A Forrester Total Economic Impact™
Study Commissioned By Arctic Wolf
May 2020

The Total Economic Impact™ Of Arctic Wolf Security Operations Solutions

Cost Savings And Business Benefits Enabled By Arctic Wolf

FORRESTER®

Table Of Contents

Executive Summary **1**

Key Findings 1

TEI Framework And Methodology 3

The Customer Journey With Arctic Wolf **4**

Interviewed Organization 4

Key Challenges 4

Key Results 5

Analysis Of Benefits **7**

Security And IT Operation Reduction In Effort To Manage Incidents 7

Quicker Time-To-Value Delivery Using Arctic Wolf Security Operations 9

Cost Of Alternate Software And Infrastructure To Attain Same Level Of Security Posture 11

Flexibility 12

Analysis Of Costs **13**

Direct Costs Of Arctic Wolf Security Operations Solution 13

Financial Summary **15**

Arctic Wolf Security Operations: Overview **16**

Appendix A: Total Economic Impact **18**

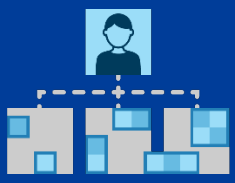
Project Director:
Henry Huang

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

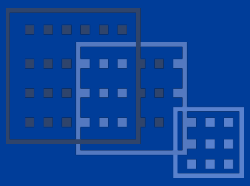
FORRESTER®

Key Benefits



Lowered security and IT effort to manage incidents:
$556,677

Quicker time-to-value delivery with Arctic Wolf:
$966,888



Avoided software and infrastructure costs to reach same level of security:
$1,415,505

Executive Summary

Arctic Wolf provides Security Operations as a managed service solution helping organizations improve cybersecurity defenses with the cloud-native Arctic Wolf™ Platform and a team of security experts that augment existing in-house IT and security teams and capabilities. Services under this umbrella include managed detection and response (MDR), continuous vulnerability management (Managed Risk), as well as cloud infrastructure and SaaS monitoring (Managed Cloud Monitoring). 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 utilizing Security Operations solutions. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Security Operations solutions and how they affect cybersecurity when enlisting the services of Arctic Wolf.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed two customers with extensive experience with Arctic Wolf's Security Operations solutions: MDR and Managed Risk. Our findings revealed that the comprehensive coverage across multiple segments of cyber security helped in two main ways:

- Security Operations services elevate the available security infrastructure to its full capability potential. As an example, without Arctic Wolf, recorded logs were not digested due to a lack of human operators performing the forensic activities. In another instance, the implementation of security orchestration automation and response (SOAR) was not leveraged because of gaps in the security group.
- Security Operations services become an extension and enhancement of the internal security professionals at these organizations, integrating in streamlined processes and workflows. Security capability was now easily scalable, where previously it was an arduous process to hire and then train qualified professionals. With Arctic Wolf, organizations were able to accomplish more without overworking internal resources.

Prior to using Arctic Wolf for security operations, the interviewed customers were unable to truly realize the value of their security investments due to the constrained personnel resources. Additionally, they had difficulty with bringing to light the real threats within the numerous security-relevant events identified by those tools. One interviewee stated: "Arctic Wolf distills billions of events for us into 15 escalations that we actually need to review. What type of time savings does that say?"

Key Findings

Quantified benefits. The interviewed organization experienced the following risk-adjusted present value (PV) quantified benefits:

- **The reduction in security and IT operator effort to manage incidents netted a significant time benefit for employees and it allowed organizations to avoid hiring additional security professionals.** Serving as an extension of a SOC, Arctic Wolf offloads a significant volume of work from internal security teams. For a resource-constrained but growing organization that requires improved capabilities in detection and response, Arctic Wolf saves: 1) 50% of effort from the internal security operations group for triage and investigation activities and 2) 90% for IT operations that are involved in incident management. This benefit results in a three-year savings of $557K (PV).

FORRESTER®

ROI
411%

Benefits PV
$2.9 million

NPV
$2.3 million

Payback
< 6 months

› **Leveraging Arctic Wolf for Security Operations greatly decreased the cost and improved speed— including that of contractors — to stand up the solution and recoup the investment.** Traditional point solutions require expertise and time to set up, which imposes additional costs in the form of professional services, contractors, new hire FTEs, and time. Where this would typically take upwards of 10 months for a traditional SIEM and associated logging tools to baseline and operate in an efficient steady state, Arctic Wolf is ready to go in a single month. The avoidance of effort, requiring additional people and the subsequent time delta yields a savings of $967K PV over three years.

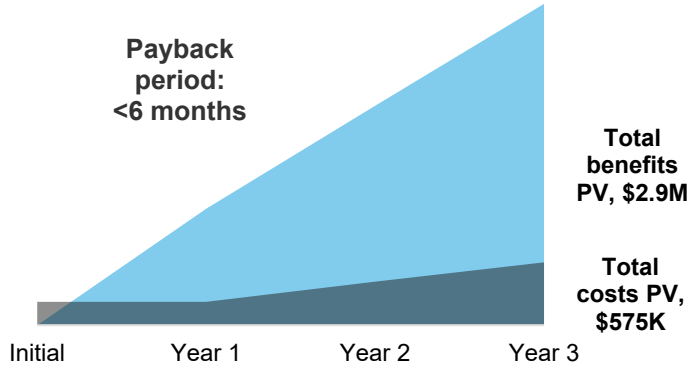
› **Software and hardware infrastructure purchases and maintenance that would have otherwise been necessary to attain a proactive security posture is avoided as Arctic Wolf supplants these point solutions.** The alternative of using Arctic Wolf for Security Operations requires significant capex and opex in the form of personnel and software to attain a similar level of efficiency. For example, logging systems allow organizations to extract risk determination insights, but would normally require an entire team to manually sort and classify the data if not for Arctic Wolf. The three-year savings associated with this benefit amounts to $1.4M PV.

Costs. The interviewed organization experienced the following risk-adjusted PV costs:

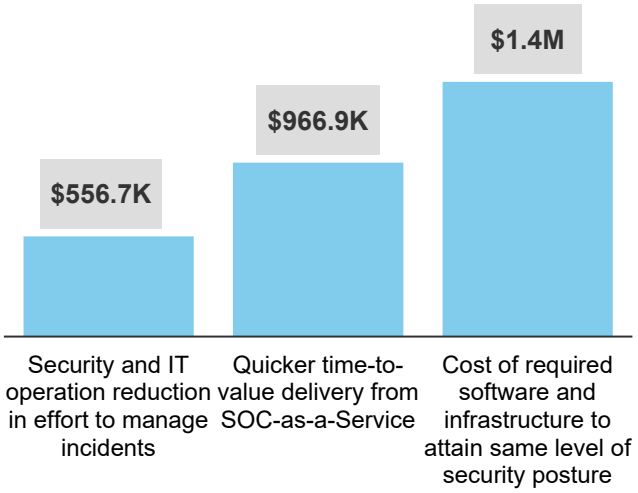
› **Direct costs of Arctic Wolf Security Operations solutions.** The cost of services provided by Arctic Wolf is based upon factors such as the number of users covered and assets monitored, such as servers. Over the course of a three-year assessment, a PV cost of $575K is incurred. No indirect costs assumed internally are incurred.

Forrester's interviews with two existing customers and subsequent financial analysis found that the interviewed organizations experienced benefits of $2.9 million versus costs of $575K, (calculated as the net present value, or NPV, of three years of economic impact) adding up to a NPV of $2.3 million and an ROI of 411%.

Financial Summary



Benefits (Three-Year)



FORRESTER®

TEI Framework And Methodology

From the information provided in the interview, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering implementing Arctic Wolf Security Operations.

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 Security Operations can have on an organization:

The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

DUE DILIGENCE
Interviewed Arctic Wolf stakeholders and Forrester analysts to gather data relative to the usage of Security Operations.

CUSTOMER INTERVIEWS
Interviewed two organizations using Security Operations to obtain data with respect to costs, benefits, and risks.

FINANCIAL MODEL FRAMEWORK
Constructed a financial model representative of the interview using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewed organizations.

CASE STUDY
Employed four fundamental elements of TEI in modeling Arctic Wolf Security Operations' impact: benefits, costs, flexibility, and risks. Given the increasing sophistication that enterprises have regarding ROI analyses related to IT investments, Forrester's TEI methodology serves to provide 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 Arctic Wolf 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 report to determine the appropriateness of an investment in Arctic Wolf Security Operations.

Arctic Wolf 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.

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

The Customer Journey With Arctic Wolf

BEFORE AND AFTER THE SECURITY OPERATIONS INVESTMENT

Interviewed Organization

For this study, Forrester interviewed two customers that have been using the Artic Wolf platform and solutions for over a year. Characteristics of the organizations are as follows:

- The first organization is a regional bank in the United States with extensive regulatory overwatch and an explicit need for cybersecurity. This growing multilocation bank is unable to scale security operations to match the growth and regulatory pressures they face. Forrester's financial analysis emphasizes the insights that were collected from this organization.
- The second organization is one of the largest global law firms with over two thousand endpoints and upwards of 500 servers. This organization relies on a small security operations team that is augmented with Arctic Wolf's services. Prior to adopting Arctic Wolf, this organization assessed itself on a security maturity scale as being a 6 of 10.

Key Challenges

Both interviewed customers stated that resource constraints limited the effectiveness of their security programs. While many security tools and infrastructure had been deployed to pave the way for success, there was a persistent gap in security coverage and response, which was ultimately attributable to constrained people resources. These organizations were often in a reactive mode, and thus they were unable to free up the time to be proactive on the security front. Some of the difficulties that these organizations stated can be summed up with the following:

- **Security tool investments did not give back very much without the appropriate people resources.** While security tools are invaluable, the level of information that was provided by these systems did not always result in the accurate identification of incidents. In order to take a successful deep dive, and ultimately identify actionable alerts and real threats, many more people were required. This expansion in staff was not an option given the difficulty in bringing new security professionals on board to do the amount of investigative and triage work to truly unlock the power of these systems. For executive teams, it was easy to highlight the lack of returns from platforms that had insufficient allocations of people resources, which hamstrung the organizations' ability to investigate and apply an affirmative confirmation of resolution on the totality of alerts.
- **Unanticipated runaway costs of security tools were difficult to manage.** The interviewed financial services organization provided context in that many investments took longer and required more people resources than expected, essentially growing capex and opex that was difficult to estimate and secure. As the same firm stated:

  "I had stood up [a vulnerability management platform] to do our own continuous vulnerability scanning . . . and cumbersome is a nice way to put it. Reporting was a struggle, trying to understand the patches that were needed, the time spent to care for and feed the scanner, I can't even count the hours."

> "We were not being successful with deciphering our logs at all. We were pulling 50% of the logs that we needed for visibility, and probably actively monitoring 20% of what we were selecting. Because this was all manual, the level correlation we achieved was next to zero."
>
> *CSO, financial services*

> "Being the only person at the organization looking after security was me, and I don't have the time to oversee and tune everything. This is where Arctic Wolf steps in."
>
> *Global infosec director, legal organization*

- **Growth in security maturity and usage of tools continually added to integration and ramp-up costs.** The growing stack of security tools for the financial services organization created two problems:
    - Internal FTE and solution ramp-up times were often lengthy, which included both acclimation and environment configuration for the tools being used. Indirect costs of security point products were difficult to measure until after acquisition or, at the very least, an extensive pilot or proof of concept.
    - Secondly, new tools needed proper integration with the other point solutions within the security stack; without which the business lost the benefits of automation and orchestration. With many point solutions, what would be the centralized solution to bring all the information together so that efficiency could be improved? This was a costly exercise that required a collaboration between SecOps, DevOps, and external professionals.

> "Without having to increase staffing in any way, shape, or form, we're able to increase to a true 24x7 operation. The correlation and monitoring activity, we've got it all now."
>
> *CSO, financial services*

Key Results

The interview revealed that key results from the Arctic Wolf Security Operations investment include:

- **Continuous 24x7 monitoring without an increase in staff.** The Arctic Wolf Concierge Security Team provides 24x7 security coverage. For many organizations that are resource constrained, it is difficult to provide around-the-clock coverage, which typically requires having either multiple shifts or multiple people on call. With continuous coverage, organizations can have incidents handled almost immediately, with alerts for on-site teams only if absolutely necessary. The delta in time to respond can often be upwards of 6 hours according to the interviewees, minimizing the impact of off-shift security incidents.
- **Data centralization helped provide better intelligence and visibility while enabling user behavioral analytics (UBA).** The organizations described that the information brought to a centralized point gave them the visibility and reporting capabilities to make compliance activities much easier, especially on providing evidence. The UBA component brought forth a new angle on whether internal activities on the network were either legitimate work activities or something nefarious, decreasing investigative activities for the internal teams by presenting all activities through a new lens.
- **Arctic Wolf brought automation and orchestration.** By leveraging Arctic Wolf for security operations, the organizations instantly attained elements of SOAR. Workflows were streamlined and removed the need for internal responders to expend significant amounts of time as the orchestration was handed to the Concierge Security Team at Arctic Wolf.
- **Reduction of security alerting noise by 60% increased focus on incidents that required action.** In addition to going through over 15 billion events and terabytes of logs in a month, the Arctic Wolf cloud-native platform and Concierge Security Team was able to distill these events down to those that mattered, thereby reducing the work of internal SecOps and IT. The reclaimed time was reallocated to provide business value elsewhere.

> "There are things that we would have had to purchase internally to do similar monitoring as what Arctic Wolf provides — things like network flow analyzers, IPS, and additional firewalls. They would have been all separate. Where now, we are fed all the digested information from Arctic Wolf."
>
> *CSO, financial services*

› **Arctic Wolf became an extension of the organization's security team.** The global infosec director at an interviewed organization stated:

"They've taken a lot off my plate. Once I gave them the data they need, they became essentially an extension of my office. Now, I lean on them even more."

Trust had developed between the interviewees and Arctic Wolf to such a degree that one interviewee's dedicated security engineer lead ended up knowing as much if not more about the inner workings of the client's network as they did themselves, which was extremely meaningful.

"The big thing about Arctic Wolf is the ability to contain cost. We wanted to know how we could incrementally scale without surprises. We don't care about how large our logs are now and how many users we have, we have the security in knowing the incremental cost and that we can have that when we need it."

CSO, financial services

Analysis Of Benefits

QUANTIFIED BENEFIT DATA

Total Benefits

REF.	BENEFIT	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Atr	Security and IT operation reduction in effort to manage incidents	$192,960	$192,960	$295,200	$681,120	$556,677
Btr	Quicker time-to-value delivery from Security Operations	$388,800	$388,800	$388,800	$1,166,400	$966,888
Ctr	Cost of required software and infrastructure to attain same level of security posture	$589,498	$557,498	$557,498	$1,704,493	$1,415,505
	Total benefits (risk-adjusted)	$1,171,258	$1,139,258	$1,241,498	$3,552,013	$2,939,070

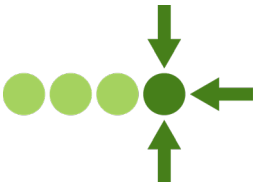
The table above shows the total of all benefits across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the interviewed organization expects risk-adjusted total benefits to be a PV of more than $2.9 million.

Security And IT Operation Reduction In Effort To Manage Incidents

The financial services organization noted first and foremost that they had seen a dramatic decline in the human effort required by its internal personnel — exactly as Arctic Wolf's Security Operations solutions are intended to address. This is addressable to two groups:

- SecOps professionals who are typically the first line of defense and are typically entrusted to incident identification, incident examination, triage, and remediation.
  - A primary driver for the reduction was the elimination of noise so that only qualified incidents surface, thereby eliminating wasted effort on the identification segment of the workflow.
  - Examination, triage, and remediation also became easier because of the quality of contextual information that was brought to light. The provided information was not generic nor specific to the organization's network characteristics.
  - The global legal organization cited that Arctic Wolf brought about a 60% reduction in false positives — allowing internal SecOps to focus on where it mattered the most.
  - Arctic Wolf handled investigation and containment in an automated fashion, that is until the matter needed escalation. They orchestrated nearly all elements.
- IT operators that also serve as incident responders played a large role in remediation and response. Arctic Wolf was described as having offered remedial actions, which needed to be taken, as "on a plate," if it had not been addressed by the Arctic Wolf Concierge Security team already. For many of these incident responders, the result was a reduction on 90% of their tasks, freeing them up to perform other value-add IT tasks.

The presented model contains some assumptions of how time is saved that have been aligned closely to how the interviewed financial services organization operates.



Arctic Wolf remediates a majority of incidents and leaves only a small number of incidents for internal responders to act on with maximum intelligence.

- The SecOps group is primarily one person, but it grows over time to address more advanced matters such as threat hunting.
- The SecOps individual is focused on the workstream of inoculating and removing threats, but they see a dramatic drop in manual effort as Arctic Wolf takes the brunt of the work.

Parsing down the calculations further, it is important to note the following based on the factors communicated by the financial organization:

- SecOps typically balances time between managerial, reporting, and threat mitigation duties, with the last task taking much of its focus.
- The IT operation personnel at the organization spend 40% of their time on security-related incidents, which include primarily remediation and response.
- While many incidents are remediated by the Arctic Wolf Concierge Security Team to reduce effort on the part of the client, the remaining incidents that require a further level of attention by IT or SecOps are provided with enough contextual information for a deterministic treatment of the incident.

With these matters in account, Forrester expects that the three-year benefits for a very lean SecOps and IT staff to accumulate a time savings of $556,677 PV.

Investigations and triages dissipate through a reduction in the number of incidents that truly need attention after passing through Arctic Wolf.

Security And IT Operation Reduction In Effort To Manage Incidents: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
A1	Number of SecOp FTEs		1	1	2
A2	SecOp effort reduced on incident examination, triage, and remediation	% reduction of SecOps effort	50%	50%	50%
A3	SecOps annual salary, fully loaded	$120K*1.2X benefits modifier	$144,000	$144,000	$144,000
A4	Number of IT FTEs		4	4	5
A5	IT time spent on security-related incidents		40%	40%	40%
A6	IT security-based incident deflected by Security Operations		90%	90%	90%
A7	IT annual salary, fully loaded	$70K*1.2X benefits modifier	$84,000	$84,000	$84,000
At	Security and IT operation reduction in effort to manage incidents	(A1*A2*A3)+ (A4*A5*A6*A7)	$192,960	$192,960	$295,200
	Risk adjustment	0%			
Atr	Security and IT operation reduction in effort to manage incidents (risk-adjusted)		$192,960	$192,960	$295,200

Quicker Time-To-Value Delivery Using Arctic Wolf Security Operations

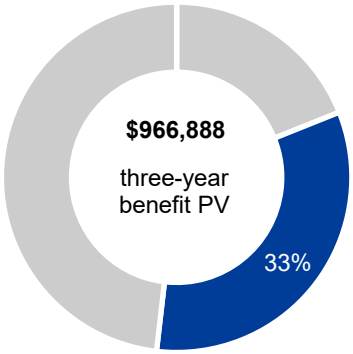
Critical to the financial services organization that Forrester interviewed was being able to immediately realize value. Having previously experimented with multiple solutions that required a lengthy process of deployment, integration, baselining, and an FTE ramp-up period, the organization wanted a solution that provided value especially when security solutions were evolving at a quick pace. A protracted implementation would result in keeping the organization at a disadvantage to the continually evolving base of malicious actors. When implementing Arctic Wolf's Security Operations solutions, the organization was able to stand up the service in less than a month, which included the baselining and integration of the existing security stack, making for a seamless and straightforward transition.

For the interviewed organization, Forrester assumes that:

- Multiple integrations to platforms such as endpoint detection and response (EDR), firewalls, and multiple logging systems are made to Arctic Wolf for real-time ingestion. These integrations are performed by Arctic Wolf.
- Baselining and acclimation to the local network by Arctic Wolf is done with an extensive ramp process that takes approximately one month.
- Onboarding and ramp to alternative solutions such as security information and event management (SIEMs) software and additional logging software would require a significant amount of human effort to become proficient with the tools, requiring as much as three additional SecOps personnel, regardless of being contractors or full-time employees.
- Professional services and implementation providers, if used, would be more costly and hence mostly avoided on alternate solutions.

A SIEM and log analysis are foundational anchors for organizations that have mature security programs, and for the purposes of this report, they have been calculated into Forrester's analysis; and for example, these anchors are needed by the interviewed financial services firm. With Arctic Wolf, the time-to-deploy and become effective took one month, whereas even a single solution can take as much as 10 months to produce real results.

Realizing that SIEM and logging tools vary to a degree on complexity, which can affect the amount of effort that needs to be put into standing up a competitive SIEM tool, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $966,888.



Quicker time-to-value delivery from Arctic Wolf: 33% of total benefits

Time-to-value with Arctic Wolf is one-month vs 10 months for just a traditional SIEM or logging tool.

Impact risk is the risk that the business or technology needs of the organization may not be met by the investment, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for benefit estimates.

FORRESTER®

Quicker Time-To-Value Delivery From Security Operations: Calculation Table					
REF.	**METRIC**	**CALC.**	**YEAR 1**	**YEAR 2**	**YEAR 3**
B1	SecOps involved in SIEM and log analyses activities		1	1	1
B2	Additive SecOps needed with alternative SIEM + log analyses		3	3	3
B3	Deployment time of Arctic Wolf Security Operations	Calculated in months	1	1	1
B4	Deployment time of SIEM and logging system	Calculated in months	10	10	10
B5	Cost of SecOps FTE annually, fully loaded	$120K*1.2x benefits modifier	$144,000	$144,000	$144,000
Bt	Quicker time-to-value delivery from Arctic Wolf Security Operations	(B4-B3)/12*(B1+B2)*B5	$432,000	$432,000	$432,000
	Risk adjustment	↓10%			
Btr	Quicker time-to-value delivery from Arctic Wolf Security Operations (risk-adjusted)		$388,800	$388,800	$388,800

Cost Of Alternate Software And Infrastructure To Attain Same Level Of Security Posture

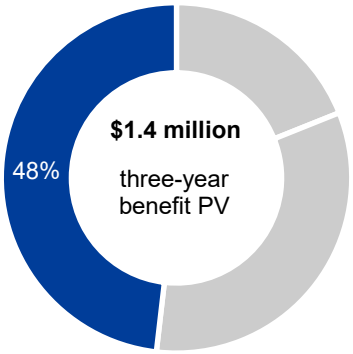
The interviewed organizations stated that without the use of Arctic Wolf, additional software, infrastructure, and people resources would be necessary to run these assets in order to achieve a similar level of preparedness. One main concern of taking this path was the runaway costs that these alternative pieces would have incurred. Additional (and sometimes an increased number of) software such as a formal SIEM, intrusion prevention system (IPS), SOAR, and different network analyzers were all separately needed to attain a similar level of security posture if not using Arctic Wolf.

While the costs of these devices and software are sizeable, the cost and the ability to hire additional security professionals are an additional challenge. Forrester estimates that for an organization to manage these additional security components, as to reach a similar level of posture as what Arctic Wolf provides, the personnel required are:

- Three SecOps personnel are especially mandatory if significant emphasis is placed on log-level investigative work. Further, SIEM monitoring and data consolidation are tasks these FTEs would need to assume responsibility for.
- Two IT FTEs are needed to maintain, monitor, and support the disparate point solutions.

This additional infrastructure alone costs an estimated $137K in Year 1, with that cost adding up to $330K over three years. After including the personnel required to support that infrastructure, the costs rise as high as $1.76M PV over three years.

Recognizing that organizations all come from different starting points, there can be a degree of variance in how much an organization can save. To account for this, Forrester has adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $1,415,505.



Cost of alternate software and infrastructure to attain same level of security posture:
48% of total benefits

Cost Of Alternate Software And Infrastructure To Attain Same Level Of Security Posture: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
C1	Alternate SIEM solution, non-MDR cost for similar users and asset base		$16,872	$16,872	$16,872
C2	Incremental SecOps labor required to run non-MDR solution	3 FTEs* $144,000K/yr	$432,000	$432,000	$432,000
C3	Incremental IT labor required to run alternate non-MDR solution	2 FTEs* $84,000/yr	$168,000	$168,000	$168,000
C4	Cost of software and infrastructure, excluding SIEM		$120,000	$80,000	$80,000
Ct	Cost of alternate software and infrastructure to attain same level of security posture	C1+C2+C3+C4	$736,872	$696,872	$696,872
	Risk adjustment	↓20%			
Ctr	Cost of alternate software and infrastructure to attain same level of security posture (risk-adjusted)		$589,498	$557,498	$557,498

FORRESTER®

Flexibility

The value of flexibility is clearly unique to each customer, and the measure of its value varies from organization to organization. There are multiple scenarios in which a customer might choose to implement Arctic Wolf and later realize additional uses and business opportunities, including:

- **The growth of the security stack, either organically or through mergers and acquisitions, can be incorporated by Arctic Wolf in most cases without incurring additional cost.** Footprint growth typically entails an increase of network and security infrastructure, all producing more data. Additionally, different tools are inevitably brought in to create added layers of protection. While there are costs for sensors to capture the data flow, there are no integration costs for the client.
- **A single pane of glass for compliance purposes, to tackle a multitude of regulatory measures.** As a financial institution, the interviewed organization was accustomed to a number of regulatory measures. Growth often leads to additional compliance measures to adhere to the Sarbanes-Oxley Act (SOX), for instance, as it is required of all publicly traded organizations. Both the California Consumer Privacy Act (CCPA) and the Payment Card Industry Data Security Standard (PCI-DSS) increase scrutiny that commonly come with an increased footprint. Arctic Wolf's single pane of glass centralizes all information and provides upfront compliance-related reporting, which allows the organization's audit efforts to lessen even with rapid growth.

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

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for a future additional investment. This provides an organization with the "right" or the ability to engage in future initiatives but not the obligation to do so.

Analysis Of Costs

QUANTIFIED COST DATA

Total Costs

REF.	COST	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Dtr	Direct costs of Arctic Wolf Security Operations solution	$213,300	$0	$223,965	$235,164	$672,429	$575,077
	Total costs (risk-adjusted)	$213,300	$0	$223,965	$235,164	$672,429	$575,077

The table above shows the total of all costs across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the interviewed organization expects risk-adjusted total costs to be a PV of approximately $575K.

Direct Costs Of Arctic Wolf Security Operations Solution

The costs of Arctic Wolf's Security Operations for the interviewed financial services firm is based on a few simple factors that are assessed by Arctic Wolf. No additional costs were noted as the solution requires a very small amount of training and internal costs such as integration or customization. Readers should note that cost basis has been based upon list pricing, to err on the side of Forrester's conservative analysis.

The factors that contribute to the cost of Arctic Wolf's Security Operations are:

- The number of corporate users under management.
- The number of servers being monitored.
- The number of sensors and the bandwidth that passes through these sensors.
- Managed Risk and Managed Cloud Monitoring are not included in this Forrester analysis of costs, though the pricing frameworks are similar.

Based upon the information provided by the customer, Forrester calculates that the organization spends an estimated $383,385 PV across the span of a three-year period. Of note, however, is that the discrepancy in bandwidth and sensors between organizations can vary greatly, even for those with similar user base sizes.

Recognizing the level of variance that these factors can have on the final costs for potential customers, Forrester has adjusted this cost upward by 50% to account for most potential situations, yielding a three-year, risk-adjusted total PV of $575,077.

Costs are controlled based upon growth of covered resources, which is a departure from traditional security programs.

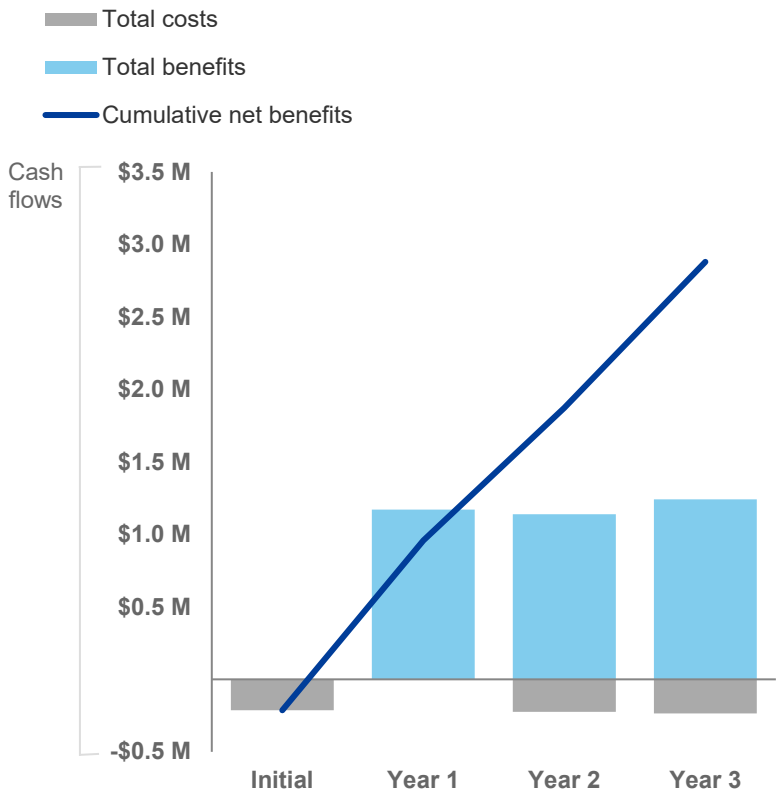
Implementation risk is the risk that a proposed investment may deviate from the original or expected requirements, resulting in higher costs than anticipated. The greater the uncertainty, the wider the potential range of outcomes for cost estimates.

Direct Costs Of Arctic Wolf Security Operations Solution: Calculation Table						
REF.	**METRIC**	**CALC.**	**INITIAL**	**YEAR 1**	**YEAR 2**	**YEAR 3**
D1	MDR users covered		$66,600		$69,930	$73,427
D2	Servers monitored		$3,600		$3,780	$3,969
D3	Sensors monitored		$72,000		$75,600	$79,380
Dt	Direct costs of Arctic Wolf Security Operations solution	D1+D2+D3	$142,200	$0	$149,310	$156,776
	Risk adjustment	↑50%				
Dtr	Direct costs of Arctic Wolf Security Operations solution (risk-adjusted)		$213,300	$0	$223,965	$235,164

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 interviewed 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 Table (Risk-Adjusted)

	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Total costs	($213,300)	$0	($223,965)	($235,164)	($672,429)	($575,077)
Total benefits	$0	$1,171,258	$1,139,258	$1,241,498	$3,552,013	$2,939,070
Net benefits	($213,300)	$1,171,258	$915,293	$1,006,334	$2,879,584	$2,363,993
ROI						411%
Payback period						<6 months

FORRESTER®

Arctic Wolf Security Operations: Overview

The following information is provided by Arctic Wolf. Forrester has not validated any claims and does not endorse Arctic Wolf or its offerings.

Arctic Wolf Security Operations Offerings

Arctic Wolf offers three major security operations solutions: Managed Detection and Response, Managed Risk, and Managed Cloud Monitoring. Each of these solutions is delivered as a concierge service and built on the Arctic Wolf Platform.

Arctic Wolf Platform

To successfully defend against today's threats requires analyzing massive amounts of data. This means gathering telemetry from a number of IT and security products and processing it as quickly as possible. While most organizations have tools that generate this data, they lack the ability to make sense of the data or get value from it.

Arctic Wolf® uses the cloud-native Arctic Wolf™ Platform to deliver security operations as a concierge service. While other systems have very narrow visibility from limited dimensions, Arctic Wolf's vendor-neutral platform works with your existing technology stack and records more than 60 billion daily security events from networks, endpoints, and cloud infrastructure to eliminate blind spots.

The platform is designed to collect, enrich, and analyze security data at scale, and is the foundation on which we build our solutions that are delivered by the Concierge Security® Team (CST).

Concierge Security Team

Organizations everywhere struggle to keep up with the increasing volume and complexity of cyberattacks that can lead to costly breaches, significant loss, and downtime. Compounding this challenge is alert fatigue, the lack of process, and the inability to attract and retain the cybersecurity expertise necessary to provide 24x7 coverage of the IT environment.

With a complete understanding of your unique IT environment; the Arctic Wolf Concierge Security® Team (CST) continuously monitors security events enriched and analyzed by the Arctic Wolf™ Platform to provide your resource-constrained IT team with coverage, security expertise, and strategic security recommendations tailored to your specific needs to continuously improve your overall posture.

Managed Detection And Response

Organizations everywhere are struggling with detecting and responding to modern cyberthreats efficiently. While many IT departments have deployed security tools in an attempt to address this, the lack of 24x7 coverage, extensive security expertise, and a well-staffed security team means many threats go unnoticed and can linger in the environment for months. Many high-profile data breaches occur not because the security tool failed to raise an alert — they fail because the alert isn't addressed or is overlooked.

Built on the industry's only cloud-native platform to deliver security operations as a concierge service — the Arctic Wolf™ Managed Detection and Response solution eliminates alert fatigue and false positives to promote a faster response with detection and response capabilities that are tailored to the specific needs of your organization. Your Arctic Wolf Concierge Security® Team (CST) works directly with you to perform threat hunting, incident response, and guided remediation, while also providing strategic recommendations tailored to the unique needs of your environment.

Managed Risk

IT departments everywhere struggle with the complexity of identifying and managing security risks within their environment. Often, even fundamental information like what assets exist, which systems have vulnerabilities, and which systems are not configured properly is too hard to get. And when this information is available it usually overwhelms the security team because existing tools generate too many alerts and lack context. As they struggle with what to do next and how to prioritize, these risks pile up leaving the organization vulnerable to threats and damaging data breaches.

Built on the industry's only cloud-native platform to deliver security operations as a concierge service — Arctic Wolf™ Managed Risk enables you to continuously scan your networks, endpoints, and cloud environments to quantify digital risks. Your security advisor from the Concierge Security® Team (CST) works directly with you to discover risks beyond simple vulnerabilities, benchmark the current state of your environment, and implement risk management processes that harden your security posture over time.

Managed Cloud Monitoring

As businesses everywhere have moved onto the cloud, they have faced new security challenges. Legacy security tools, such as firewalls, advanced endpoint protection, or SIEM appliances, cannot defend cloud workloads, and cloud vendors do not take responsibility for many key security areas. Businesses struggle to staff their teams with cybersecurity cloud experts. And the threat to cloud platforms is rising.

Built on the industry's only cloud-native platform to deliver security operations as a concierge service — Arctic Wolf™ Managed Cloud Monitoring enables you to detect cloud vulnerabilities and attacks as they occur, across multiple major cloud platforms. Your security advisor from the Concierge Security® Team (CST) works directly with you, bringing their cloud security expertise to bear to guide implementation, risk surface identification, and ongoing cloud monitoring, enhancing your cloud strategy security posture.

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.