoided Cost Of Building And Managing An In-House Digital Risk Solution 8

Vendor Consolidation From Enhanced Digital Risk Security And Domain Management 9

Unquantified Benefits 10

Flexibility 11

Analysis Of Costs 12

Bolster Software License Fee 12

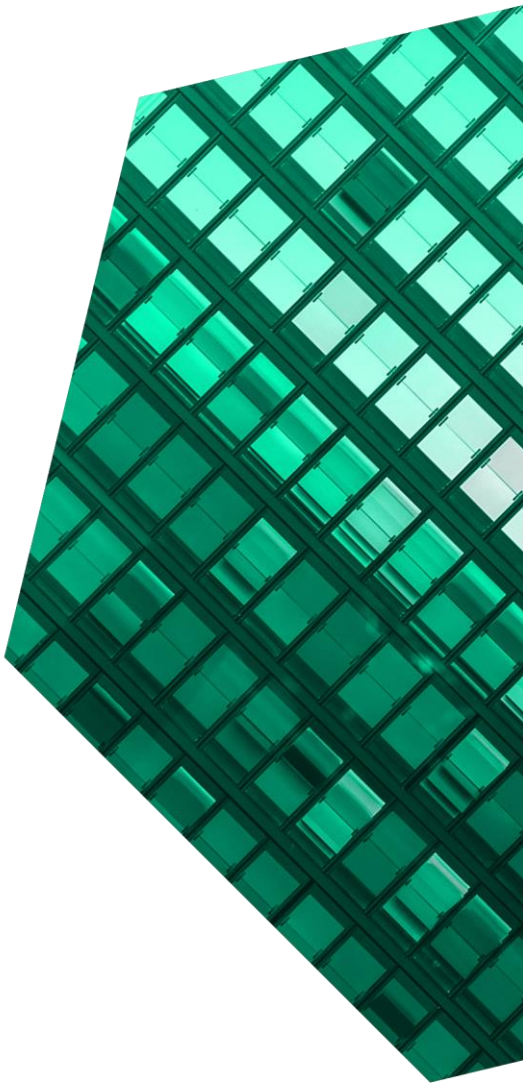
Domain Management Expenses 13

Financial Summary 14

Appendix A: Total Economic Impact 15

Appendix B: Endnotes 16

Consulting Team: Judd Grutman
Kris Peterson



ABOUT FORRESTER CONSULTING

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

Executive Summary

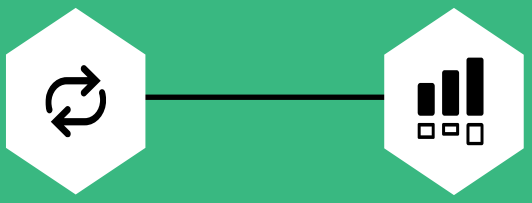
The scope, speed, and volume of digital attacks continue to outpace enterprise security teams, jeopardizing brand reputation, user trust, and organizational security. Relying on legacy detection and mitigation processes has become insufficient to take on bad actors and wastes an organization's resources. With Bolster's AI-powered security workflow and sophisticated domain takedown capabilities, organizations can manage and remediate digital risks at scale while saving time and money.

Bolster offers a proactive and automated digital risk platform that equips enterprises with real-time detection, analysis, and takedown capabilities to prevent and remediate fraud, phishing, typosquatting, and other digital attacks. Through patented computer vision and natural language processing (fields of artificial intelligence or AI) and machine learning (ML) technologies, Bolster's proprietary threat intelligence helps its customers stay ahead of external bad actors in a world where the digital attack surface is expanding. While Bolster's security capabilities are sophisticated, its multimodule, no-code platform is easy to use and includes an intuitive dashboard that enables enterprises to manage external digital risks at scale. Bolster continues to innovate its offerings and currently provides customers a consistent experience across the open web, domain management, social media, app store, and dark web modules.

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

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed a decision-maker at an organization who has experience using Bolster. Forrester used this experience to project a three-year financial analysis.

KEY STATISTICS



Return on investment (ROI)
278%

Net present value (NPV)
$2.19M

Prior to using Bolster, the organization faced various digital attacks, including typosquatting, fake websites, and attempts to steal user credentials and breach existing accounts. However, it had not identified digital risk tools to effectively monitor and remediate attacks and it lacked a scalable complement to the takedown capabilities of its security engineers.

After the investment in several of Bolster's modules, the organization can adequately manage digital threats across the web, social media, top-level-domains (TLDs), and other attack surfaces with its existing workforce. Out of the range of modules offered by Bolster, the organization purchased open web, social media, app store, and domain management. Key results from the investment include significant productivity gains for security

engineers and cost avoidances from the enhanced takedown and domain management capacity that Bolster provides.

KEY FINDINGS

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

- **Increased productivity for security engineers.** Bolster provides enhanced domain takedown capacity, including zero-touch takedowns, which frees up work hours for the interviewee's security engineering team. With Bolster, the organization saves 12,000 engineering hours annually on managing and completing domain takedowns. Using Bolster to make quick and accurate fraud determinations and effectively remediate typosquatting and other malicious sites within minutes is estimated to save the organization approximately $1.4 million over three years.
- **Avoided costs of building and managing an in-house solution.** The interviewee's organization relies on Bolster's real-time application programming interface (API) for its threat modeling and to provide continuous, 360° digital monitoring of its external attack surfaces at scale. Contracting with Bolster to utilize its proprietary threat intelligence and spam detection enables the interviewee's organization to avoid having to build and manage an in-house solution, which is estimated to save approximately $1.1 million over three years.
- **Vendor consolidation and domain management cost savings.** The interviewee's organization uses Bolster to manage its digital risk security across the web, TLDs, and social media.[1] As a result, the organization avoids using unnecessary digital risk tools each year to detect and remediate brand infringements, malicious ads, and sites, spam, and other fraudulent activities across different attack surfaces. Bolster also enables the organization to efficiently and strategically purchase defensive domains based on threat level and cost This vendor consolidation, including vendor-associated subscription and service costs, and domain management cost savings is estimated to save the organization approximately $484,300 over three years.

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

- **Increased threat visibility.** Bolster's AI-based solution and no-code customer dashboard give the interviewee's organization quick access to digital security exposure, including action items to remediate suspicious activity before it becomes a bigger threat. Bolster's solution makes for rapid time to value by reducing deployment expenses, regular training, and administrative costs. Moreover, while each security breach is unique, enterprises spend a median of 37 days and a mean of $2.4 million to find and recover from a breach according to Forrester research.[2]
- **Brand reputation protection.** With Bolster, the organization observes a reduction in negative social media posts and other critical online commentary. Bolster enables the organization to detect and mitigate misuse of its brand, logo infringement, and phishing, reducing overall consumer concerns and deception.
- **Customer security and trust.** Bolster helps the organization provide its customers with a consistently secure user experience, including a reduction in fake sites and online scams.

Costs. Three-year, risk-adjusted PV costs include:

- **Bolster software license fee.** Bolster charges a license fee for its software that is determined by the number of threat modules needed. This cost includes takedown costs that are priced based on the number or tiered number of takedowns needed. The three-year license fee is estimated to cost $579,000 for three of Bolster's threat modules and unlimited takedowns.

- **Domain management expenses.** Bolster strategically purchases domains that pose threats to its customers. Defensive domain purchasing by Bolster is dependent on customer approval and made with customer-allocated funds. It is estimated to cost $209,000 over three years.

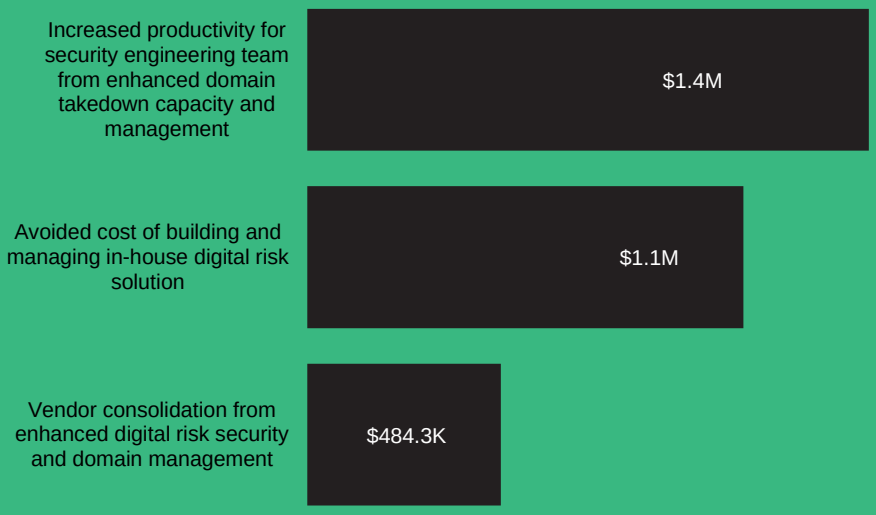
The interview and financial analysis found that the representative's organization experiences benefits of $2.98 million over three years versus costs of $788,000, adding up to a net present value (NPV) of $2.19 million and an ROI of 278%.

ROI
278%

BENEFITS PV
$2.98M

NPV
$2.19M

Benefits (Three-Year)



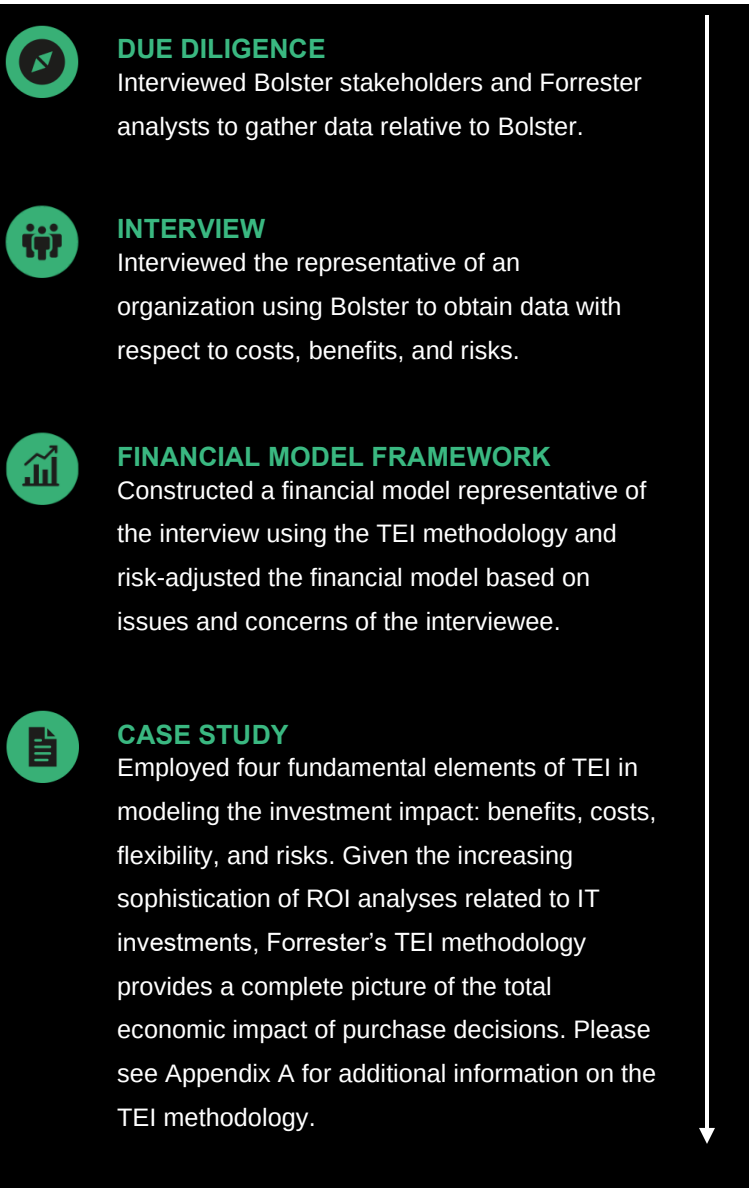
“We know that [Bolster] has this capability, we know that we are doing the right thing to protect user trust and [have] the peace of mind that comes with that.”

— Director of engineering and security, web file hosting

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 Bolster.

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 Bolster can have on an organization.



The Bolster Customer Journey

Drivers leading to the Bolster investment

INTERVIEWEE'S ORGANIZATION

Forrester interviewed the director of engineering and security of an organization who has experience using Bolster. The interviewee's organization has the following characteristics:

- Annual revenue in excess of $2 billion.
- Over 100 million users.
- Global workforce with a 40-person security engineering team.

KEY CHALLENGES

Prior to using Bolster, the interviewee's organization did not use digital risk tools to detect, monitor, or remediate external attacks.

The interviewee noted how their organization struggled with common challenges, including:

- **Needing comprehensive solution for expanding digital attack surfaces.** The organization needed a threat detection engine to proactively monitor, detect, and help remediate digital attacks, such as phishing scams aimed at taking over its users' accounts. The organization could not automatically detect or monitor external digital risks, nor could it assess its overall digital risk exposure. Moreover, the organization needed a consistent management tool to seamlessly address threats across the web, social media, and app stores due to its expanding digital attack surfaces and attackers leveraging multiple digital channels to launch scams.
- **Needing additional capacity for domain takedowns.** The organization experienced numerous instances of domain squatting or hijacking, including on domains still in the build or prebuild stage, which required takedowns. Completing a takedown was a manual, time-consuming task for the interviewee, requiring a painstaking and tactical process by the organization's security engineers.
- **Needing additional capabilities for domain management.** Given the interviewee's organization's global user base, the interviewee faced more fake and fraudulent websites than it could (or even needed to) remediate. As a result, the interviewee looked for a way to effectively address typosquatting and strategically purchase defensive domains in a way that that included accounting for domain costs and threat levels.
- **Protecting brand reputation and user trust.** The organization needed to mitigate negative social media resulting from digital fraud schemes targeting its customers. Before Bolster, the interviewee could not ensure the organization was continuously protecting its brand and users from untrusted products and outside attacks.

USE CASE DESCRIPTION

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

Key Assumptions

- **Annual revenue over $2 billion**
- **100 million users**
- **Global workforce with a 40-person security engineering team**
- **1,200 domain takedowns completed annually through Bolster**
- **Defensive domain buying budget of $7,000 per month**

Analysis Of Benefits

Quantified benefit data

Total Benefits						
Ref.	**Benefit**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Atr	Increased productivity for security engineering team from enhanced domain takedown capacity and management	$564,663	$564,663	$564,663	$1,693,990	$1,404,234
Btr	Avoided cost of building and managing in-house digital risk solution	$986,000	$123,250	$123,250	$1,232,500	$1,090,823
Ctr	Vendor consolidation from enhanced digital risk security and domain management	$194,750	$194,750	$194,750	$584,250	$484,314
	Total benefits (risk-adjusted)	$1,745,413	$882,663	$882,663	$3,510,740	$2,979,371

INCREASED PRODUCTIVITY FOR SECURITY ENGINEERING TEAM FROM ENHANCED DOMAIN TAKEDOWN CAPACITY AND MANAGEMENT

Evidence and data. Bolster's platform enabled the interviewee's organization to experience significant output gains for its security engineers.

- The director of engineering explained that, with Bolster, its organization was able to manage and remediate fake domains without the time-consuming and manual review and mitigation processes it security engineers previously employed.
- When asked how many domain takedowns Bolster completed for their organization, the director of engineering stated, "They take [down] around 100 sites per month."
- Furthermore, the interviewee confirmed a significant time savings from utilizing Bolster's takedown capacity. They said that, before the solution, their staff spent anywhere from a few hours to a few days to complete a domain takedown, with an approximation of 10 hours per takedown.

Modeling and assumptions. To quantify this benefit, Forrester assumes:

- Bolster completes 1,200 zero-touch domain takedowns annually.
- The 10 hours the security engineer team saves managing a takedown includes detection, monitoring, and completion activities.
- The fully burdened annual salary of a security engineer is $145,000.
- The team reallocates 75% of its saved time to other value-added tasks.

Risks. Factors impacting the realization of this benefit include:

- The prevalence and resilience of rogue domain creation.
- The experience and skillset of the personnel assigned to tasks related to domain takedowns.

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 $1.4 million.

Increased Productivity For Security Engineering Team From Enhanced Domain Takedown Capacity And Management					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Domain takedown incidents per year	Interview	1,200	1,200	1,200
A2	Average hours saved on detection, monitoring, and completion of each domain takedown incident	Interview	10	10	10
A3	Subtotal: Number of hours saved annually	A1*A2	12,000	12,000	12,000
A4	Average hours worked annually per security engineering team member	TEI standard	2,080	2,080	2,080
A5	Subtotal: Security engineering team member annual workloads saved	A3/A4	5.77	5.77	5.77
A6	Fully burdened annual salary per security engineering team member	TEI standard	$145,000	$145,000	$145,000
A7	Productivity recapture	TEI standard	75%	75%	75%
At	Increased productivity for security engineering team from enhanced domain takedown capacity and management	A5*A6*A7	$627,404	$627,404	$627,404
	Risk adjustment	↓10%			
Atr	Increased productivity for security engineering team from enhanced domain takedown capacity and management (risk-adjusted)		$564,663	$564,663	$564,663
	Three-year total: $1,693,990			**Three-year present value: $1,404,234**	

AVOIDED COST OF BUILDING AND MANAGING AN IN-HOUSE DIGITAL RISK SOLUTION

Evidence and data. The interviewee's organization did not have to build and manage an in-house solution to continuously detect, monitor, and help remediate external digital attacks.[3] Instead, the interviewee was able to confidently rely on Bolster's proprietary risk intelligence and services for its digital threat modeling and management.

- The director of engineering indicated that their organization lacked the bandwidth to build a solution itself.
- The interviewee's organization avoided the cost of software engineers' time needed to support an in-house solution, including the potential hiring of additional engineers. They said: "We [would have] need a year with a full engineering team … 10 people. But in this particular case, [we] will also have to leverage some talent … that my team probably doesn't have. There's also a kind of expansion of the talent set that we have to hire."

"We are investing but saving costs by getting this capability and leveraging something that's out there."

Director of engineering and security, web file hosting

Modeling and assumptions. To model this benefit, Forrester assumes:

- The organization needs 10 software engineers working 80% of their workloads in Year 1 to build an in-house digital risk solution.
- The organization needs one software engineer working full time (or two software engineers working half time) in Year 2 and Year 3 to manage an in-house digital risk solution.
- The interviewee's software engineers receive a fully burdened annual salary of $145,000.

Risks. Factors impacting the realization of this benefit include:

- The existing software engineering workforce of an organization and its skillset.
- The total hours and number of engineers required and allocated by an organization to build and manage an in-house digital risk solution.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1,09 million.

Avoided Cost Of Building And Managing In-House Digital Risk Solution

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Number of engineers supporting in-house solution	Interview	10.00	1.00	1.00
B2	Portion of time spent building and managing in-house solution	TEI standard	0.80	1.00	1.00
B3	Fully burdened annual salary	TEI standard	$145,000	$145,000	$145,000
Bt	Avoided cost of building and managing in-house digital risk solution	B1*B2*B3	$1,160,000	$145,000	$145,000
	Risk adjustment	↓15%			
Btr	Avoided cost of building and managing in-house digital risk solution (risk-adjusted)		$986,000	$123,250	$123,250
	Three-year total: $1,232,500			**Three-year present value: $1,090,823**	

VENDOR CONSOLIDATION FROM ENHANCED DIGITAL RISK SECURITY AND DOMAIN MANAGEMENT

Evidence and data. The organization was able to consolidate digital risk tools, including vendor-associated subscription and service costs, with Bolster's modules for open web, social media, app store, and domain management services.

- The director of engineering and security noted that their organization did not need two digital risk tools after using Bolster's domain, web, app store, and social media threat modules.
- The interviewee's organization avoided $105,000 in defensive domain costs by strategically purchasing malicious domains recommended by Bolster based on cost and threat level.

Modeling and assumptions. To model this benefit, Forrester assumes:

- The interviewee does not need two digital risk tools as a result of using Bolster.
- A digital risk tool costs $50,000 annually, including subscription and service fees.
- A digital risk tool costs $50,000 annually, including subscription and service fees.

Risks. Factors impacting the realization of this benefit include:

- The extent of an organization's attack surfaces.
- The capabilities of an organization's workforce.
- The interviewee's domain management capacity and the number of fake sites in existence.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV (10% reduction) of $484,300.

data analysis and research, enterprises spend a median of 37 days and a mean of $2.4 million to find and recover from a breach. However, Forrester research has also found that "organizations that lack incident and crisis response preparation [take] longer to recover from breaches" and that "preparation prior to a breach is critical to reduce recovery time and costs."[4]

Vendor Consolidation From Enhanced Digital Risk Security And Domain Management

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Number of digital risk tools not needed	Interview	2	2	2
C2	Average cost per digital risk tool annually, including subscription and service costs	TEI standard	$50,000	$50,000	$50,000
C3	Subtotal: Digital risk tool consolidation annually	C1*C2	$100,000	$100,000	$100,000
C4	Avoided defensive domain costs from enhanced domain management	Interview	$105,000	$105,000	$105,000
Ct	Vendor consolidation from enhanced digital risk security and domain management	C3+C4	$205,000	$205,000	$205,000
	Risk adjustment	↓5%			
Ctr	Vendor consolidation from enhanced digital risk security and domain management (risk-adjusted)		$194,750	$194,750	$194,750
	Three-year total: $584,250		**Three-year present value: $484,314**		

UNQUANTIFIED BENEFITS

The interviewee mentioned the following additional benefits that their organization experienced but was not able to quantify:

- **Increased threat visibility.** The interviewee's organization can quickly assess its digital attack risks because of Bolster's straightforward setup. Bolster hosts the service, and it requires no coding or engineering to implement and deploy. Moreover, Bolster's intuitive dashboard helps mitigate security breaches by alerting the interviewee's organization to how many times it is affected and how many sites the solution is taking down. While security breaches are unique, they can be very costly: According to Forrester

"I like their flexibility and their willingness to partner with you, understand your problems, and adapt their business in order to support [yours]."

Director of engineering and security, web file hosting

“If we were the ones doing it, we’d have to communicate with the domains, spend time trying to reach out the right way to points of contact, send emails, and who knows what else can be involved in the process.”

Director of engineering and security, web file hosting

- **Brand reputation protection.** The director of engineering and security observed that because Bolster’s service looks for fake domains and targeted bad actors that were trying to create fake sites and otherwise imitate or misuse the organization’s brand and logo, there is less noise on social media. The interviewee’s organization can then avoid harm to its reputation from online criticism.
- **Customer security and trust.** Similarly, because Bolster enables the interviewee’s organization to actively monitor phishing scams, the director of engineering and security indicated: “[While the organization] has seen a lot of attacks on [our site] and account takeovers … we are able to associate [them] to fake domains … when that happens, we reset the password or like to add another verification and make sure that we are talking with the customer.”

FLEXIBILITY

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

- **Optimized risk response and remediation.** In collaboration with the interviewee’s organization, Bolster developed a proprietary method of recommending defensive domain purchases by cost and threat level, which helps the interviewee’s organization focus on the most suspicious activity before it becomes a bigger threat. As the director of engineering and security stated: “Actually that’s the one thing I requested from them. Kind of like we partnered … they built it, and we took advantage of it.”
- **Trusted advice and partnership.** Not only does Bolster help the interviewee’s organization adjust and respond to digital threats, but Bolster has also become a trusted partner and source of advice for the organization. Through the partnership, Bolster adds value during deployment, listens to the organization’s needs, and adapts to new changes to fit the organization’s exposure. As the director of engineering and security stated: “That’s something you see happening in bigger companies that have more mature products. But I’m very, very confident that [Bolster] is flexible if [you] are willing to work with them.” While the organization only deployed a portion of Bolster’s platform, Bolster continues to innovate by adding features and functionality to their product offerings and allowing for shared and continued growth between the organization and their customers.

“We treat Bolster as a black box where we monitor the matrix.”

Director of engineering and security, web file hosting

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

Total Costs

Ref.	Cost	Initial	Year 1	Year 2	Year 3	Total	Present Value
Dtr	Bolster software license fee	$0	$233,000	$233,000	$233,000	$699,000	$579,437
Etr	Domain management expenses	$0	$84,000	$84,000	$84,000	$252,000	$208,896
	Total costs (risk-adjusted)	$0	$317,000	$317,000	$317,000	$951,000	$788,333

BOLSTER SOFTWARE LICENSE FEE

Evidence and data. Bolster is licensed on an annual basis. The cost of deploying Bolster's platform varies across organizations and is dependent upon the number of threat modules and takedowns purchased, as well as the complexity of processes associated with software implementation for an organization.

According to the director of engineering and security, the interviewee's organization purchased three threat modules from Bolster with unlimited takedowns for three years. They said, "The cost that we pay, it's like $700,000 for a three-year subscription."

Additionally, the director of engineering and security indicated that there were no implementation or training costs. They said: "In the case of Bolster, [the deployment] process was pretty simple because it is hosted on their side. The only information they need from us is the domain and some URLs."

Modeling and assumptions. To model this benefit, Forrester assumes that the interviewee pays the same license fee of $233,000 each year and that it includes unlimited takedowns.

Risks. Digital risk management needs can suddenly increase for an organization due to a spike in popularity, publicity, and user activity.

Results. Forrester has used the annual license fee of $233,000 as provided by the interviewee and has made no risk adjustment to this amount, yielding a three-year, risk-adjusted PV (discounted at 10%) of $579,000.

Bolster Software License Fee

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
D1	Annual license fee for unlimited takedowns and three modules	Interview	$0	$233,000	$233,000	$233,000
Dt	Bolster software license fee	D1	$0	$233,000	$233,000	$233,000
	Risk adjustment	0%				
Dtr	Bolster software license fee (risk-adjusted)		$0	$233,000	$233,000	$233,000
Three-year total: $699,000			**Three-year present value: $579,437**			

DOMAIN MANAGEMENT EXPENSES

Evidence and data. Bolster offers domain management services, which includes the strategic purchase of defensive domains. The cost of utilizing Bolster's domain management services varies across organizations and is dependent upon the number of defensive domains authorized to be purchased, as well as the complexity of implementing domain purchase decisions.

The interviewee's organization authorized Bolster to purchase $7,000 worth of defensive domains on its behalf every month, as explained by its director of engineering and security: "Buying the domains is an initial cost that we pay. That's like $7,000 per month."

Modeling and assumptions. To model this benefit, Forrester assumes:

- Bolster receives the interviewee's organization's entire annual budget for domain purchases.
- The interviewee's organization's annual budget for domain purchases remains constant.

Risks. Domain management expenses can change unexpectedly. The need for defensive domain purchasing can suddenly increase when an organization experiences a spike in popularity, publicity, and user activity.

Results. Forrester has used the annual domain management expenses of $84,000 as provided by the interviewee and has made no risk adjustment to this amount, yielding a three-year, risk-adjusted PV (discounted at 10%) of $209,000.

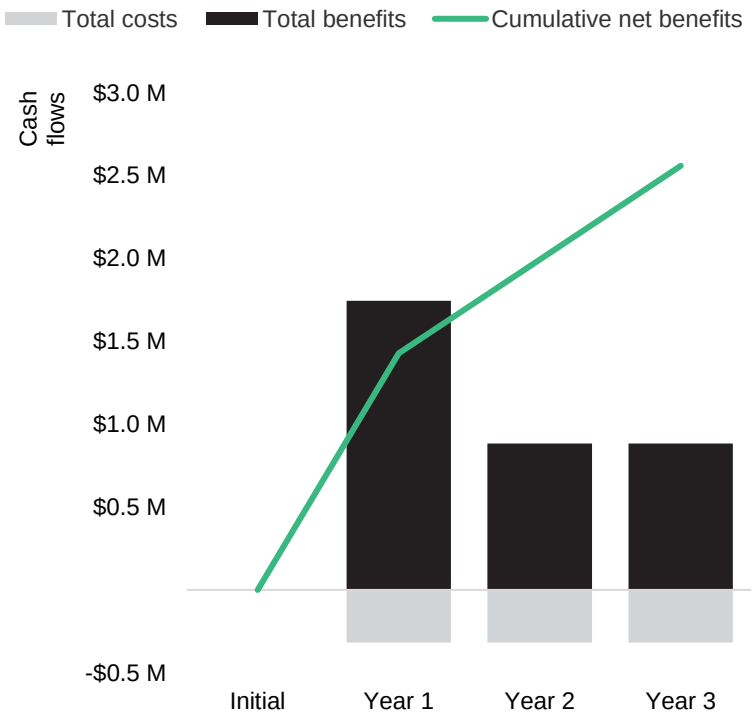
Domain Management Expenses

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
E1	Annual budget for domain purchases	Interview		$84,000	$84,000	$84,000
Et	Domain management expenses	E1	$0	$84,000	$84,000	$84,000
	Risk adjustment	0%				
Etr	Domain management expenses (risk-adjusted)		$0	$84,000	$84,000	$84,000
	Three-year total: $252,000			**Three-year present value: $208,896**		

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

These risk-adjusted ROI, and NPV 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	$0	($317,000)	($317,000)	($317,000)	($951,000)	($788,333)
Total benefits	$0	$1,745,413	$882,663	$882,663	$3,510,740	$2,979,371
Net benefits	$0	$1,428,413	$565,663	$565,663	$2,559,740	$2,191,038
ROI						278%

Appendix A: Total Economic Impact

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

TOTAL ECONOMIC IMPACT APPROACH

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

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

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

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

The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

PRESENT VALUE (PV)

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.

NET PRESENT VALUE (NPV)

The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made, unless other projects have higher NPVs.

RETURN ON INVESTMENT (ROI)

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

DISCOUNT RATE

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

PAYBACK PERIOD

The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

Appendix B: Endnotes

[1] As of the writing of this report, Bolster is the only digital risk solution that provides security support for the social media platform WhatsApp.

[2] Every year, Forrester delivers the Forrester Analytics Business Technographics® Security Survey. In 2022, the survey analyzed data regarding the costs and effects of security breach found enterprises spend a median of 37 days and a mean of $2.4 million to find and recover from a security breach. Globally, organizations took a median of 27 days to find an adversary and eradicate an attack and a median of 10 days to recover from a breach, totaling 37 days to find and recover from a breach. It also cost organizations a global mean of $2.4 million in total per breach. Source: “The 2021 State Of Enterprise Breaches,” Forrester, Inc., April 8, 2022.

[3] As referenced herein, an “in-house solution” is intended to represent an alternative solution to Bolster and one that does not contain Bolster’s full array of product offerings and services. Moreover, building and maintaining an “in-house solution” assumes utilizing open source code and an internal team of engineers. All costs associated with an “in-house solution” include security operations costs.

[4] Source: “The 2021 State Of Enterprise Breaches,” Forrester, Inc., April 8, 2022.


FORRESTER®