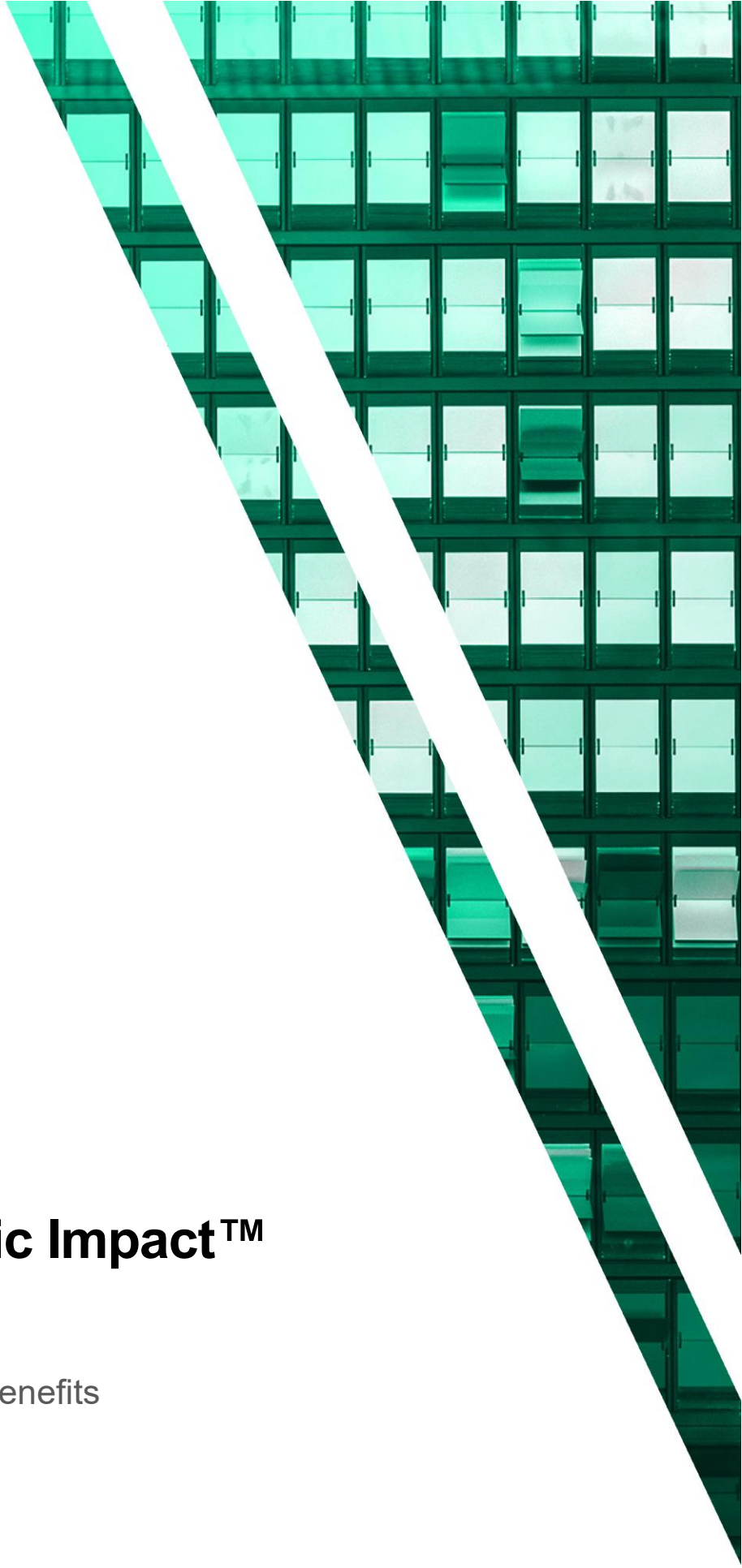
FORRESTER®



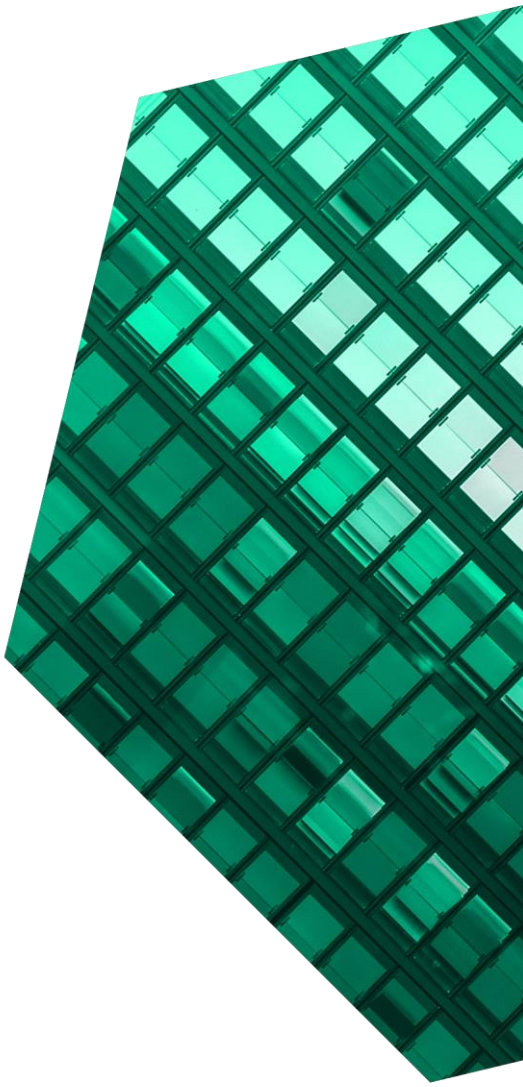
The Total Economic Impact™ Of Arctic Wolf

Cost Savings And Business Benefits Enabled By Arctic Wolf

OCTOBER 2023

Table Of Contents

Consulting Team: Sam Sexton
Matt Dunham
Henry Huang



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

In today's threat landscape, security teams need advanced technology and reliable expertise to detect and respond to sophisticated cyberattacks. Failure risks security breaches, lost revenue from partners, and damage to employee productivity. However, security teams lack the bandwidth to sift through alerts and respond to potential incidents. To ensure 24/7 protection, firms need to drastically increase staffing to manage the ever-increasing number of threats — but many cannot afford to do so.

Arctic Wolf enables security teams to effectively detect, prioritize, investigate, and respond to security alerts with 24/7 managed detection and response. In addition to its threat response technology, Arctic Wolf security operations solutions include ongoing risk management, security awareness training, and cyber incident response services that provide customers with readily available guidance to help them improve their overall security posture.

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

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four representatives with experience using Arctic Wolf. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that is a company with 800 employees and $50 million in annual revenue.

KEY STATISTICS

Return on investment (ROI)
414%

Net present value (NPV)
$1.11M

90%
Reduction in the likelihood and impact of a breach

Prior to using Arctic Wolf, these interviewees noted how their organizations had a variety of security alert solutions in place but did not have an existing 24/7 managed detection and response solution. As the threat of cyberattacks increased, interviewees' customers began asking them to implement round-the-clock security monitoring to protect sensitive data. However, the interviewees lacked the budget and the personnel to provide the 24/7 threat detection that customers requested. Additionally, the existing security team had limited visibility into various alerts and vulnerabilities in the security ecosystem.

After the investment in Arctic Wolf, the interviewees significantly improved their security posture, enabling them to reduce the likelihood and impact of a security breach and retain key customers. Additionally, Arctic Wolf drastically reduced the amount of time security teams spent investigating and responding to security

incidents, leading to substantial time and labor savings.

KEY FINDINGS

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

- **Over 90% reduction in time spent investigating security incidents.** Prior to implementing Arctic Wolf, the composite organization would spend an average of 10 hours investigating each ticketed security incident. With Arctic Wolf, the organization is able to quickly analyze the relevant data and endpoint information to understand the incident, streamlining the incident review process. Over the course of the three-year analysis, this benefit is valued at $124,000.
- **Reduced likelihood and impact of a security breach by 90%.** By enabling the composite organization to investigate more incidents, the investment in Arctic Wolf reduces the likelihood of a breach by approximately 90%. Arctic Wolf also minimizes the time employees need to spend responding to such breaches and allows the composite organization to remediate incidents faster than previously, leading to a sharp decline in the impact of a security breach. In total, this benefit is valued at $404,000 over three years.
- **Avoided revenue loss from improved customer retention.** The composite organization works with customers in sensitive industries that require their information be protected by a 24/7 managed detection and response system. After implementing Arctic Wolf, the composite organization improves customer retention, equating to a risk-adjusted $856,000 over the three years.

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

- **Improvement in understanding of security posture.** Arctic Wolf assigns a dedicated team of cybersecurity experts to each organization to provide their security teams with custom guidance. This allows the composite organization to improve its security expertise and proactively adjust its protocols to strengthen its security posture.
- **Simpler, more affordable purchasing of cybersecurity insurance.** With Arctic Wolf, the composite organization reduces its overall risk profile, making it easier to obtain favorable insurance coverage terms and potentially lower premiums.

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

- **Licensing costs of $232,000.** Arctic Wolf charges the composite organization based on the number of employees and the number of servers.
- **Implementation and maintenance costs $37,000.** The composite organization has two internal employees that devote part of their time to implementing Arctic Wolf, while one employee dedicates a portion of their time to the ongoing maintenance of the platform.

The representative interviews and financial analysis found that a composite organization experiences benefits of $1.38 million over three years versus costs of $269,000 adding up to a net present value (NPV) of $1.11 million and an ROI of 414%.

ROI
414%

BENEFITS PV
$1.38M

NPV
$1.11M

PAYBACK
<6 months

Benefits (Three-Year)

“I can go home at night and not worry about security. … If something goes wrong, I’m going to get a call. I got my weekends back.”

— CIO, HVAC solutions

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 Arctic Wolf.

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 Arctic Wolf can have on an organization.

Forrester Consulting conducted an online survey of 351 cybersecurity leaders at global enterprises in the US, the UK, Canada, Germany, and Australia. Survey participants included managers, directors, VPs, and C-level executives who are responsible for cybersecurity decision-making, operations, and reporting. Questions provided to the participants sought to evaluate leaders' cybersecurity strategies and any breaches that have occurred within their organizations. Respondents opted into the survey via a third-party research panel, which fielded the survey on behalf of Forrester in November 2020.

DUE DILIGENCE

Interviewed Arctic Wolf stakeholders and Forrester analysts to gather data relative to Arctic Wolf.

INTERVIEWS

Interviewed four representatives at organizations using Arctic Wolf to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewees' organizations.

FINANCIAL MODEL FRAMEWORK

Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewees.

CASE STUDY

Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

The Arctic Wolf Customer Journey

Drivers leading to the Arctic Wolf investment

Interviews			
Role	**Industry**	**Annual Revenue**	**Employees**
Director of IT	Law	$26 million	200
CIO	HVAC solutions	$100 million	100
VP of IT	Building supply distribution	$24 million	200
IT director	Construction services	$570 million	1,500

KEY CHALLENGES

Prior to the investment in Arctic Wolf, the interviewees had a variety of security tools in place but lacked a 24/7 threat detection tool. The interviewees noted how their organizations struggled with common challenges, including:

- **Minimal bandwidth on the security team.** The interviewees shared that their security teams did not have the staff to provide the 24/7 coverage that some of their customers were asking for. As cybersecurity became an increasingly salient concern for clients, the interviewees' organizations risked losing customers to firms with round-the-clock security monitoring, since they lacked the budget for additional hires. The IT director at the construction services firm shared, "We couldn't expect a small network team to be available 24/7 and keep an eye on all the data that's coming from all of our different security tools."
- **Limited visibility into the networks.** The interviewees' organizations had limited visibility and contextual information into various alerts and vulnerabilities that appeared in their security systems. The lack of visibility made it difficult to proactively identify and respond to threats, increasing the risk of security breaches. The VP of IT at the building supply distributor noted: "We wouldn't get alerted when it was a small problem. We'd get alerted when it was becoming a bigger problem."
- **Lack of in-house security expertise.** Interviewees reported that their organizations lacked the necessary expertise to optimize their security best practices, negatively impacting their overall security posture. The VP of IT at the building supply distributor described why a stronger security system was necessary: "There were more and more hackers out there and it was becoming more and more of an issue in security and IT departments. It's always been an

> **"You either onboard a full-time security professional or you bring in a SIEM. For a fraction of the cost … Arctic Wolf was both a resource and cost-effective approach to solving the business need."**
>
> *Director of IT, law*

issue, but it keeps getting crazier and crazier every year."

- **Disorganized documentation.** Some interviewees noted that their organizations lacked a consistent documentation process. As a result, they could not create root causes analyses, much less a central information repository in its environment.
- **Increasing cost of cybersecurity insurance.** In recent years, cybersecurity insurance premiums have increased, particularly for firms with higher risk profiles. Interviewees noted that their lack of comprehensive security monitoring and incident response capabilities resulted in sharp premium hikes.

INVESTMENT OBJECTIVES

The interviewees' organizations searched for a solution that could:

- Offer 24/7 managed detection and response (MDR) security, supported by experienced cybersecurity professionals to augment their existing security staff.
- Improve the visibility of their overall security environments.
- Streamline their processes for documentation.

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of the four interviewees, and it is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The composite organization has 800 employees and an annual revenue of $50 million. The composite organization has a two-person security team and a variety of security alert solutions in place but does not have an existing MDR or security information and event management (SIEM) solution in place. The organization is industry-agnostic but deals with many clients in sensitive industries or industries that are subject to intense scrutiny and regulation around their cybersecurity environment.

Deployment characteristics. The composite organization adopts Arctic Wolf's 24/7 MDR solution to increase the number of threats it can detect and respond to without having to increase the size of its security team. As part of the deployment, the organization also gains access to a dedicated security concierge, who advises the organization on active threats, vulnerabilities, and security best practices. By improving the composite organization's security posture, Arctic Wolf enables the composite organization to assure its customers that their information is protected.

Key Assumptions

- **$50 million annual revenue**
- **800 employees**
- **Two security FTEs**
- **No existing MDR/SIEM**
- **Heavy client base in sensitive industries**

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits

Ref.	Benefit	Initial	Year 1	Year 2	Year 3	Total	Present Value
Atr	Time savings on triage and investigation of security incidents	$0	$43,346	$50,065	$57,825	$151,235	$124,226
Btr	Avoided and reduced impacts of security breach	$0	$153,873	$162,945	$172,613	$489,431	$404,236
Ctr	Avoided revenue loss via improved customer retention	$0	$256,500	$348,840	$444,771	$1,050,111	$855,642
	Total benefits (risk-adjusted)	$0	$453,719	$561,850	$675,208	$1,690,777	$1,384,104

TIME SAVINGS ON TRIAGE AND INVESTIGATION OF SECURITY INCIDENTS

Evidence and data. Interviewees told Forrester that Arctic Wolf provided significant time savings on investigation and triage of potential security incidents, primarily by consolidating information from myriad security tools.

- The VP of IT for the building supply distributor explained: "[With our prior security, finding out what happened and when] was a never-ending thing. Now, with Arctic Wolf, we have all that data cataloged and indexed and everything, so it's a lot easier to search. We can go out there and say, 'Okay, we have this incident with this associate, and we can look up everything that associate has done.' It's all because of the new tools and sensors."
- The IT director for the construction services organization concurred: "We now get notifications of potential problems in minutes, and that's extremely valuable to us. … It's made us more flexible because we don't have to invest as much effort in monitoring and managing our security, so we can focus on other areas."
- The CIO for the HVAC solutions organization described a before/after scenario for Forrester: "Before, somebody would tell us their account was hijacked, and we'd have to go through all of our logs to figure out that they simply failed to log on correctly. With Arctic Wolf, I get an email saying, 'This person had a failed log-on attempt, here's the location, here's all the information.' Before we'd have to spend a few hours, and now it's just instantaneous."

> **"We're able to focus more on solving business-related issues and less about actively maintaining our cybersecurity visibility."**
>
> *Director of IT, law*

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

- The composite organization handles 80 ticketed incidents per year before Arctic Wolf, increasing by 10% each year.

- Before Arctic Wolf, each incident requires 10 hours of investigation labor time.
- With Arctic Wolf, each incident requires 45 minutes to fully investigate.

Risks. Factors that could impact the size of this benefit for organizations include:

- The number of ticketed incidents handled per year.
- The time required to investigate each incident.
- The degree to which Arctic Wolf's ability to consolidate information reduces labor time per incident.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $124,000.

Time Savings On Triage And Investigation Of Security Incidents

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
A1	Ticketed incidents per year handled before Arctic Wolf	Interviews		80	88	97
A2	Total investigation labor time required per incident before Arctic Wolf (hours)	Interviews		10	10	10
A3	Investigation labor time required per incident after Arctic Wolf (hours)	Interviews		0.75	0.75	0.75
A4	Labor time avoided due to Arctic Wolf (hours)	A2-A3		9.3	9.3	9.3
A5	Fully loaded security FTE hourly rate	TEI standard		$62	$65	$68
At	Time savings on triage and investigation of security incidents	A1*A4*A5	$0	$45,627	$52,700	$60,868
	Risk adjustment	↓5%				
Atr	Time savings on triage and investigation of security incidents (risk-adjusted)		$0	$43,346	$50,065	$57,825
	Three-year total: $151,235			**Three-year present value: $124,226**		

AVOIDED AND REDUCED IMPACTS OF SECURITY BREACH

Evidence and data. Interviewees noted that Artic Wolf made them feel much more confident in their organizations' ability to handle potential incidents by improving the speed at which incidents were investigated, improving overall visibility into the security environment, and providing additional support via Arctic Wolf's concierge services.

- The director of IT for the law firm told Forrester how improved security with Arctic Wolf wasn't just a hypothetical for their organization: "We had an incident around a zero-day vulnerability and Arctic Wolf helped identify it, notify us, and put a plan into action. They even performed initial triage until our forensic cybersecurity organization came in. … Without Arctic Wolf, it would have been a total shutdown."
- The VP of IT for the building supply distributor told Forrester how Arctic Wolf helped proactively prevent threats from escalating: "Initially, we were monitoring everything we thought we should be looking at. After working with Arctic Wolf, we realized there's a whole bunch of other information out there. … It really opened our eyes to finding issues when they're tiny problems, before they become bigger problems."
- The IT director for the construction services firm described how Arctic Wolf's concierge services improved their organization's security and mitigated the impact of potential breaches: "We have monthly sessions with the concierge team, and they've been valuable. They've given us a lot of guidance in hardening our network and giving us areas we need to look at for strengthening our security."

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

- A security breach for the composite organization costs an average of $42,000 in Year 1 or $53 per employee. With employee growth, this equals $46,746 by Year 3.[2]
- Without any intervention, the composite organization experiences 3.2 security breaches per year. Each breach impacts 50% of the organization's employees and causes them to lose 3.6 hours in productivity.[3]
- Arctic Wolf reduces the likelihood of a security breach by 90% by enabling more investigation of incidents. Faster incident remediation reduces the impact of remaining breaches by 90%.
- Improvements and additional support from Arctic Wolf via their concierge service reduces lost productivity from breaches.

Risks. Factors that could impact the size of this benefit for organizations include:

- The number and cost of breaches.
- The amount of lost productivity per employee per breach.
- The degree to which Arctic Wolf can prevent, mitigate, and avoid productivity losses from breaches.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $404,000.

> **"A client asked about our cybersecurity portfolio, and when they saw what [Arctic Wolf] was doing, they described it as best-in-class security posture."**
>
> *Director of IT, law*

Avoided And Reduced Impacts Of Security Breach						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
B1	Estimated cost of single security breach, excluding productivity ($53 per employee)	Forrester research		$42,400	$44,520	$46,746
B2	Estimated annual security breaches	Forrester research		3.2	3.2	3.2
B3	Reduced likelihood of a breach due to Arctic Wolf enabling more incident investigation	Interviews		90%	90%	90%
B4	Subtotal: Value of avoided breaches due to Arctic Wolf	B1*B2*B3		$122,112	$128,217.6	$134,628.48
B5	Estimated annual breaches after Arctic Wolf	B2-(B3*B2)		0.32	0.32	0.32
B6	Reduced impact of a data breach with Arctic Wolf due to faster incident remediation	Interviews		90%	90%	90%
B7	Subtotal: Reduced costs of breach with Arctic Wolf	B1*B5*B6		$12,211	$12,822	$13,463
B8	Number of internal employees	Composite, 5% growth YoY		800	840	882
B9	Average hourly salary for business users	TEI standard		$60	$63	$66
B10	Diminished/lost user productivity during breach (hours)	Forrester research		3.6	3.6	3.6
B11	Percentage of employees impacted per breach	Interviews		50%	50%	50%
B12	Subtotal: Avoided lost internal productivity due to Arctic Wolf reducing risk	B5*B8*B9*B10*B11		$27,648	$30,482	$33,606
Bt	Avoided and reduced impacts of security breach	B4+B7+B12	$0	$161,971	$171,521	$181,698
	Risk adjustment	↓5%				
Btr	Avoided and reduced impacts of security breach (risk-adjusted)		$0	$153,873	$162,945	$172,613
	Three-year total: $489,431			**Three-year present value: $404,236**		

AVOIDED REVENUE LOSS VIA IMPROVED CUSTOMER RETENTION

Evidence and data. Interviewees explained to Forrester that improving their organizations' security posture was vital for retaining business from customers in highly regulated or scrutinized industries.

- The VP of IT for the law firm noted: "Large clients ask how we monitor our environment and being able to respond with, 'I have Arctic Wolf, and they provide 24/7, 365 monitoring of our environment and retain security logs for three years.' That reflects well on us. … It's because of our partnership with Arctic Wolf that we're able to respond positively on security questionnaires and audits that have allowed us to maintain our relationships with some of our clients."
- The CIO of the HVAC solutions organization explained the importance of being able to prove adequate security for retaining business: "The regulation that impacts our clients has language that sets up clear preferences. [Having better

security] puts us ahead of the curve. … It puts us above a lot of other companies that haven't started updating their security or aren't going to."

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

- The composite organization stands to lose 3% of its annual revenue in business due to inadequate security in Year 1, increasing to 5% in Year 3.
- Arctic Wolf enables the composite to fully avoid this revenue loss.

Risks. Factors that could impact the size of this benefit for organizations include:

- Clients that require improved security for retention.
- The amount of revenue impacted by potential client loss.
- The degree to which Arctic Wolf can mitigate potential losses.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $856,000.

"We work with major vendors, and now we're able to go to them and say, 'Look, I'm COC (Certificate of Conformity) compliant, here's my certifications, here's my testing.' It builds a level of trust when we're working on projects with partners."

CIO, HVAC solutions

Avoided Revenue Loss Via Improved Customer Retention

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
C1	Company revenue	Composite		$50,000,000	$51,000,000	$52,020,000
C2	Percentage of revenue at risk without Arctic Wolf monitoring platform	Interviews		3%	4%	5%
C3	Operating margin	Assumption		18%	18%	18%
Ct	Avoided revenue loss via improved customer retention	C1*C2*C3	$0	$270,000	$367,200	$468,180
	Risk adjustment	↓5%				
Ctr	Avoided revenue loss via improved customer retention (risk-adjusted)		$0	$256,500	$348,840	$444,771
	Three-year total: $1,050,111			**Three-year present value: $855,642**		

UNQUANTIFIED BENEFITS

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

- **Improved understanding of security posture.** Arctic Wolf's improved visibility enabled the interviewees' organizations to gain a fuller understanding of their security posture, allowing for better long-term planning.

  The CIO of the HVAC solutions organization explained: "[Before Arctic Wolf, it was nonstop, just putting out fires. … With Arctic Wolf, it was nice to hear validation that we're taking the right steps, and that if we pull these levers and push these buttons, we'd be 10% better. We get actionable advice."

  The VP of IT for the building supply distributor told Forrester: "[Thanks to Arctic Wolf,] we get to spend more time being proactive. … We can spend more time adding new benefits and features for our associates or customers."

- **Simpler, more affordable purchasing of cybersecurity insurance.** The additional security features of Arctic Wolf, along with programs at Arctic Wolf designed to work with cybersecurity insurers, made the process of purchasing cybersecurity insurance easier and more affordable.

  The VP of IT for the building supply distributor said: "Having Arctic Wolf has also helped us better prepare for cyber insurance renewals. … We can have reports and show everything we're able to do. … It definitely helped with the premium**.**"

  Arctic Wolf customers can benefit from cyber insurance premium savings of up to 80% with select insurance carriers. Because cybersecurity insurance premiums are industry-specific and the composite organization is industry-agnostic, Forrester was not able to quantify this savings for the composite organization.

> **"Arctic Wolf definitely fills in quite a few boxes on the cybersecurity insurance questionnaire that's sent over every year."**
>
> *IT director, construction services*

FLEXIBILITY

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

- **Ability to focus on more strategic work.** By reducing maintenance and investigation time, Arctic Wolf enabled the interviewees' organizations to refocus on more strategic, long-term work. The CIO of the HVAC solutions organization noted, "Arctic Wolf gave us back time to look at automating workflows and where we can use AI and OCR [optical character recognition] instead of having somebody manually key something and get it wrong."
- **Ease of integration with other solutions.** Arctic Wolf's ability to integrate other solutions enabled the interviewees' organizations to add capabilities without having to worry about compromising security. The director of IT for the law firm told Forrester: "If I move and implement an additional security product, I don't have to ask Arctic Wolf if they can integrate it into my environment. They go, 'Here's this knowledge base over here, this is how you integrate it, go ahead and follow these

steps, but if you need any help, let us know.' Arctic Wolf allows us to be flexible with our security program."

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

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Dtr	Ongoing licensing and professional services costs for Arctic Wolf	$0	$93,280	$93,280	$93,280	$279,840	$231,974
Etr	Total implementation and maintenance costs	$2,805	$13,466	$14,140	$14,140	$44,551	$37,356
	Total costs (risk-adjusted)	$2,805	$106,746	$107,420	$107,420	$324,391	$269,330

ONGOING LICENSING AND PROFESSIONAL SERVICES COSTS FOR ARCTIC WOLF

Evidence and data. Arctic Wolf charged the interviewees' organizations ongoing license fees based on the number of employees and the number of servers.

Modeling and assumptions. Forrester assumes the composite organization pays $84,800 per year in licensing and professional services fees to Arctic Wolf.

Risks. The specific licensing fees could vary by organization. For more specific pricing estimates, contact Arctic Wolf.

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 $232,000.

Ongoing Licensing And Professional Services Costs For Arctic Wolf						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
D1	Annual licensing and professional services costs for Arctic Wolf	Interview		$84,800	$84,800	$84,800
Dt	Ongoing licensing and professional services costs for Arctic Wolf	D1	$0	$84,800	$84,800	$84,800
	Risk adjustment	↑10%				
Dtr	Ongoing licensing and professional services costs for Arctic Wolf (risk-adjusted)		$0	$93,280	$93,280	$93,280
	Three-year total: $279,840			**Three-year present value: $231,974**		

TOTAL IMPLEMENTATION AND MAINTENANCE COSTS

Evidence and data. The interviewees provided detailed descriptions of the process of implementing and maintaining Arctic Wolf:

- Interviewees told Forrester that a small team working with Arctic Wolf for a few weeks completed the initial implementation. The interviewees shared that it was a relatively quick and straightforward implementation process.
- Interviewees' organizations incurred a small professional services fee as part of the implementation.
- Interviewees reported that a small amount of internal labor was required to maintain the platform on an ongoing basis.

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

- The implementation team consists of two security FTEs. Each devotes 12.5% of their time over the course of a month to setting up Arctic Wolf.
- One security FTE devotes 10% of their time to maintaining the platform on an ongoing basis.
- Security FTEs involved in implementation and maintenance each have a fully burdened salary of $128,250.

Risks. Factors that could impact the size of this cost for organizations include:

- The number of FTEs required for implementation and maintenance.
- The percentage of FTE time required for implementation and maintenance.
- The annual fully loaded FTE salary.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $37,000.

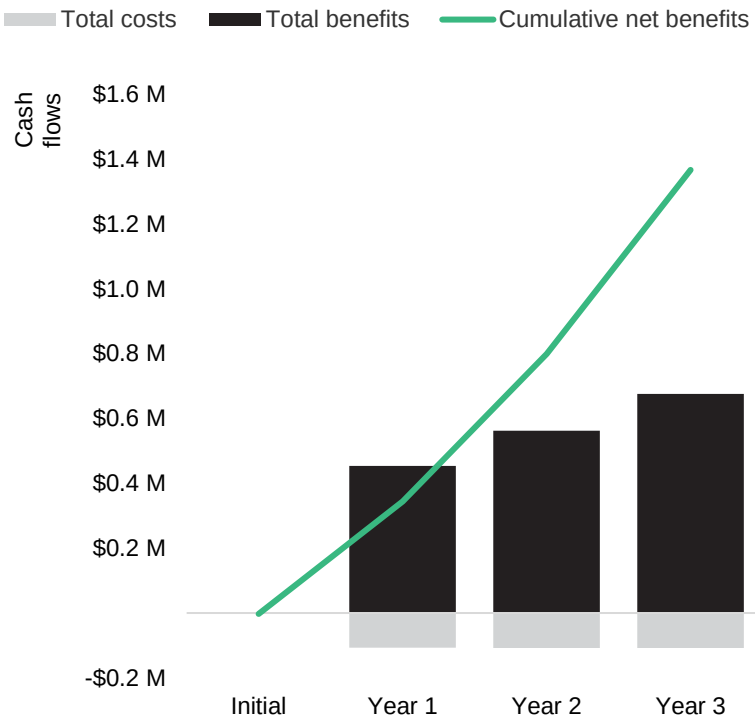
Total Implementation And Maintenance Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
E1	Security FTEs required for implementation and maintenance	Interview	2	1	1	1
E2	Percentage of time spent on implementation	Interview	12.5%			
E3	Months required for implementation	Interview	1			
E4	Percentage of time spent on maintenance	Interview		10%	10%	10%
E5	Fully loaded security FTE salary	TEI standard	$128,250	$128,250	$134,663	$134,663
Et	Total implementation and maintenance costs	(E1*E2*(E3/12 months)*E5) +(E1*E4*E5)	$2,672	$12,825	$13,466	$13,466
	Risk adjustment	↑5%				
Etr	Total implementation and maintenance costs (risk-adjusted)		$2,805	$13,466	$14,140	$14,140
	Three-year total: $44,551			**Three-year present value: $37,356**		

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	($2,805)	($106,746)	($107,420)	($107,420)	($324,391)	($269,330)
Total benefits	$0	$453,719	$561,850	$675,208	$1,690,777	$1,384,104
Net benefits	($2,805)	$346,972	$454,430	$567,789	$1,366,386	$1,114,774
ROI						414%
Payback						<6 months

Appendix A: Total Economic Impact

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

TOTAL ECONOMIC IMPACT APPROACH

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

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

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

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

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] 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, Q1 2021.
[3] Ibid.


FORRESTER®