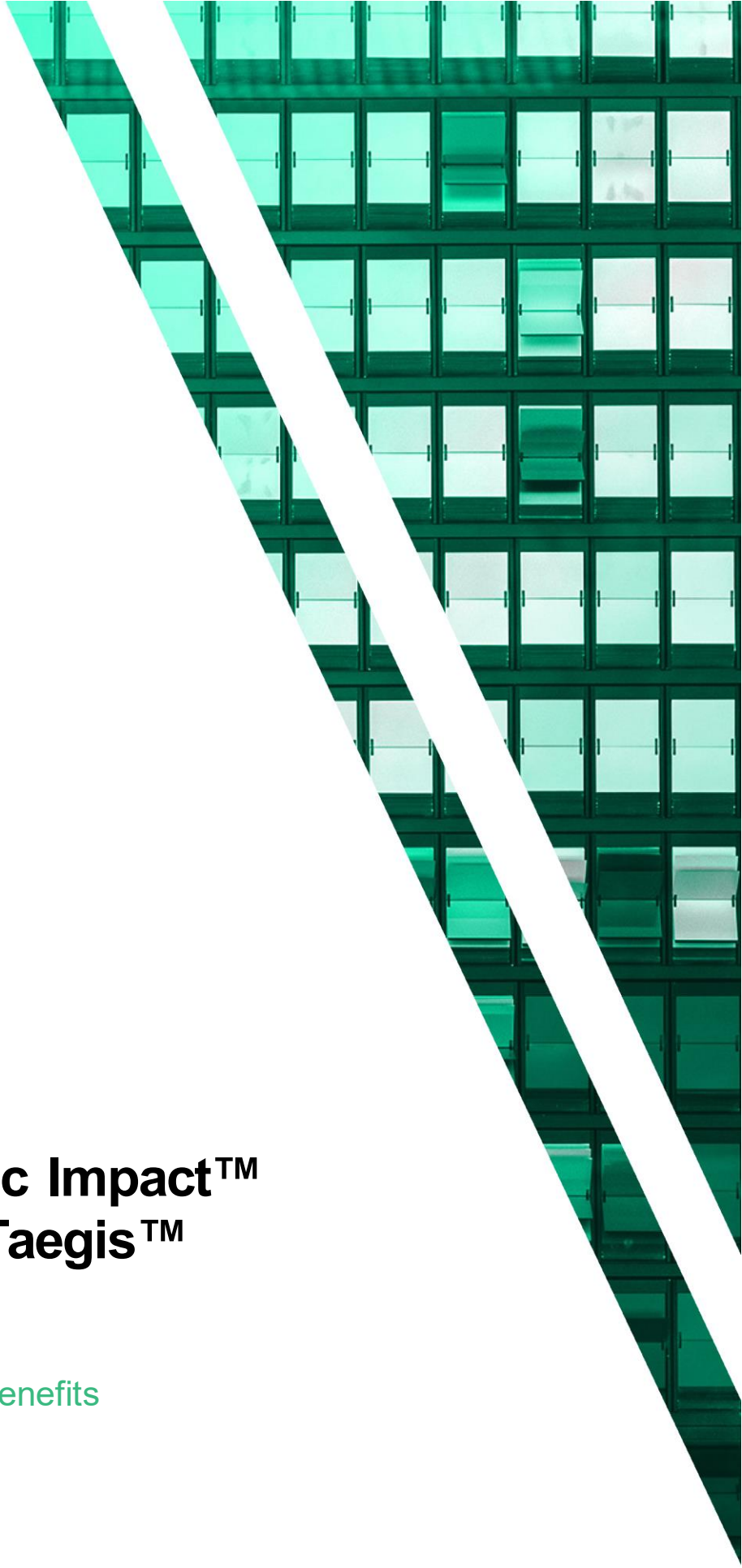
FORRESTER®



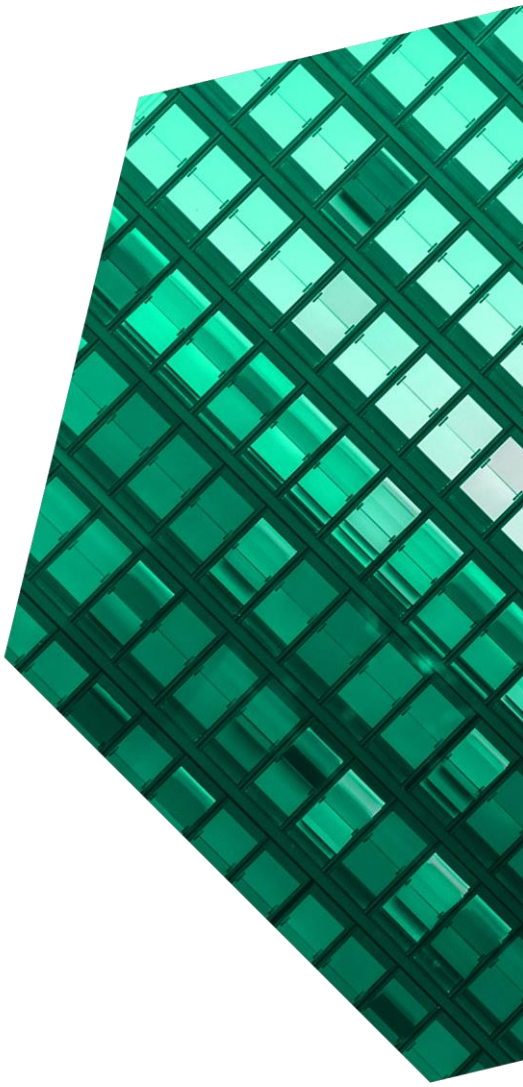
The Total Economic Impact™ Of Secureworks® Taegis™ ManagedXDR

Cost Savings And Business Benefits Enabled By ManagedXDR

December 2020

Table Of Contents

Consulting Team: Amy Harrison



Executive Summary

Secureworks Taegis™ ManagedXDR service, based on its Taegis™ XDR software, delivers the best of two worlds to organizations. Security leaders trust the experts at Secureworks to quickly identify and alert them to legitimate attacks, and to provide the tools for effective collaboration on incident response.

"Using [ManagedXDR], we're not doing it all ourselves, but we have a superior tool set and the ability when we need to." – VP, corporate and information security

Chief information security officers (CISOs) are rapidly becoming business managers who protect their firm's brand, strengthen its reputation, and build customer trust. CISOs wrestle with keeping pace with the latest threats and technologies, while being pressured to wisely leverage their resources to create a team with the right mix of business and technical skills.

Security leaders who were interviewed for this study discuss how they leveraged the capabilities of the ManagedXDR service to capitalize on the experience the Secureworks team brings. This expertise freed up the interviewed customers' internal security operations professionals to perform higher value security work for their company.

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

The ManagedXDR solution delivers security analytics software, 24/7 analyst investigation, threat hunting, and incident response in a single solution. The ManagedXDR solution combines Secureworks Taegis XDR software with a team of experts who cumulatively possess multiple years of experience in detecting, identifying, and responding to security incidents. The combination of XDR software with proactive threat hunting and incident response allows organizations to establish trust and confidence in

KEY STATISTICS

Return on investment (ROI)
413%

Payback period
<3 months

Secureworks to outsource their threat detection and response.

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

Prior to using ManagedXDR, the security leaders utilized legacy technology solutions and hired a team of security operations professionals who spent their days combing through alert logs and looking for abnormalities. However, interviewees found that their teams were overloaded with data, and they would not discover potential threats until days or even weeks later. A study conducted by the Ponemon Institute found that the average cost of a data breach in the year 2020 is $3.86 million, and the average time to

identify and contain a breach is 280 days.[1] It's widely accepted that the longer a breach goes undetected, the more costly it is for the affected organization. Highly regulated industries, such as healthcare and financial services — which are particularly susceptible to intruders — could pay millions of dollars in fines if their breaches are not detected and reported within specific time limits.

Before Secureworks, interviewees universally expressed their lack of adequate staff to provide the 24/7 coverage their organizations required. But, hiring security staff is expensive, time-consuming, and risky, considering the difficulty of retaining security talent.

After the investment in ManagedXDR, the customers described a scenario where for a similar or lower investment, they were able to expand their coverage to 24/7 support, reduce their need to hire additional personnel, and have peace of mind that an experienced partner, with more than 20 years of experience detecting threats, was "watching the shop."

"One of the things that I love about working with Secureworks is that I'm not chasing down noise. Using [ManagedXDR], whenever I get an alert, it is an actual issue that I need to do something with."

Senior security leader, healthcare

KEY FINDINGS

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

- **Decreased risk exposure.** Breaches are inevitable in today's ever-escalating environment. The goal is to minimize the impact of a breach by detecting and responding as quickly as possible. By working with ManagedXDR, and leveraging the Taegis™ XDR software, the composite organization decreased its risk exposure by 85%, saving $1,000,709 over three years.
- **Avoided costs by outsourcing security operations.** By eliminating the need to increase existing security staffing levels, the mid-sized composite organization avoided the cost of hiring and retaining two additional security operations FTEs. This resulted in a three-year, risk-adjusted savings of $1,255,164.
- **Security team productivity gains of $383,532 over three years.** By leveraging ManagedXDR, interviewees increased their coverage from an eight-hour day to 24/7 support. Because their security teams were spending less time on tedious but crucial Level 1 type work, they now were freed up to perform more productive and valuable work for the organization. Interviewees reported that their security analysts now have time to improve their skills and education, proactively look for security threats, and represent the security team proactively in new projects being developed.
- **Business user productivity gains of $950,572 over three years.** In addition to lost revenues or loss of business due to system downtime, a breach forces a halt in productivity of most information workers. This impacts the business' ability to conduct back-office tasks, which forces delays in accounts payable or receivable. One information security and compliance leader described getting hit with a virus, which took eight hours to remediate before Secureworks.

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

- **Baseline security reviews help leaders take proactive steps.** In the quarterly security baseline review, Secureworks analyzes data from their customers' infrastructure and applies threat intelligence to make recommendations to increase their security standing. Security leaders leverage QBR reports to inform their executives about the current posture of the company and the potential need of a future roadmap.
- **Internal implementation costs total $1,711.** Customers described a straightforward implementation at a low cost. To roll out and deploy Secureworks, organizations devoted one FTE for four weeks to install agents on their endpoints and point their logs to Secureworks.
- **Insider threat detection.** ManagedXDR helped organizations discover threats both from inside and outside the company. Insider incidents can result in fraud, privacy abuses, IP theft, and other damage. By quickly identifying and addressing insider threats, interviewees described being able to isolate and remove troubling staff from their team.
- **Early alerts build trust, even if they are false positives.** All interviewees described scenarios where the Secureworks team alerted them to potential incidents. Not all of these alerts were true external threats, but because the ManagedXDR team quickly picked them up within minutes, skeptical security professionals began to build trust with Secureworks experts.
- **Additional avenues to detect threats and enhance visibility into security gaps.** Organizations' growing remote workforce, combined with a shortage of skilled security professionals, makes their endpoints easier to reach and exploit. ManagedXDR includes an endpoint agent to identify advanced threats and threat actors that may attempt to infiltrate their organization. This capability also provides heightened visibility to keep up with adversaries and eliminate security gaps.

Costs. The three-year, risk-adjusted PV costs include:

- **The cost of ManagedXDR is $698,308.** ManagedXDR includes Taegis XDR software. Pricing is established based on the number of endpoints being covered. In addition, included in the fees paid to Secureworks are 40 hours of offsite incident response support, monthly threat hunting, and quarterly baseline security reviews.

The customer interviews and financial analysis found that a composite organization experiences benefits of nearly $3.6 million over three years versus costs of $700,019, adding up to a net present value (NPV) of $2.9 million and an ROI of 413%.

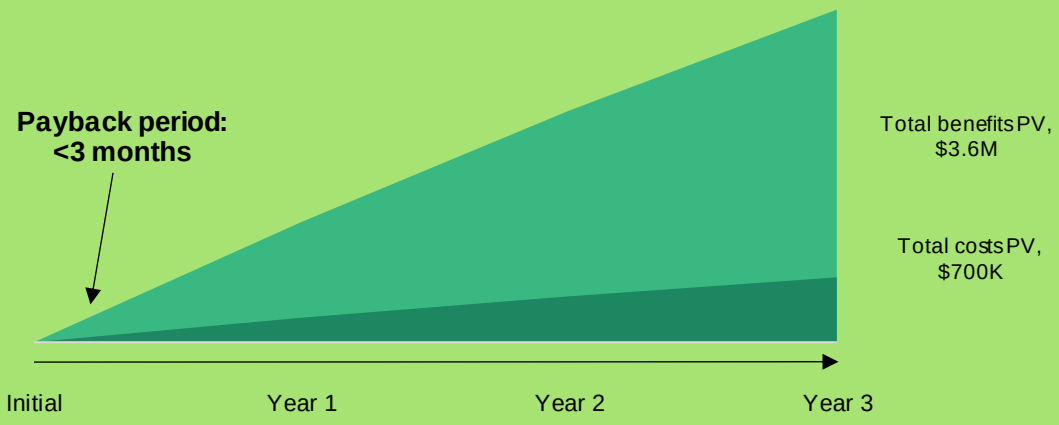
ROI
413%

BENEFITS PV
$3.6M

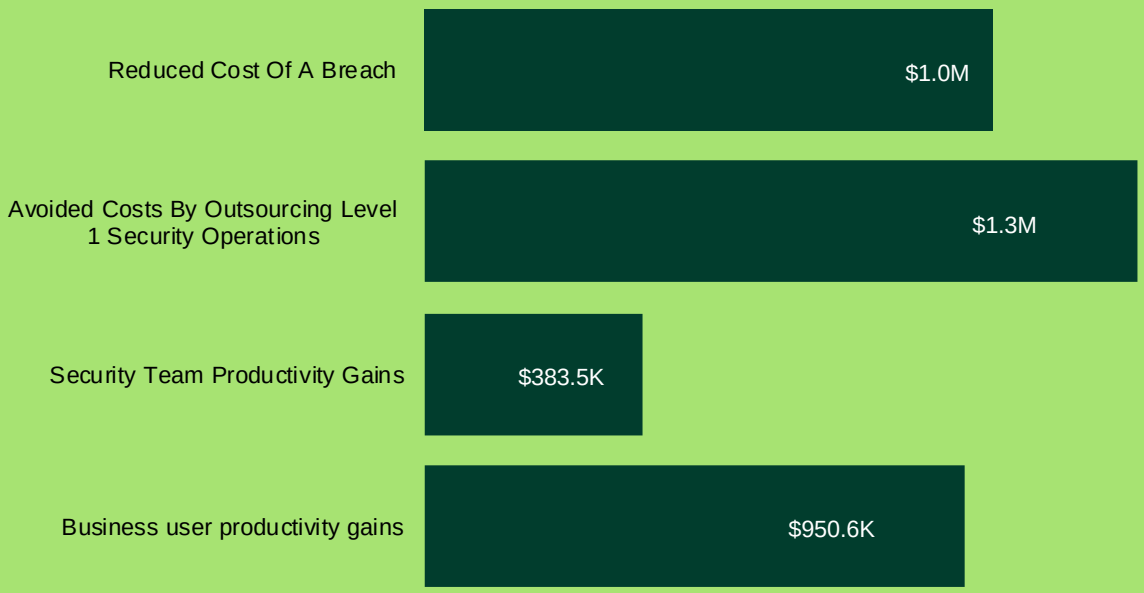
NPV
$2.9M

PAYBACK
<3 months

Financial Summary



Benefits (Three-Year)



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 ManagedXDR.

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 ManagedXDR can have on an organization.

DUE DILIGENCE

Interviewed Secureworks stakeholders and Forrester analysts to gather data relative to ManagedXDR.

CUSTOMER INTERVIEWS

Interviewed four decision-makers at organizations using ManagedXDR to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewed 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 interviewed organizations.

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 Secureworks® Taegis™ ManagedXDR Customer Journey

Drivers leading to the ManagedXDR investment

Interviewed Organizations				
Industry	**Region**	**Revenue**	**Interviewee**	**Employees**
Retailer	Headquartered in the United States	$1.2 billion	Information security and compliance leader	10,000
Financial services	Headquartered in Canada	$60 million	IT infrastructure and operations leader	250
Healthcare	Headquartered in the United States	Estimated $5 million to $10 million	Senior security leader	28
High tech	North American, headquartered in Japan	$4 billion	VP, corporate & information security	18,000

KEY CHALLENGES

The interviewed organizations struggled with common challenges, including:

- **Security software deployed without a comprehensive plan.** One interviewee described their security strategy as being the "wild, wild west" before they started working with ManagedXDR. Meaning, they had legacy security technologies deployed across the organization with no centralized place to look at events or logs.

> **"I'm doing quarterly briefings with our executive team, just to let them know what's going on in the threat landscape. They want to know where we're strong, where we're weak, and what we're doing to fix that, and how we compare to our competitors. We discuss the threat landscape because we were hit with a ransomware attack in the past, and this executive team is very leery of being hit again."**
>
> *Information security and compliance leader, retail*

- **Delayed event notification.** An interviewed organization experienced an external breach followed by a ransomware attack. Their previous provider did not notify them of the brute force attack until a week after it occurred.

  A study conducted by the Ponemon Institute reported that the number of insider-caused cybersecurity incidents has increased by 47% since 2018. In this same study, it was said that the average annual cost of insider threats has skyrocketed in only two years, rising 31% to $11.45 million.[2]

  The IT leader from the financial services firm described a scenario where an employee was running PowerShell on their SharePoint servers, which is a potential signal of an internal threat that is notoriously difficult to detect and prove. He said: "The fact that Secureworks phoned me within 15 minutes was really amazing. Just from going through logs manually, there is no way I would have discovered it in that amount of time. If undiscovered, it could have been incredibly significant."

- **Aging legacy solutions.** Interviewees from larger organizations described using legacy endpoint protection security information and event management solutions (SIEMs), but as these technologies started to age out, they were looking for a way to boost their coverage without increasing bottom-line costs. This, along with a desire to maximize the skills of existing staff, was the catalyst for exploring new technology and service options.

> **"When we were looking at hiring a security analyst internally, I would still have to get them to set up a SIEM and that could take a year or two to do. There's no quick win when you're trying to do it internally from my perspective. From our perspective, we're getting a lot more value in terms of features and capabilities of the service, than I could ever get with a single security analyst."**
>
> *IT infrastructure and operations leader, financial services*

- **Insufficient internal expertise for threat detection without significant investment.** The question of whether to build or outsource Level I type security operations center (SOC) work is about more than just deploying a comprehensive security toolset. Finding and retaining security professionals is tedious and expensive. One information security and compliance leader explained their thinking when exploring the buy versus build question: "First of all, the tools are ridiculously expensive if you are going to pick any of the big ones. I'm going to have to go out and hire like 12 experienced security professionals, and now I've got the headache of trying to keep them. Good luck, it's insane."

> **"We wanted to maximize the budget that we have and level up the skills on my team. So, we just made a decision to take that Level 1, Level 2 SOC analysis out of the organization."**
>
> *Information security and compliance leader, retail*

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and a ROI analysis that illustrates the areas financially affected. The composite organization is representative of the four companies 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 mid-sized composite organization has more than $500 million in revenue and is a business-to-consumer organization that provides services to their customers. They are a fast-growing business which is increasingly aware of how a breach could impact the brand they've worked so hard to build. They need to protect the personal identifiable information (PII) of their employees and customers, or risk being subject to regulatory fines.

Deployment characteristics. The composite organization has 1,500 employees and covers 1,800 endpoints. Currently, the security organization is made up of a VP of IT, who has oversight of all security technologies, and two full-time security operations professionals. They previously explored building out their own incident response team but chose instead to work with Secureworks.

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	Decreased risk exposure	$402,400	$402,400	$402,400	$1,207,200	$1,000,709
Btr	Avoided costs by outsourcing security operations	$504,720	$504,720	$504,720	$1,514,160	$1,255,164
Ctr	Security team productivity gains	$154,224	$154,224	$154,224	$462,672	$383,532
Dtr	Business user productivity gains	$382,239	$382,239	$382,239	$1,146,717	$950,572
	Total benefits (risk-adjusted)	$1,443,583	$1,443,583	$1,443,583	$4,330,749	$3,589,977

DECREASED RISK EXPOSURE

Secureworks enabled organizations to reduce risk exposure in the following ways:

- The technology component (Taegis XDR) of the solution provides security professionals the ability to rapidly detect and respond to advanced threats by using embedded proprietary threat intelligence, which automatically correlates endpoint, network, and cloud activity.
- The ManagedXDR service detects security-related data from endpoints, networks, cloud, and other business systems, investigates which events require action, performs impact analyses, and provides recommended actions to the customer.
- The experts at Secureworks can quickly take the appropriate threat response actions for the event. And for critical events, the incident response team is engaged.
- The senior security leader described how a threat would have impacted their organization. He said: "Before we centralized security and hired Secureworks, naive would be a good word to describe our environment. It was the perfect storm for a breach to happen. Fines start at $10,000 per Social Security number, so it could have cost us millions. It could have been very, very bad, and we were just extremely lucky about the fact that none of the data was taken."

The cost of a breach should be measured by evaluating both direct and indirect costs. For example, regulatory penalties include more than just fines: They run the gamut from mandatory audits, changes to a security program, and, in some jurisdictions, even imprisonment.

In July of 2020, Forrester fielded a survey to 300 security decision-makers to understand more around the costs involved when experiencing a breach. The Forrester TEI "Cost Of A Security Breach" survey[3] is being used as a reference point for the calculation of this benefit.

Modeling and assumptions. This section explains how the modeling is done.

- The Forrester TEI Security survey found that, on average, organizations experienced 2.6 breaches per year regardless of size of organization.
- The cost of a breach is the sum of the categories listed in Figure 1, captured from the Forrester TEI Security survey. Each category is the result of the

mean value from the survey or the specific company size of 1,000 to 1,999 employees, which is modeled after the composite organization.

- Based on the proportion of interviewees who experienced incidents or breaches, Forrester assigned a probability of experiencing such event at 50%.
- Forrester assigned an 85% improvement in avoiding costs associated with a breach by working with Secureworks, based on customer and analyst interviews.

Risks. The following risks may affect this benefit category:

- The actual number of breaches an organization experienced.
- The jurisdiction and corresponding regulatory polices where the breach occurred.
- The degree of exposure the breach introduced.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1,000,709.

Figure 1

Costs Incurred From External Sources Due To A Security Incident/Breach

Response and notification to affected parties' costs	$8,222
Regulatory fines	$19,940
Customer compensation	$18,744
Customer lawsuits/punitive damages	$43,462
Additive audit and security compliance costs	$24,206
Lost revenues/loss of business due to system downtime	$35,600
Lost revenues from customer loss	$50,547
Cost to rebuild brand equity	$13,833
Customer churn/cost to acquire new customers	$190,071
Total costs	**$404,625**

Decreased Risk Exposure

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
A1	Number of breaches annually	Forrester data	2.6	2.6	2.6
A2	Costs incurred with a breach	Forrester data	$404,625	$404,625	$404,625
A3	Total potential cost of a breach	A1*A2	$1,052,025	$1,052,025	$1,052,025
A4	Probability of experiencing a breach	50%	50%	50%	50%
A5	Reduced risk exposure after Secureworks	85%	85%	85%	85%
At	Decreased risk exposure	A3*A4*A5	$447,111	$447,111	$447,111
	Risk adjustment	↓10%			
Atr	Decreased risk exposure (risk-adjusted)		$402,400	$402,400	$402,400
	Three-year total: $1,207,200			**Three-year present value: $1,000,709**	

AVOIDED COSTS BY OUTSOURCING SECURITY OPERATIONS

Evidence and data. A Forrester report states: "Building and operating a security operations center (SOC) requires massive investment and difficult decisions, and one of the critical gating factors of success is skill availability. While technical experts and software vendors have done great work building solutions, an SOC is nothing without the right people."[4]

Interviewees were resolute in their descriptions of value received from ManagedXDR, as opposed to building out a 24/7 SOC or trying to cover security operations with the level of staffing their sized organization could afford.[5] The IT infrastructure and operations leader said, "If we were to get somewhat comparable value to ManagedXDR, we would need to hire at least three people, salary-wise, but that does not include the tools that would have been needed."

Several interviewees described the following reasons why they chose to use Secureworks instead of building out their own SOC:

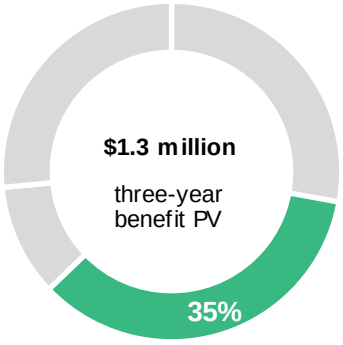
- The information security and compliance leader from a retail organization said: "I had a job posting a few months ago, and we had hundreds of people applying for it. Many were just not motivated or qualified. It's hard to find the right person and keep them, because you honestly can go down the street and make 10% to 15% more."
- The IT infrastructure and operations leader for the financial services organization said: "The value comes from having this outsourced team that our experts own, but not having to try to hire someone. Most good security analysts get gobbled up by government agencies."
- The senior security leader for the healthcare organization said: "We're a small business and everybody does everything. Not only do we have to find the right skill level, but we need to try and find a security guy that's also cool with building out an [hardware] machine."

> **"We're paying the same money to Secureworks as we would pay an engineer or analyst to work 8 hours a day, but we get 24-hour coverage. Plus, we had 40 hours of incident response offsite capabilities. Having someone we can call to walk through issues with us is a nice feature to have."**
>
> *Information security and compliance leader, retail*

Modeling and assumptions. The composite organization is a mid-sized firm with three full-time security operations professionals, and the leader of this team spends half of his time on security-related work. The model is built assuming requirements for a mid-sized organization.

- The model assumes the avoided cost of three additional full-time security operations FTEs required to perform Level 1 SOC operations in a mid-sized company. Note: Enterprise organizations that require 24/7 coverage would need a total of 11 FTEs (see Appendix C for values related to the avoided costs of enterprise-sized organizations).
- The cost of a fully burdened security operations FTE is $144,000.

- The cost to hire and retain a security operations professional is equivalent to 20% of their annual salary.



Risks. The benefits of outsourcing a security operations center may vary by the following factors:

- The size of the organization.
- The level of security coverage required.
- The cost of a security operations professional.
- The level of hiring competitiveness in the geographic market.

To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $1,255,164.

Avoided Costs By Outsourcing Security Operations

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
B1	Number of security analysts hiring avoided	Interviews	3	3	3
B2	SecOps FTE annual cost, inclusive of benefits	$120,000*1.2	$144,000	$144,000	$144,000
B3	Average recruiting and retention cost per security analyst	(B2*20%)*B1	$86,400	$86,400	$86,400
B4	Avoided cost of previous SIEM hardware, software, and support	Interviews	$112,500	$112,500	$112,500
Bt	Avoided costs by outsourcing security operations	B1*B2+B3+B4	$630,900	$630,900	$630,900
	Risk adjustment	↓20%			
Btr	Avoided costs by outsourcing security operations (risk-adjusted)		$504,720	$504,720	$504,720
	Three-year total: $1,514,160		**Three-year present value: $1,255,164**		

SECURITY TEAM PRODUCTIVITY GAINS

Evidence and data. Interviewees described that their security operations professionals were forced to spend their time looking at the multitudes of data streams and alerts and filtering out all the noise to determine which anomaly is a potential breach and worth investigating further. Secureworks Taegis XDR software analyzes an organization's data, applies advanced analytics, and provides threat intelligence alerts for any suspicious activity that needs attention.

Adding the ManagedXDR service immediately alerts the security team of threats, which reduces response times around the clock. Interviewees who previously were not able to respond to threats in off hours were now able to cover their operations with 24/7 support.

In one full quarter of ManagedXDR monitoring, one organization had more than 15 million alerts: 99.99% of the alerts were categorized at a lower level of informational severity, while 32 alerts were analyzed through Alert Triaging by the Secureworks SecOps team as part of the ManagedXDR. According to the Ponemon report, "On average, analysts were spending 24 and 30 minutes to investigate each incident they received." Much of this time is spent

downgrading alerts that have been incorrectly marked as critical (46%), mis-prioritized (52%), or determined to be a false positive (31%).[6] Because their security teams were spending less time on tedious but crucial Level 1 type work, they now were freed up to perform more productive and valuable work for the organization.

The information security and compliance leader discussed how his team not only provided more value-add work for the organization, but they had also gained more time to improve their skills, which led to a better employee experience for his team.

One executive said: "I had a team who was basically reading speeds and feeds, trying to figure out what was going on with alerts, and then closing them out all day long. Secureworks has allowed me to take that Level 1 SOC type analysis offsite and increase our coverage to 24-hour support. My team can level up on their incident response skills, and [they] have become internal consultants to the organization, getting out in front of our projects. They have time to be a voice of security and privacy in the design phase."

> **"We wanted to maximize the budget that we have and level up the skills on my team. So, we just made a decision to take that Level 1 and Level 2 SOC analysis out of the organization."**
>
> *Information security and compliance leader, retail*

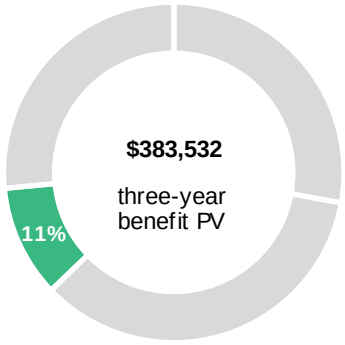
Modeling and assumptions. For the composite analysis, Forrester assumes:

- The composite organization has 2 security FTEs. Because the ManagedXDR team is handling Level 1 work, two FTEs are now free to perform higher productivity work such as proactive threat hunting, improving their skills, and acting as a security consultant in the planning phases of IT projects.
- Team members only need to spend 15% of their time performing analysis and reacting to threats.
- The cost of one fully burdened security operations FTE is $144,000.
- As a modeling best practice, Forrester applies a productivity recapture. Because not all time regained will be reutilized for new value-add work, there a 70% productivity recapture rate was applied to this benefit.

Risks. The following risks can affect the realization of this benefit:

- The number of security operations professionals may vary by company size.
- The salaries may vary by geographic region.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $383,532.



Security Team Productivity Gains					
Ref.	**Metric**	**Calculation**	**Year 1**	**Year 2**	**Year 3**
C1	SecOps FTEs reallocated from decreased incident rate		2	2	2
C2	Reduction in SOC work due to ManagedXDR		85%	85%	85%
C3	Security Ops FTE annual cost, inclusive of benefits	$120,000*1.2	$144,000	$144,000	$144,000
C4	Productivity recapture	Forrester best practice	70%	70%	70%
Ct	Security team productivity gains (risk-adjusted)	C1*C2*C3*C4	$171,360	$171,360	$171,360
	Risk adjustment	↓10%			
Ctr	Security team productivity gains (risk-adjusted)		$154,224	$154,224	$154,224
	Three-year total: $462,672			**Three-year present value: $383,532**	

BUSINESS USER PRODUCTIVITY GAINS

Evidence and data. Security events not only impact the productivity of security and IT teams, but also have a profound impact on business users. Whether it's the hours or days it takes to rebuild a worker's corrupted laptop or the negotiation of a ransomware attack, the halts in productivity are debilitating.

One senior security leader of a healthcare organization described how the business disruption impacts both staff and customers: "One of our [software] clients had an attack, and their [healthcare] clinics were down for about four to five days. That was six months ago, and they are still recovering from the effects of it. Their nursing staff are working an extra 30 to 40 hours more each week for about a month, just to get caught up on data entry and inventory. So far, I would estimate it cost them 2,000 or 3,000 extra hours. We've heard reports their patients are waiting in line [for] 5 hours to get medicines. So, it really affects literally everybody."

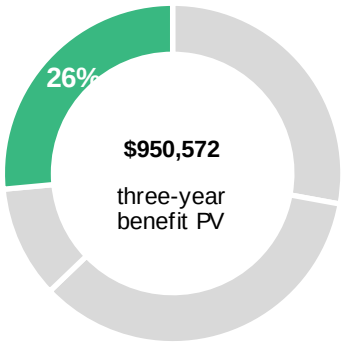
Modeling and assumptions. To measure the impact on productivity of business users for the composite organization, Forrester made the following assumptions:

- The Forrester TEI security survey found that on average, organizations experienced 2.6 breaches per year, regardless of organization size.
- The findings from the Forrester TEI security survey showed the average downtime for an employee during a security incident/breach is 3.3 hours.
- The cost of an average fully burdened business user FTE is $33 per hour.
- The composite organization has 1,500 employees.

Risks. The following risks can affect the realization of this benefit:

- The number of breaches may decrease.
- The average number of hours per employee may vary by industry.
- The size of the attack and number of employees.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $950,572.



Business User Productivity Gains

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
D1	Number of breaches	Forrester TEI Cost Of A Security Breach survey	2.6	2.6	2.6
D2	Average downtime in hours for an employee during a security incident/breach	Forrester TEI Cost Of A Security Breach survey	3.3	3.3	3.3
D3	Average salary, benefits included, for business user	Payscale	$33	$33	$33
D4	Number of employees	Composite	1,500	1,500	1,500
Dt	Business user productivity gains	D1*D2*D3*D4	$424,710	$424,710	$424,710
	Risk adjustment	↓10%			
Dtr	Business user productivity gains (risk-adjusted)		$382,239	$382,239	$382,239
	Three-year total: $1,146,717			**Three-year present value: $950,572**	

UNQUANTIFIED BENEFITS

Additional benefits that customers experienced but could not quantify include:

- **Baseline security reviews help leaders take proactive steps.** The security baseline review initially reviews the baseline infrastructure and explains their methodologies. Secureworks then analyzes data from the customer's infrastructure and applies their own threat intelligence to make recommendations about how the customer can change their infrastructure, operations, or procedures to better align with what Secureworks is seeing as threats. The leader of IT infrastructure and operations said: "That saves one of my guys operationally from having to come up with a playbook, take the time to execute it, and then report back to me. Once a month, I get this report from Secureworks, which I use to inform my superiors, which is a big help."
- **Detecting insider threats.** Whether accidental or malicious, insider incidents can result in fraud, privacy abuses, IP theft, and other damage. It's difficult for security professionals to detect this activity because insiders need privileged access to do their jobs. Also, as employees, they're entitled to privacy and due process, so security professionals must handle these incidents with greater care.[7]

  One leader of information security and compliance described how Secureworks uncovered an insider threat that finally allowed him to move the employee out of the organization: "One of my team members was an SOC analyst, but he was also a hacker. He was an OSCP, running some scripts on company machines without my knowledge. The guy was an insider threat and wouldn't follow our governance. Secureworks was able to alert me to his suspicious activity, and ultimately it was a major piece of evidence to let him go."[8]
- **Early alerts build trust, even if they are false positives.** Several interviewees described that the Secureworks team alerted them to potential breaches within 15 minutes. Some of these alerts were legitimate uses of technology by insiders, but because they were caught so quickly, it helped to build trust with leery security teams.

FLEXIBILITY

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

- **Proactive threat hunting.** It is critical to have both the skills and resources to proactively hunt for threats. One leader of information security and compliance described how in addition to scanning endpoints, Secureworks found circle accounts in their proactive threat hunting effort. He said: "Secureworks found a domain administrator account that was being used as a service account. It was really good to see that they were able to go back and look at logs over the course of weeks and identify this issue." The IT infrastructure and operations leader said that Secureworks helped them proactively look for emerging threats. In April of 2020, COVID-19 ransomware threats were becoming more prevalent, and he described how Secureworks helped his organization, "They dive into your infrastructure and explore your logs, looking for the type that bad actors could exploit."

Enterprise Organization Highlights

ENTERPRISE EXPERIENCES

Interviewees from enterprise organizations experienced similar challenges as the composite organization but at a different scale. The demands of the business and the size of the enterprise organization highlighted the following differences:

- **Security FTEs want to interact directly with threat detection tools.** Enterprises often have larger teams dedicated to security and reams of business data to protect, from their many networks and cloud solutions to their thousands of endpoints. Security operations professionals require the ability to delve into Taegis XDR dashboards and collaborate with Secureworks experts when needed. The VP of corporate information and security said: "You're giving us access to some of the tools [Secureworks] used behind the scenes, giving us so much more ability to do analysis threat research on our side. We now have an advanced set of tools and when we need Secureworks expertise, they are at our fingertips. We've been very happy."

"We're a huge global corporation with lots of intellectual property, data from thousands of employees which is desirable for the adversary. We can't forget who our biggest clients are. Banks, financial institutions, some of the biggest companies in the world. While we may not be a bank and under federal regulation, our customers are."

VP, corporate and information security, high tech

- **Data protection requirements expand beyond the enterprise to the customer ecosystem.** Organizations must not only protect their own data, but they are also legally bound to safeguard their customers' data. The exposure of this data would result in regulatory fines and severe damage to the brand.
- **Enterprises require 24/7 support.** Enterprise-level interviewees researched building their own security operations center, which requires 24/7 support for the coverage of three shifts, plus backup staff. This compounds the time and expense of hiring and retaining more than 11 staff members. In addition, infrastructure requirements such as hardware, storage, software, and maintenance costs quickly add up. Forrester modeled what the benefit might look like for an enterprise organization. And the result was savings of over four million dollars over three years. See Appendix C for more details.

"If we had to run an SOC with my current staff, we flat out couldn't do it. The thought of trying to find 12 qualified people was daunting enough. I didn't want to hire them, and I didn't want to have to try and retain 12 people. Now, we've got better tools, we're able to take certain actions and get certain data and do investigations that prior to working with [Secureworks Taegis XDR], we just weren't able to do."

VP, corporate and information security, high tech

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	Total fees paid to Secureworks	$0	$280,800	$280,800	$280,800	$842,400	$698,308
Ftr	Internal implementation cost	$0	$1,882	$0	$0	$1,882	$1,711
	Total costs (risk-adjusted)	$0	$282,682	$280,800	$280,800	$844,282	$700,019

TOTAL FEES PAID TO SECUREWORKS

Evidence and data. ManagedXDR includes Taegis XDR software. Pricing is established based on the number of endpoints being covered. For the composite organization:

- The number of endpoints is established by adding 20% to the number of employees.
- The pricing reflects both the cost of ManagedXDR and Taegis XDR software.

Also included in the pricing are:

- Forty hours of remote incident response with more than 1,600 IR engagements performed per year as a knowledge base.
- Proactive threat hunting by the advanced team of global threat hunters at Secureworks.
- Quarterly baseline security reviews.

Risks. The pricing will vary by:

- The number of endpoints being covered, and the volume of discounts being applied.
- Additional services added such as onsite incidence support.

To account for these risks, Forrester adjusted this cost upward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $698,308.

Total Fees Paid To Secureworks						
Ref.	**Metric**	**Calculation**	**Initial**	**Year 1**	**Year 2**	**Year 3**
Et	Total fees paid to Secureworks		$0	$234,000	$234,000	$234,000
	Risk adjustment	↑20%				
Etr	Total fees paid to Secureworks (risk-adjusted)		$0	$280,800	$280,800	$280,800
	Three-year total: $842,400			**Three-year present value: $698,308**		

INTERNAL IMPLEMENTATION COST

Evidence and data. Interviewees described the ease of getting ManagedXDR up and running. The costs considered for the composite organization included:

- Four weeks to install agents on their endpoints and point their logs to Secureworks.
- One full-time FTE performing this work for 8 hours a day.
- The fully burdened hourly cost for the FTE is $49 per hour.

Risks. The time to deploy may vary by:

- The size of the organization.
- The number of endpoints being covered.

To account for these risks, Forrester adjusted this cost upward by 20%, yielding a three-year, risk-adjusted total PV of $1,711.

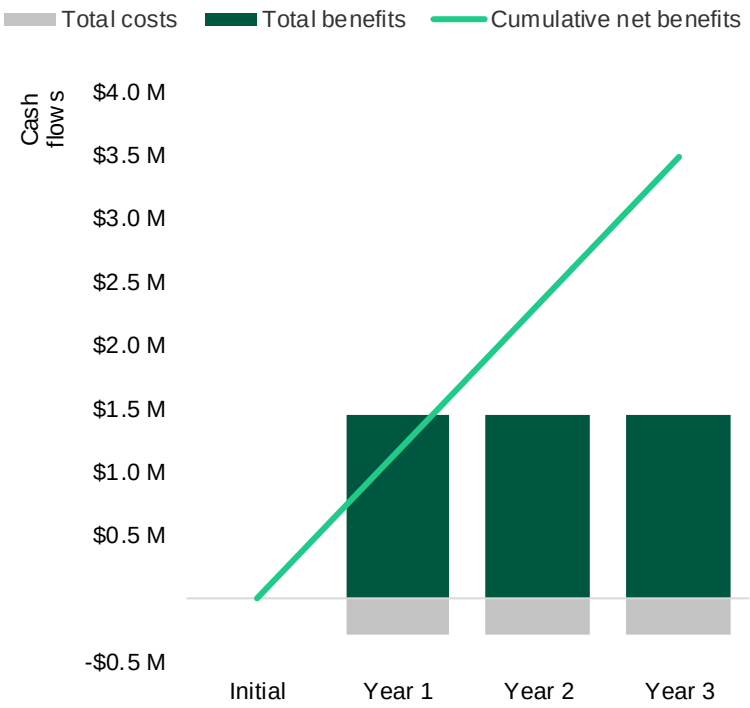
Internal Implementation Cost

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
F1	Length of implementation	4 weeks		4		
F2	Security FTEs required for implementation			1		
F3	Hours spent per week on implementation			8		
F4	Average hourly security FTE cost (rounded to nearest dollar)			$49		
Ft	Internal implementation cost	F1*F2*F3*F4	$0	$1,568	$0	$0
	Risk adjustment	↑20%				
Ftr	Internal implementation cost (risk-adjusted)		$0	$1,882	$0	$0
	Three-year total: $1,882			**Three-year present value: $1,711**		

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	$0	($282,682)	($280,800)	($280,800)	($844,282)	($700,019)
Total benefits	$0	$1,443,583	$1,443,583	$1,443,583	$4,330,749	$3,589,977
Net benefits	$0	$1,160,901	$1,162,783	$1,162,783	$3,486,467	$2,889,958
ROI						413%
Payback						<3 months

Appendix A: Total Economic Impact

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

TOTAL ECONOMIC IMPACT APPROACH

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

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

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

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

PRESENT VALUE (PV)

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

NET PRESENT VALUE (NPV)

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

RETURN ON INVESTMENT (ROI)

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

DISCOUNT RATE

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

PAYBACK PERIOD

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

Appendix B: About Secureworks

Secureworks (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

Appendix C: Enterprise Organization Benefits

The following table outlines the avoided costs enterprise organizations can expect from outsourcing Level 1 security operations. While the original benefit analysis for this cost avoidance was based on a mid-sized firm with three full-time security operations professionals (see Table B), the following table has been adjusted to account for the scale inherent in an enterprise organization.

Enterprise Avoided Costs By Outsourcing Level 1 Security Operations

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
X1	Number of security analysts hiring avoided	Interviews	11	11	11
X2	SecOps FTE annual cost, inclusive of benefits	$120,000*1.2	$144,000	$144,000	$144,000
X3	Average recruiting and retention cost per security analyst	(X2*20%)*B1	$316,800	$316,800	$316,800
X4	Avoided cost of previous SIEM hardware, software, and support	Interviews	$112,500	$112,500	$112,500
Xt	Enterprise avoided costs by outsourcing Level 1 security operations	X1*X2+X3+X4	$2,013,300	$2,013,300	$2,013,300
	Risk adjustment	↓20%			
Xtr	Enterprise avoided costs by outsourcing Level 1 security operations (risk-adjusted)		$1,610,640	$1,610,640	$1,610,640
	Three-year total: $4,831,920		**Three-year present value: $4,005,423**		

Appendix D: Endnotes

[1] Source: “Cost of a Data Breach Report 2020,” Ponemon Institute, April 2020.
[2] Source: “2020 Cost of Insider Threats Global Report,” Ponemon Institute.
[3] Source: “Cost Of A Security Breach,” Internal Forrester Survey Data, August 2020. Forrester conducted a survey with 300 global cybersecurity leaders in August of 2020 to determine the impact of cybersecurity breaches. The survey encapsulates organizations with a minimum of 1,000 FTE and quantifies the financial impact experienced. The cost of a material breach indicated is based upon the FTE count and revenue figures per annum, adjusted to the composite organization used in this study. Factors that contribute to the cost of a breach include: Response and notification to affected parties, regulatory fines, customer compensation, customer lawsuits /punitive damages, additive audit and compliance costs, lost revenues/loss of business due to system downtime, lost revenues from customer loss, cost to rebuild brand equity, customer churn/cost to acquire new customers and the cost of internal workforce productivity loss.
[4] Source: “Security Operations Center (SOC) Staffing,” Forrester Research, Inc., August 2, 2013.
[5] Level 1 SOC analysts are triage specialists who monitor, manage, and configure security tools, review incidents to assess their urgency, and escalate incidents if necessary.
[6] Source: “Cost of a Data Breach Report 2020,” Ponemon Institute, April 2020.
[7] Source: “Recruiting And Retaining Insider Threat Analysts,” Forrester Research, Inc., March 7, 2019.
[8] OSCP: offensive security certified professional.


FORRESTER®