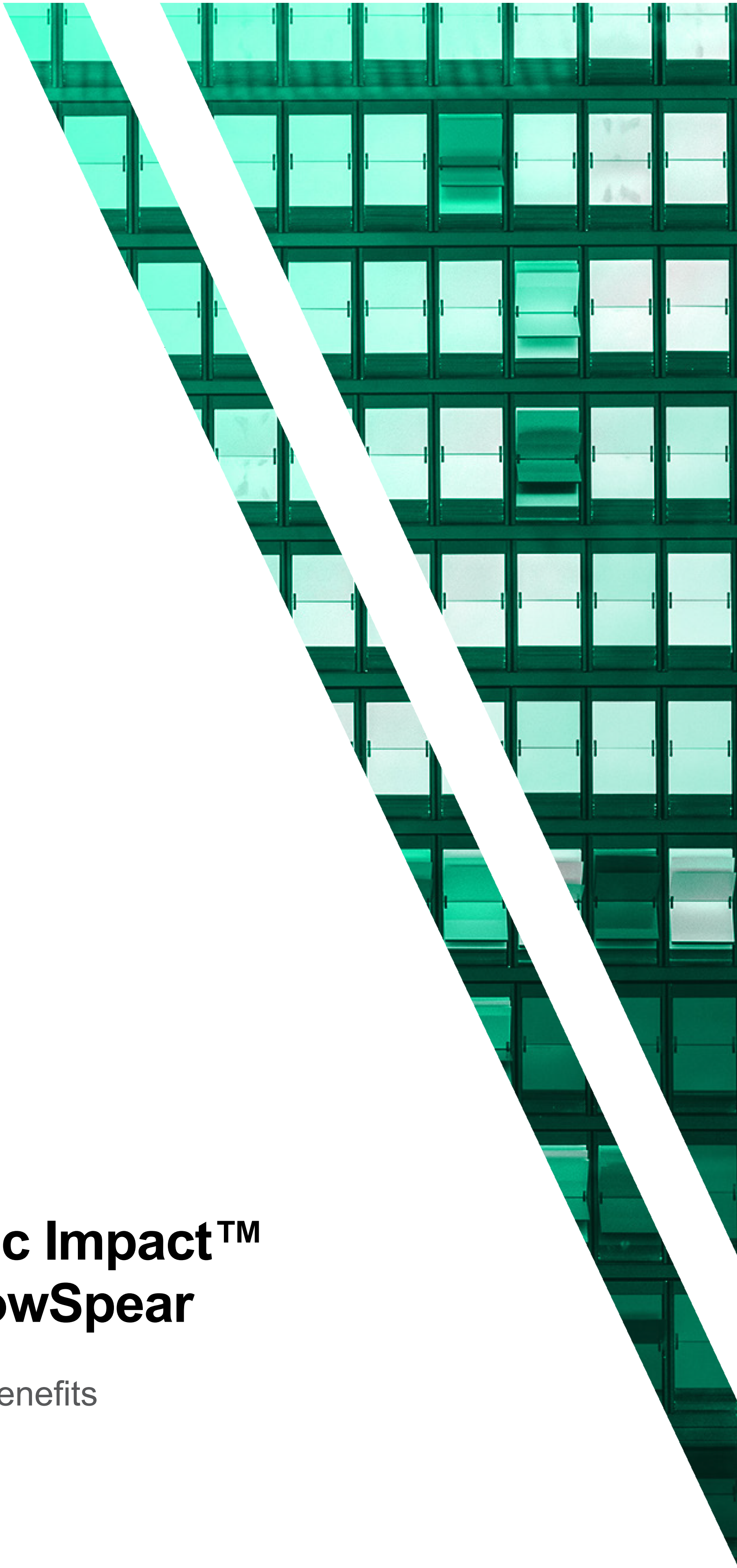


The Total Economic Impact™ Of SpearTip ShadowSpear

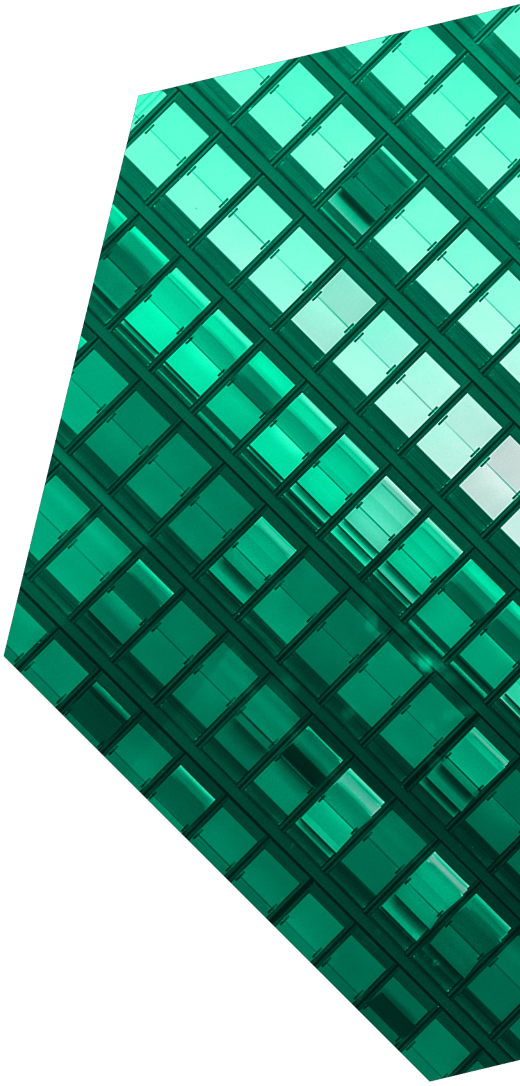
Cost Savings And Business Benefits Enabled By ShadowSpear

OCTOBER 2021

A FORRESTER TOTAL ECONOMIC IMPACT™ STUDY COMMISSIONED BY SPEARTIP

Table Of Contents

Consulting Team: Andre Girard



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 cybersecurity threat landscape has never been more treacherous. The frequency and sophistication of attacks is on the rise. Organizations are overwhelmed trying to keep pace, facing hiring challenges due to scarce and expensive skilled resources; recognizing 24/7/365 coverage is crucial; and trying to stay current with cybersecurity software capabilities. Adding the capabilities of a security operations-as-a-service platform like SpearTip's ShadowSpear could control costs while providing protection.

KEY STATISTICS

Return on investment (ROI)
254%

Net present value (NPV)
$1.91M

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

SpearTip is a cybersecurity managed service provider that maintains a 24/7/365 security operations center (SOC). The company offers cloud-based cyber counterintelligence services to help protect organizations by identifying and minimizing their cyber risk and vulnerabilities. Services provided include incident/breach response, security advisory services, and ShadowSpear, SpearTip's proprietary SOC-as-a-service platform. ShadowSpear provides enterprise detection and response visibility, cloud security information and event management (SIEM), and prevention technology.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four decision-makers with experience using ShadowSpear. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization.

Prior to using SpearTip ShadowSpear, the customers managed security independently with teams comprising IT technicians who had limited cybersecurity experience and utilized point solutions providing differing levels of visibility to network elements. These organizations found that staffing, equipping, and maintaining an in-house SOC was outside their areas of expertise and often prohibitively expensive. They recognized that bad actors were getting more sophisticated and were acting more frequently; they were not in a position to know if they had the right software, the right level of staffing, or the right training and certifications to keep up with the ongoing threats.

Only one customer monitored alerts with a team staffed 24/7, and the organizations' self-assessed degree of cybersecurity system-monitoring coverage ranged from 5% to 99% of their endpoints. Before using ShadowSpear, two of the organizations utilized SpearTip Incident Response services to investigate and neutralize a ransomware attack; one of the customers learned of SpearTip as a result of one its clients bringing SpearTip in due to an insurance broker referral.

Because of their investment in ShadowSpear, the organizations:

- Gained a managed security services partner that monitors, identifies, and neutralizes cyberthreats around the clock.
- Improved operational efficiency by consolidating all security notifications and progress updates on the ShadowSpear dashboard, reducing false alerts, and reallocating technicians to other tasks.
- Reduced their expenditures for dedicated security software and infrastructure.
- Have not had any ransomware attacks since utilizing ShadowSpear services.
- Gained an awareness of their cybersecurity protection level and experienced a trust level that takes cybersecurity out of their daily concerns and activities.

KEY FINDINGS

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

- **Data breach risk reduction valued at $1.1 million.** The interviewees described many ways that ShadowSpear improved their previous processes for preventing breaches. The shift to 24/7/365 coverage was considered essential due to attacks frequently occurring during off-hours and holidays.
- **Security team efficiency gain valued at nearly $706,000.** Deploying ShadowSpear offloaded most network-monitoring responsibilities, improving productivity for customers' security teams. Interviewees addressed new initiatives by reallocating their security labor and budget. The added capabilities and expertise of SpearTip also accelerated the speed at which malicious activity was isolated, neutralized, and eliminated.
- **Reduction in on-premises labor, software, and infrastructure cost valued at more than $416,000.** The interviewees' organizations eliminated a significant portion of their security software licensing and supporting infrastructure costs. Some customers used the implementation of ShadowSpear to advance IT cloud migration projects.
- **Accelerate merger and acquisition activity due to confidence in cybersecurity protection valued at almost $424,000.** Some interviewees had confidence improvements extending all the way to their C-suite and there were no longer conflicts to move forward with M&A activities due to cybersecurity concerns.

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

- **Confidence in ShadowSpear's ability to keep pace with the evolving threat landscape.** Interviewees are confident that ShadowSpear is keeping ahead of bad actors with both its proprietary platform and its cybersecurity technical team.
- **Direct availability of SpearTip representatives.** Customers valued their managed security provider relationship with SpearTip and the ability to directly reach a security technician without working through a call center if there were any questions or issues.
- **Avoiding alert fatigue.** Prior to implementing ShadowSpear, in-house security teams faced a flood of alerts, many of which were false-positives. SpearTip's singular focus on monitoring security provided interviewees with valuable confidence that issues would not be overlooked.
- **Gaining SpearTip as an extension of their team.** Customers valued the ready availability of SpearTip technicians and their frequent — and educational — discussions.

- **The collaborative culture of SpearTip.** Interviewees said the cooperative approach of SpearTip security analysts stood in contrast to experiences with other vendors.
- **Easy, disruption-free implementation.** Interviewees described ShadowSpear's implementation process as simple and quick. Organizations were eager to rapidly scale the deployments due to the minimal impact on IT staff and lack of business interruptions.
- **Improved employee satisfaction.** 24/7 availability of expertise and assistance from SpearTip educated and provided certainty about the right course of action that eased the minds of the customers' IT teams.

Costs. Risk-adjusted PV costs include:

- **Planning, implementation, and ShadowSpear contract cost, totaling $1.5 million over three years.** Planning was focused on aligning the customer's security team with ShadowSpear processes. ShadowSpear is a software-as-a-service (SaaS) solution, which means implementation is mainly interfacing with customers' data feeds. Training was minimal, focused on ShadowSpear's easy-to-use application. Licensing is also straightforward, based upon the number of endpoints.

The decision-maker interviews and financial analysis found that a composite organization experiences benefits of $2.66 million over three years versus costs of $751,000, adding up to a net present value (NPV) of $1.91 million and an ROI of 254%.

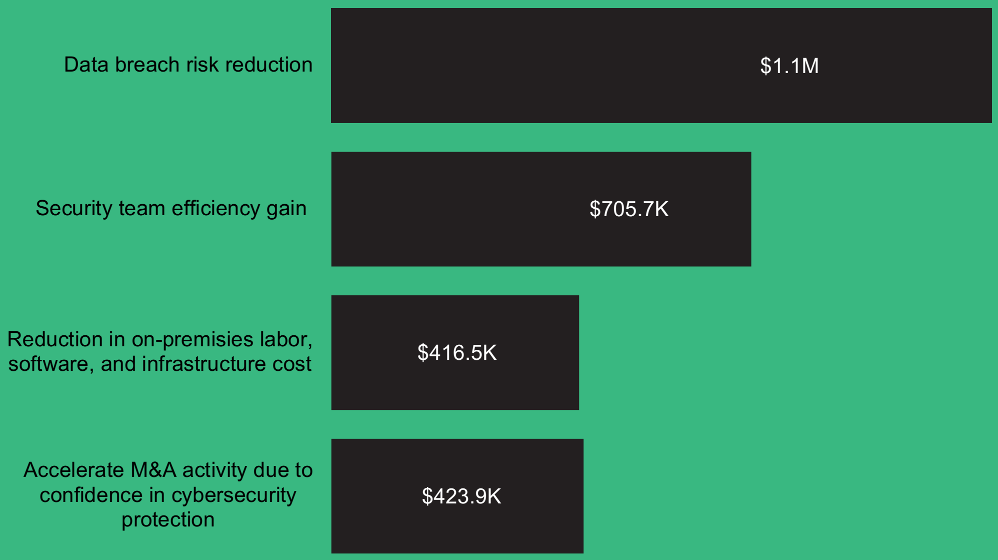
ROI
254%

BENEFITS PV
$2.66M

NPV
$1.91M

PAYBACK
<6 months

Benefits (Three-Year)



> “ShadowSpear supplied us with a complete security package for our cloud. I call it SOC-in-a-box. They came as a complete package to monitor threat and vulnerabilities. So it replaced any tool we would’ve used. We did not purchase a SIEM, network-monitoring software, or additional scanners — we’re using ShadowSpear.”— Director of threat and vulnerability management, financial services

TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in the ShadowSpear platform.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that ShadowSpear can have on an organization.

DUE DILIGENCE

Interviewed SpearTip stakeholders and Forrester analysts to gather data relative to ShadowSpear.

DECISION-MAKER INTERVIEWS

Interviewed four decision-makers at organizations using ShadowSpear 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 decision-makers.

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.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by SpearTip 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 SpearTip ShadowSpear.

SpearTip 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.

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

The SpearTip ShadowSpear Customer Journey

Drivers leading to the ShadowSpear investment

Interviewed Decision-Makers

Interviewee	Industry	Region	Endpoints Protected
Director of threat and vulnerability management	Financial services	Global	Companies interviewed had deployments of up to 15,000 endpoints
VP of technology	Managed IT service provider	North America	
Chief security officer (CSO)	Healthcare nonprofit	North America	
Co-founder	IT service provider	North America	

KEY CHALLENGES

Before the investment in SpearTip ShadowSpear, the interviewees' organizations internally managed their cybersecurity activities. However, they struggled to find and afford the specialized resources necessary to keep up with the continually evolving cybersecurity threat landscape. Recognizing the limits to this approach, some of the interviewees had investigated the use of managed security services vendors, seeking a partner that balanced deep expertise with flexibility and responsiveness.

The interviewees shared common challenges prior to their SpearTip ShadowSpear investment, including:

- **The scarcity and price premium of IT security technicians.** Decision-makers were unable to staff comprehensive cybersecurity teams due to the difficulty of finding specialized expertise and the price-premium of cybersecurity technicians over IT staff of comparable seniority.

- **Gaps in security-monitoring coverage.** Interviewees said that their midsized organizations struggled to find the staffing and budget to provide 24/7/365 coverage on their own. Security was often the part-time responsibility of several IT staff, rather than the provenance of a dedicated security group.

- **Budget constraints limiting scope of security coverage.** Interviewees' organizations found it difficult to afford extending their security monitoring to all endpoints. A VP of technology with a managed IT service provider said that prior to ShadowSpear, cost limited their security monitoring to only cover 5% of their endpoints.

- **Disparate tooling systems and processes that lacking automation.** Interviewees' security teams wasted time and risked overlooking security events by needing to log into multiple systems that lacked integration. Security processes were similarly disjointed.

- **The frequency and sophistication of cyberattacks were increasing.** Threat actors continue to evolve — launching attacks more frequently, finding new attack vectors, and developing more advanced techniques — making it ever-more critical for organizations to harden their IT security.

> **"We reached a point where we realized that building our own SOC team wasn't the best choice for us. Part of it was that we realized that it would take a long time to build out a true SOC team, and we wouldn't be able to effectively support our clients at a reasonable cost."**
>
> *VP of technology, managed IT service provider*

SOLUTION REQUIREMENTS/INVESTMENT OBJECTIVES

The interviewees' organizations searched for a solution that could:

- Provide a SIEM solution that extends their security architecture to monitor 100% of IT endpoints.
- Reduce the likelihood and impact of data breaches.
- Shift monitoring, investigation, and recovery activities to a cybersecurity service provider with specialized expertise.
- Respond rapidly to security incidents with a SOC that provides full 24/7/365 availability.

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 decision-makers that Forrester interviewed and is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The composite organization is a North America-based, midsized enterprise. It has 5,000 endpoints, comprising internal devices and those monitored for their clients. The organization monitors, investigates, and conducts recovery with an in-house team of IT technicians lacking specialized cybersecurity backgrounds.

The maturity of the organization's cybersecurity strategy is considered basic: meaning it has limited internal cybersecurity team expertise, a lack of full 24/7/365 active monitoring, and security tooling with incomplete capabilities or integration.

Key assumptions

- **Midsized corporation**
- **Basic security maturity level**
- **5,000 endpoints**
- **Internally managing cybersecurity**
- **Lacking full endpoint visibility and security**

Deployment characteristics. The composite organization's interaction with SpearTip began with a cybersecurity incident response (IR). The composite company subsequently expanded its engagement with SpearTip by utilizing ShadowSpear, the service this TEI covers, to address the cybersecurity needs of its endpoints (internal and clients').

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	Data breach risk reduction	$438,445	$446,919	$456,241	$1,341,605	$1,110,722
Btr	Security team efficiency gain	$261,000	$285,300	$309,600	$855,900	$705,665
Ctr	Reduction in on-premises labor, software, and infrastructure cost	$164,250	$167,625	$171,169	$503,044	$416,453
Dtr	Accelerated M&A activity due to confidence in cybersecurity protection	$56,250	$174,375	$304,313	$534,938	$423,882
	Total benefits (risk-adjusted)	$919,945	$1,074,219	$1,241,322	$3,235,487	$2,656,722

DATA BREACH RISK REDUCTION

Evidence and data. SpearTip ShadowSpear provided customers with a unified SOC as a service that helped discover, isolate, and respond to malicious activities on their networks. The interviewees recognized the additional security capabilities their organization gained by utilizing ShadowSpear.

- ShadowSpear provided 100% visibility into the organizations' networks and the expertise to recognize threats that the interviewees' security teams did not see.

- All of the interviewees recognized that ensuring cybersecurity has never been more critical as the capabilities and sophistication of threat actors continues to rapidly evolve.

- Prior to implementing ShadowSpear, SpearTip's IR services helped two of the four interviewee organizations recover from ransomware attacks. Since implementing ShadowSpear, none of the organizations has suffered a data breach.

- ShadowSpear monitored the interviewees' environments 24/7/365 and could start acting against threats at times when their organizations did not have internal support.

- Utilizing ShadowSpear saved interviewees the expense and delay of building, equipping, and staffing an in-house SOC that could operate around the clock and keep pace with an ever-evolving threat landscape. A CSO at a healthcare nonprofit explained, "We didn't have in-house expertise, and trying to hire and build that out internally just wasn't cost effective — it didn't make sense."

- The interviewees noted that SpearTip worked collaboratively with their IT security teams to rapidly neutralize attacks and reduce the likelihood of their recurrence. The co-founder of

> **"The frequency of events was rising, and the attacks were becoming more sophisticated, going from recovering from backups to business-crippling attacks."**
>
> *VP of technology, managed IT service provider*

an IT service provider said, “SpearTip worked hand in hand with my teammates and went right to work coaching us on how to put a stop to this whole thing.”

> **“We had all the things in place to catch 99.9% of anything that might come in. We had everything in place to catch everything except what ultimately led me to SpearTip. We had an attack from the inside — I had never contemplated [malware that had been hidden in an acquired business’ server that was awakened by a simple adjustment by an IT technician].”**
>
> *Co-founder, IT service provider*

Modeling and assumptions. Forrester assumes the following about the composite organization:

- Forrester used research statistics for the number of breaches per year at a typical maturity level, the average cost per data breach exclusive of internal user downtime, and the average hourly cost per employee.[2]
- The composite organization comprises a combination of 4,500 employees and customers’ employees.
- Shadowspear reduces the probability the composite organization experiences a data breach by 55%, due to the very basic maturity level of the comp.
- Organizations can expect each breach to impact 5% of all employees. This is an additional cost to the points above.

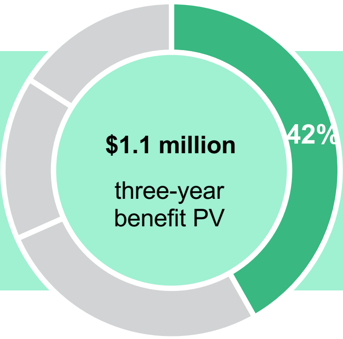
Risks. Risks that could impact the realization of this benefit include:

- The maturity of organization’s previous security architecture and strategy.
- The percentage of employees and customers impacted by the breach and the duration of associated downtime.
- The organization’s location, size, and industry.

> **“Within an hour of me calling them, they were in my network and doing their thing.”**
>
> *Co-founder, managed IT service provider*

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 more than $1.1 million.

Data breach risk reduction:
42% of total benefits



Data Breach Risk Reduction

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Average number of data breaches per year	Forrester research	2.5	2.5	2.5
A2	Average potential cost of a data breach, exclusive of end-user downtime	Forrester research	$302,637	$302,637	$302,637
A3	Reduced likelihood of a breach	Interviews	55%	55%	55%
A4	Subtotal: avoided costs of remediation, customer resolution, fines, brand rebuild, and all other external-facing costs	A1*A2*A3	$416,126	$416,126	$416,126
A5	Number of employees (internal and customer)	Composite	4,500	4,950	5,445
A6	Average salary — business user (hourly)	Payscale.com	$38	$38	$38
A7	Diminished/eliminated user productivity hours per breach	Forrester research	3.6	3.6	3.6
A8	Average percentage of employees affected per breach	Forrester research	20%	20%	20%
A9	Productivity recapture	Interviews	80%	80%	80%
A10	Subtotal: cost of reduced end-user productivity	A5*A6*A7*A8*A9	$99,692	$109,662	$120,628
At	Data breach risk reduction	A4+A10	$515,818	$525,787	$536,754
	Risk adjustment	↓15%			
Atr	Data breach risk reduction (risk-adjusted)		$438,445	$446,919	$456,241
	Three-year total: $1,341,605		Three-year present value: $1,110,722		

SECURITY TEAM EFFICIENCY GAIN

Evidence and data. Upon implementing ShadowSpear, the interviewees' organizations shifted cybersecurity monitoring, analysis, and incident resolution to SpearTip. Decision-makers reduced labor costs by refocusing an average of two security technicians onto other initiatives and eliminating a 20% (FTE) yearly expansion of their security (team) staff. Interviewees eliminated $20,000 of annual training and certification expenditures for in-house staff due to their trust in the around-the-clock availability and deep cybersecurity expertise of SpearTip analysts.

- Alerts and updates on issues and mitigation efforts are available through the ShadowSpear dashboard. Interviewees noted that the ability to

> **"If I had to hire staff to do these same types of security initiatives, it would cost me two, three times as much as what I'm paying SpearTip. It gives me a little more freedom to use those dollars to repurpose and bring in other talent to do things that are going to help move the business forward financially."**
>
> *CSO, healthcare nonprofit*

focus on only the ShadowSpear user dashboard instead of multiple separate systems streamlined the effort of their security team. The CSO at a healthcare nonprofit estimated that it increased his technicians' efficiency by 20% to 25%, freeing them to work on other tasks.

- Interviewees shared that IT security technicians with appropriate expertise and certifications were hard to find. As the director of threat and vulnerability management at a financial services organization explained: "Finding enough people capable of doing this work and immediately training them up is just too heavy of a lift. Avoiding that freed up valuable resources."

"We needed to establish a SOC for the cloud. That means hiring a leader and multiple associates with appropriate skills and implementing multiple tools as we shifted from on-prem to what would be best for our cloud environment. It probably would have taken a year to bring in the talent and new cloud-focused tools, and to develop the necessary APIs, all while keeping up with the implementation we had already begun."

Director of threat and vulnerability management, financial services

- Customers noted that high demand for cybersecurity expertise drove labor rates for these technicians 25% higher than IT staff of comparable seniority. In comparison to this price-premium for direct hires, ShadowSpear licensing provided significant cost savings for the interviewees. Noted the CSO at a healthcare nonprofit: "The cost model made sense. Cost is always a driving factor, and if you try to drill into bringing high-level security engineers onboard, you can't compete. It would just not be worth it."

- Shifting most of the alert-monitoring responsibility to ShadowSpear allowed customers to reallocate their security budget. Interviewees eliminated the expense and delay of building and staffing an in-house SOC. A VP of technology from a managed IT service provider said, "Instead of hiring a couple analysts just to monitor security events all day for clients, we now just add these SpearTip alerts on top of an existing department's day-to-day operations because it's not that much time."

Modeling and assumptions. Based on customer interviews, Forrester estimates the following for the composite organization:

- The cybersecurity team FTEs represent labor required for risk reduction, monitoring, analysis, and recovery roles within the IT organization.

- The specialized skills and expertise required for IT security professionals are in high demand and increase average compensation approximately 25% higher than for IT roles with a similar seniority level.

- The average fully burdened salary for the IT security team is $135,000 annually.

- The rapidly evolving cybersecurity threat landscape necessitates yearly staffing growth and ongoing professional training and certification.

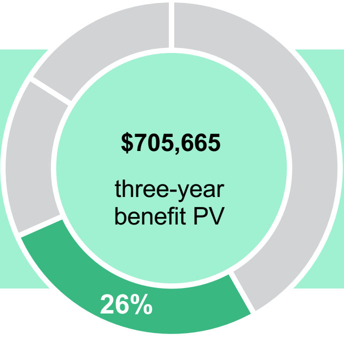
Risks. The reduction in security labor, training, and certification cost will vary with:

- The size and labor cost of the security team.

- The extent and pace at which the organization transitions security monitoring, analysis, and recovery responsibilities to SpearTip.
- The extent of security training provided to staff.
- Certification requirements for professionals in specific industries or security roles.

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 nearly $706,000.

Security team efficiency gain: **26%** of total benefits



Security Team Efficiency Gain

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Security labor reallocation (FTE)	Interviews	2.0	2.2	2.4
B2	Annual labor cost	Payscale.com	$135,000	$135,000	$135,000
B3	Subtotal: total security labor savings	B1*B2	$270,000	$297,000	$324,000
B4	Security training and certification savings	Interviews	$20,000	$20,000	$20,000
Bt	Security team efficiency gain	B3+B4	$290,000	$317,000	$344,000
	Risk adjustment	↓10%			
Btr	Security team efficiency gain (risk-adjusted)		$261,000	$285,300	$309,600
	Three-year total: $855,900			**Three-year present value: $705,665**	

REDUCTION IN ON-PREMISES LABOR, SOFTWARE, AND INFRASTRUCTURE COST

Evidence and data. Customers benefited from the ShadowSpear deployment by refocusing internal IT team labor spent on security-related tasks back to their core system administration responsibilities. The interviewees' organizations realized additional value by reducing existing security software license costs and associated infrastructure expenditures and by accelerating their technology modernization schedules.

- The interviewees noted that ShadowSpear improved the efficiency of their IT staff by filtering all of the alerts and forwarding only actionable items.
- Upon implementing ShadowSpear, interviewees' organizations reduced their security software license expenses by eliminating tools that were no longer used and avoiding the purchase of new software packages.
- Interviewees reduced their on-premises IT infrastructure as the responsibility to store security log files shifted to SpearTip and older security solutions, many of which were purchased outright and maintained locally, were eliminated. One interviewee noted that they removed a server at each of their client locations.

- Utilizing ShadowSpear lowered IT labor expenses previously dedicated to security by reducing time wasted monitoring multiple systems for security events on in-house and client networks. A VP of technology at a managed IT service provider said: “It saved a tremendous amount of time. The techs can have multiple responsibilities now because they won’t have to full-time just monitor and look, sift through all these alerts and stuff.”
- Several interviewees accelerated a larger organizational goal of moving to the cloud by reducing the volume of traditional server hardware as part of their ShadowSpear implementation.

> **“We didn’t have a dedicated group focused on security, we just had people doing that. And now we just don’t need to do that because SpearTip is such a good partner.”**
>
> *CSO, healthcare nonprofit*

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

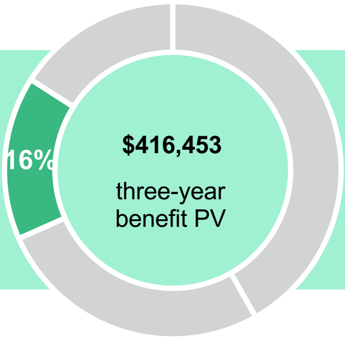
- Customers eliminated some of their cybersecurity software after implementing ShadowSpear. Note that some of the software was owned, not on an annual subscription model.
- Security software license costs under subscription pricing increase at 5% per year.
- Portions of IT infrastructure dedicated security are repurposed.
- The average fully burdened salary for a member of the IT team is $110,000 annually.

Risks. Realization of this benefit could be impacted by the following risks:

- The percentage of IT labor focused on cybersecurity.
- The average salary for IT staff.
- The number of endpoints protected by ShadowSpear.
- The amount of security software that is licensed, rather than owned outright, and can be eliminated for a cost savings.
- The impact that ShadowSpear has on an organization’s IT infrastructure compared to its previous security architecture.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of more than $416,000.

Reduction in on-premises labor, software, and infrastructure cost: **16%** of total benefits



Reduction In On-Premises Labor, Software, And Infrastructure Cost

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Eliminated/reduced software licenses (SIEM only)	Interviews	$75,000	$78,750	$82,688
C2	Repurposing of IT labor (FTE)	Interviews	0.25	0.25	0.25
C3	Annual IT labor cost	Payscale.com	$110,000	$110,000	$110,000
C4	Total repurposing of IT labor	C2*C3	$27,500	$27,500	$27,500
C5	Infrastructure cost reduction	Interviews	$80,000	$80,000	$80,000
Ct	Reduction in on-premises labor, software, and infrastructure cost	C1+C4+C5	$182,500	$186,250	$190,188
	Risk adjustment	↓10%			
Ctr	Reduction in on-premises labor, software, and infrastructure cost (risk-adjusted)		$164,250	$167,625	$171,169
	Three-year total: $503,044		**Three-year present value: $416,453**		

ACCELERATED M&A ACTIVITY DUE TO CONFIDENCE IN CYBERSECURITY PROTECTION

Evidence and data. Interviewees said that the capabilities of ShadowSpear and the expertise and support available from SpearTip as a security partner allowed them to focus on growth initiatives. Recognition that cybersecurity threats were monitored and controlled gave decision-makers the confidence to invest in business expansion.

- Interviewees noted that ensuring cybersecurity is addressed has become an increasingly vital and resource-consuming business priority. Implementing ShadowSpear provided the time and energy to focus on other initiatives. As the CSO of a healthcare nonprofit said, “It gave me the luxury to focus on other core solutions to help move the business forward.”
- A co-founder of an IT service provider explained how the SpearTip team and the ShadowSpear service are a central part of his organization’s investigation and acquisition process. SpearTip is brought in to immediately analyze and wrap the acquired infrastructure in ShadowSpear protection upon finalization of the transaction.

> **“SpearTip completely saved that investment for me and my partners. I’m going the distance with ShadowSpear.”**
>
> *Co-founder, managed IT service provider*

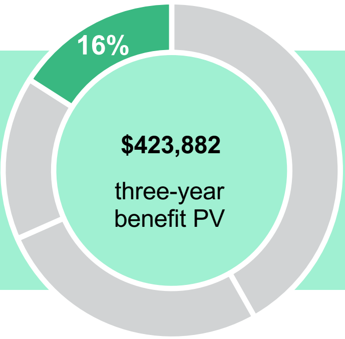
Modeling and assumptions. For the composite organization, Forrester assumes that:

- Trust in the organization’s cybersecurity protection level by decision-makers and investors allows consideration of business expansion.
- The organization operates in a market segment in which consolidation is possible.

Risks. The impact of this benefit could vary based on the revenue of acquired companies; an organization’s ongoing business growth and expansion strategy; and its location, size, and industry.

Results. To account for these risks, Forrester adjusted this benefit downward by 25%, yielding a three-year, risk-adjusted total PV of nearly $424,000.

Accelerated M&A activity due to confidence in cybersecurity protection: **16%** of total benefits



Accelerated M&A Activity Due To Confidence In Cybersecurity Protection

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	New revenue due to additional M&A activity	Interviews	$750,000	$1,500,000	$1,500,000
D2	Recurring revenue due to additional M&A activity (10% annual growth)	1.1*(D1(y-1) +D2(y-1))		$825,000	$2,557,500
D3	Total additional revenue due to M&A activity	D1+D2	$750,000	$2,325,000	$4,057,500
D4	Net margin	Estimate	10%	10%	10%
Dt	Accelerated M&A activity due to confidence in cybersecurity protection	D3*D4	$75,000	$232,500	$405,750
	Risk adjustment	↓25%			
Dtr	Accelerated M&A activity due to confidence in cybersecurity protection (risk-adjusted)		$56,250	$174,375	$304,313
	Three-year total: $534,938		**Three-year present value: $423,882**		

UNQUANTIFIED BENEFITS

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

- **Confidence in ShadowSpear's ability to keep pace with the evolving threat landscape.** Interviewees were confident that ShadowSpear is keeping ahead of bad actors with both its proprietary platform and its cybersecurity technical team. SpearTip engineers can rapidly develop new integrations or respond to new threats without waiting on external vendors. As the director of threat and vulnerability management at a financial services organization said, "Their ability to write their own APIs gives us a lot of comfort and was reaffirming of our decision."

- **Direct availability of SpearTip representatives.** Customers valued their relationship with SpearTip and the ability to directly reach a security technician without working through a call center if they had questions or encountered any issues. The CSO of a healthcare nonprofit said that one of the reasons they did not go with a competitor was because "they didn't provide me the person that I could reach out and touch — that single throat to choke."

- **Avoiding alert fatigue.** One interviewee admitted that the sheer number of alerts — and that the vast majority of them are false-positive — had led to alert fatigue among his technicians. SpearTip's singular focus on monitoring security provided valuable confidence that issues would not be overlooked.

- **Gaining SpearTip as valuable team member.** A CSO at a healthcare nonprofit explained: "They are an extension of my team. I bring them into board meetings to speak of cybersecurity, their solutions, and what's out there in the dark web. That comfort is extremely important to me, my team, and the board."

- **The collaborative culture of SpearTip.** Several interviewees noted the cooperative teamwork approach of SpearTip security analysts and highlighted the contrast to their experiences with other vendors. Customers highlighted this quality as a driving factor in plans to expand their engagement with SpearTip.

- **Easy, disruption-free implementation.** A CSO at a healthcare nonprofit said: "SpearTip's implementation process was pretty seamless — no disruption to the business. There was no impact to any of the other services or cloud solutions we had."

> **"I was impressed with how [SpearTip] handled things and communicated while they were doing a client's attack recovery. They were very, very cooperative, and very willing to explain what their software was, what it did, how to work through the incident response plan, what forensic data they actually needed. It was a very different experience than some encounters I had with potential partners."**
>
> *VP of technology, managed IT service provider*

- **Improved employee satisfaction.** 24/7 availability of expertise and assistance from SpearTip educated customers' IT technicians and provided certainty about the right course of action, easing the minds of their teams. Knowing SpearTip was monitoring around the clock helped them sleep at night.

FLEXIBILITY

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

- **Easing the transition to a distributed workforce.** The COVID-19 pandemic spurred a transformational shift to widespread remote workforces. The SaaS-based delivery model of ShadowSpear natively supports maintaining endpoint security-monitoring capabilities as their locations change — without needing to do any remapping. A VP of technology with a managed IT service provider said: "With a lot of people working from their homes or from unmanaged equipment connecting to the corporate network, ShadowSpear reduced the risk by having visibility to all of the endpoints."
- **Acceleration of cloud initiatives**. Prior to the investment in ShadowSpear, interviewees' organizations managed security with a combination of point solutions. Shifting to ShadowSpear reduced the volume of on-premises software and accelerated their transition to a virtual IT infrastructure in the cloud.
- **Gaining a flexible vendor.** Interviewees said one of the reasons their organizations chose — and stayed with — SpearTip was because of their flexibility. ShadowSpear pricing based on the number of endpoints protected made it easy for customers to scale up their engagement. Interviewees also valued SpearTip's flexibility in processes and openness to requests or suggestions.

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

"SpearTip can keep up better than some larger organizations. They're more like a sports car than a tank — a little bit more nimble, a little bit more agile at this point, which is what you need to keep up with cybersecurity right now."

Director of threat and vulnerability management, financial services

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
Etr	Planning, implementation, and ShadowSpear contract cost	$22,000	$267,300	$294,030	$323,433	$906,763	$751,000
	Total costs (risk-adjusted)	$22,000	$267,300	$294,030	$323,433	$906,763	$751,000

PLANNING, IMPLEMENTATION, AND SHADOWSPEAR CONTRACT COST

Evidence and data. All four interviewees found the implementation process to be relatively seamless; there were no business disruptions. Planning was straightforward, mostly focused on clarifying roles between SpearTip's SOC and the customer's security and IT teams. Licensing is based upon the number of endpoints.

- ShadowSpear technology is a SaaS-based solution, so no installation was required. SpearTip's team had appropriate APIs to effectively source necessary log files.
- Communications processes and roles were determined quickly and without any confusion.
- SpearTip ShadowSpear implementation includes installation support and initial training.

> **"A service like what SpearTip offers is going to become as normal as the light bill over the next few years. There is no other way."**
>
> *Co-founder, IT service provider*

> **"I like the simplicity of their pricing, an all-in-one monthly per-workstation cost. Instead of worrying about how much data was being ingested and net pay for certain levels of service, it is great having an all-encompassing price."**
>
> *VP of technology, managed it service provider*

Modeling and assumptions. Forrester assumes the following about the composite organization:

- Licensing costs for ShadowSpear are based on the number of monitored (virtual or physical) endpoints, with volume-based discounts.
- Implementation support and training is provided by SpearTip and included in the base price of ShadowSpear.

Risks. Forrester identified the following risks associated with the planning, implementation, and ShadowSpear contract costs:

- Licensing will vary based on negotiated terms.
- Licensing volume will change over time.

- Planning and implementation will vary due to organization readiness and complexity of the technical environment.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $751,000.

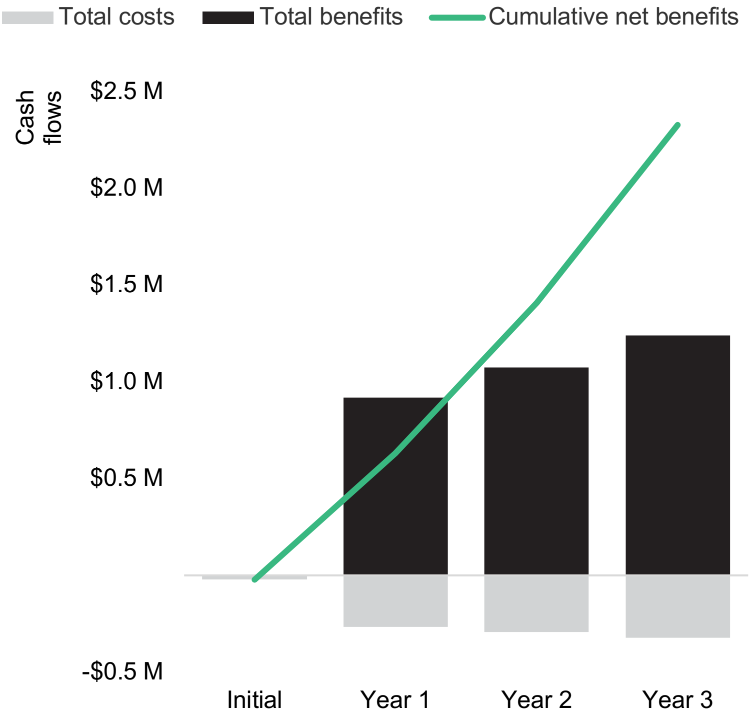
Planning, Implementation, And ShadowSpear Contract Cost

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
E1	Planning and implementation	Interviews	$20,000			
E2	ShadowSpear contract	Interviews		$243,000	$267,300	$294,030
Et	Planning, implementation, and ShadowSpear contract cost	E1+E2	$20,000	$243,000	$267,300	$294,030
	Risk adjustment	↑10%				
Etr	Planning, implementation, and ShadowSpear contract cost (risk-adjusted)		$22,000	$267,300	$294,030	$323,433
	Three-year total: $906,763			Three-year present value: $751,000		

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	($22,000)	($267,300)	($294,030)	($323,433)	($906,763)	($751,000)
Total benefits	$0	$919,945	$1,074,219	$1,241,322	$3,235,487	$2,656,722
Net benefits	($22,000)	$652,645	$780,189	$917,889	$2,328,724	$1,905,722
ROI						254%
Payback (months)						<6

Appendix A: Total Economic Impact

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

TOTAL ECONOMIC IMPACT APPROACH

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

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

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

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

The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV Sources are calculated for each total cost and benefit estimate. NPV Sources in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value Sources 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] 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: "Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q4 2020."

FORRESTER®