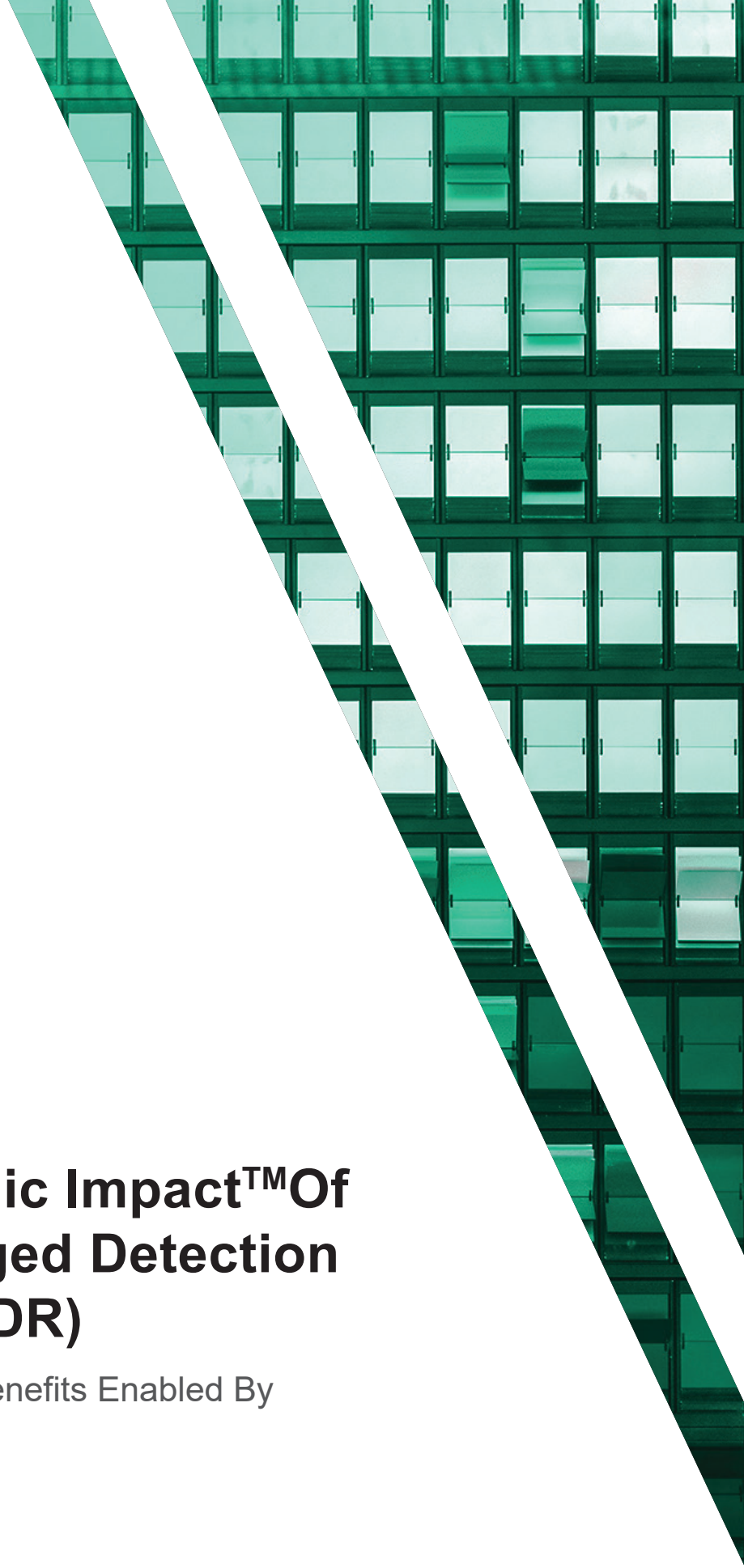
FORRESTER®



The Total Economic Impact™ Of Deepwatch Managed Detection and Response (MDR)

Cost Savings And Business Benefits Enabled By Deepwatch MDR

NOVEMBER 2021

Table of Contents

Executive Summary **3**

Key Findings 4

TEI Framework and Methodology 6

The Deepwatch Managed Detection and Response Customer Journey **7**

Interviewed Organization 7

Key Challenges 7

Analysis of Benefits **8**

Efficiency Gain Through Automation 8

Reduced Event Response Cost 10

Retired Legacy System 11

Unquantified Benefits 12

Analysis Of Costs **14**

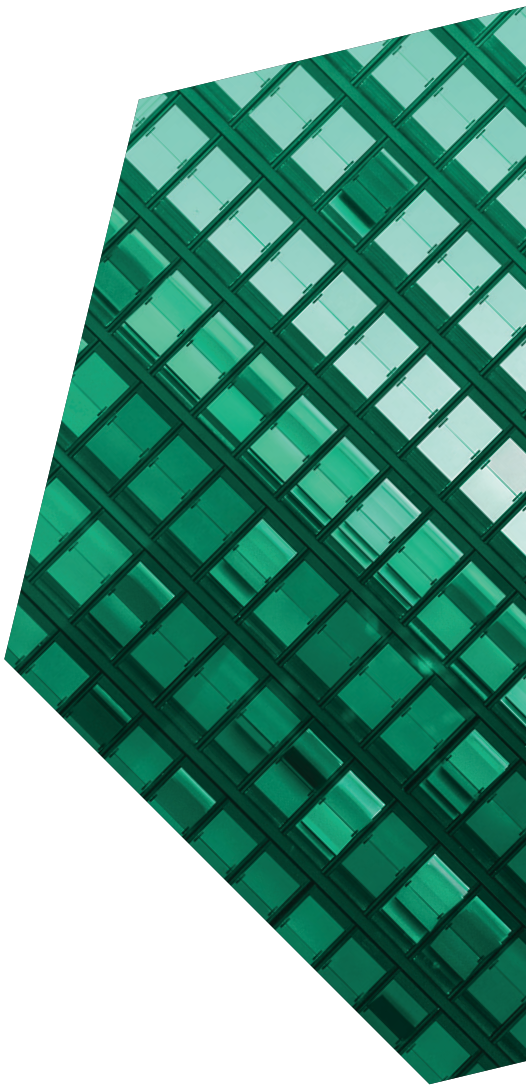
Fees Paid To Deepwatch 14

Financial Summary **15**

Appendix A: Total Economic Impact **16**

Appendix B: Endnotes **17**

Project Lead: Mary Barton



Executive Summary

Organizations use Deepwatch to allow their security teams to move from reactive to proactive initiatives, achieving a significant reduction in incident response costs, a higher security maturity rating, and an improved ability to respond to new threats in a complex and dynamic environment.

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

Deepwatch provides managed detection and response protection 24/7/365 via Deepwatch MDR, which is backed by a team of resources referred to as the "Deepwatch squad". Each squad includes named resources that develop a deep, contextual knowledge of each customer's IT environment, security posture, key areas of risk and tolerance, and unique reporting requirements. This contextual awareness allows Deepwatch MDR to identify potential threats and continually improve their customers' risk profiles. Shared dashboards, ticketing, access to named resources 24/7/365 and real-time communications via third-party apps, phone, or email enable customers to be in constant communication with Deepwatch MDR. Deepwatch MDR builds and maintains a proprietary Security Content Library with updated security content, related use cases, and new content developed on a weekly basis. The squads leverage Deepwatch MDR's proprietary maturity model (patent pending), which provides a clear roadmap and next best actions for customers to benchmark and improve their overall security posture.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed one experienced Deepwatch MDR user, Alliance Data. Forrester used this experience to project a three-year financial analysis.

KEY STATISTIC CALL OUT

Return on investment (ROI)	Net present value (NPV)
432%	**$8.2 million**

Prior to using Deepwatch MDR, Alliance Data was utilizing a homegrown security solution and managing its own on-premises security information and event management system (SIEM). It was augmenting staff with a third-party provider, primarily to gain 24/7 coverage as opposed to a true managed security service. However, Alliance Data found the management burden of operating the SIEM to be cumbersome, leaving it with less opportunity to focus on more strategic efforts.

After the investment in Deepwatch MDR, Alliance Data has experienced a reduction in the number of anomalous events requiring manual attention, a notable uptick in its security maturity rating from PWC, and the ability to redirect resources to continuous improvement efforts.[1] Key results from the investment include efficiency gains in event response, reduced infrastructure costs, and key personnel freed to refocus on higher priority activities.

> **Flexibility has been one of the biggest differentiators in ultimately choosing Deepwatch — they can react to new and emerging threats or new tools and technologies that we're introducing internally. That and their willingness to work directly with us on a variety of things, so as iron sharpens iron, we can make each other better.**
>
> — Team member, Alliance Data

KEY FINDINGS

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

- **Reduced anomalous event investigation by analysts of up to 86%.** The reduction from an average 28,000 anomalous events per month at the outset of the engagement with Deepwatch MDR to an average 4,000 per month and saved an estimated $6.2 million over three years.
- **Reduced cost of event response by analysts of up to 86%.** As the number of anomalous events decreased, so did the number of events that required escalation for investigation by the security team. The result is a savings of an estimated $1.9 million over three years.
- **Retired legacy system and maintenance costs equivalent to two FTEs.** With Deepwatch MDR, there is no need to manage an on-premises SIEM. This would result in a savings of an estimated $2 million over three years.

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

- **Increased capability maturity model integration (CMMI) rating**
- **Named squad model**
- **Regulatory compliance**
- **Partnership and transparency**
- **Response preparedness**
- **Breadth of experience**

Costs. Risk-adjusted PV costs include:

- **Direct cost of Deepwatch MDR**. The amount of daily data that is analyzed for this customer by Deepwatch MDR has increased from 150 GB to 1 TB over the three-year period, resulting in an estimated cost of $1.9 million over three years.

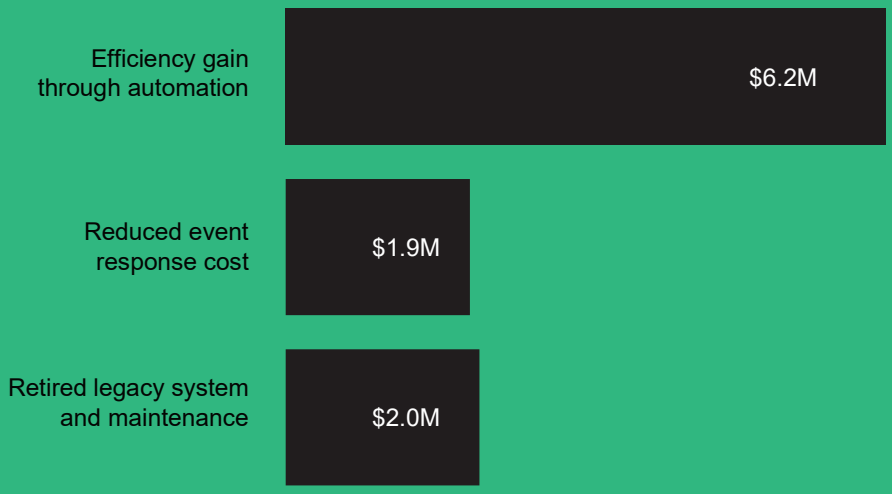
The customer interview and financial analysis found that this customer experiences benefits of $10.1 million over three years versus costs of $1.9 million, adding up to a net present value (NPV) of $8.2 million and an ROI of 432%.

432%
ROI

$10.1 million
BENEFITS PV

$8.2 million
NPV

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 the Deepwatch Managed Detection and Response (MDR).

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 the Deepwatch MDR can have on an organization.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Deepwatch and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the study to determine the appropriateness of an investment in Deepwatch MDR.

Deepwatch 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.

Deepwatch provided the customer name for the interview but did not participate in the interview.

DUE DILIGENCE

Interviewed Deepwatch stakeholders and Forrester analysts to gather data relative to Deepwatch MDR.

CUSTOMER INTERVIEWS

Interviewed decision-makers at an organization using Deepwatch MDR to obtain data with respect to costs, benefits, and risks.

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 organization.

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 Deepwatch Managed Detection and Response Customer Journey

Drivers leading to the Deepwatch MDR investment

INTERVIEWED ORGANIZATION

Forrester interviewed Alliance Data, who is a Deepwatch customer that provides loyalty and marketing services and payment solutions to primarily consumer-based businesses and end customers across a breadth of industries. With two banks to handle the financial aspect of offering branded credit cards, the company is also subject to regulatory and compliance oversight.

KEY CHALLENGES

The customer had an inefficient in-house security system. However, it needed a certain degree of modernization that could meet Alliance Data's needs for a robust security response system in the face of a complex and dynamic threat landscape.

The interviewed organization faced challenges, such as:

- **Lower maturity model rating.** The customer saw an improvement in its maturity rating after the adoption of Deepwatch in its annual NIST assessment.
- **Expensive, complicated SIEM.** Managing an on-premises SIEM was costly and less effective than needed.
  One team member expressed frustration: "At the heart of all of this is the security information and event management system, also known as SIEM. That SIEM is the lifeblood. It's the heart of everything we do, and it's complex and can be difficult to maintain and manage."
- **Suboptimal solutions.** One team member expressed frustration with the time required to simply manage and maintain what was in the end, not a full solution. Rather than devoting resources to the management of a complicated but limited system, the customer wanted to shift those resources to threat intervention innovation.
  The director of Alliance Data explained further, "We were sinking hundreds of man-hours into the administration of a few key security solutions."

Analysis of Benefits

Quantified benefit data

Total Benefits						
Ref	**Benefit**	**Year 1**	**Year 2**	**Year 3**	**TOTAL**	**PRESENT VALUE**
Atr	Efficiency gain through automation	$1,300,000	$2,600,000	$3,800,000	$7,700,000	$6,200,000
Btr	Reduced event response cost	$400,000	$800,000	$1,200,000	$2,400,000	$1,900,000
Ctr	Retired legacy system and maintenance	$700,000	$700,000	$700,000	$2,100,000	$2,000,000
	Total benefits (risk-adjusted)	$2,400,000	$4,100,000	$5,700,000	$12,200,000	$10,100,000

EFFICIENCY GAIN THROUGH AUTOMATION

Evidence and data. At the time Alliance Data first engaged with Deepwatch, they were filtering 150 GB of data per day. At the end of Year 1, that number had increased to 500 GB, and at the end of Year 2, the customer decided to increase the amount of data analyzed to a full terabyte per day. Automation improvements led to a simultaneous reduction in the average anomalous events closed per month from 28,000 to 4,000.

- Alliance Data increased the amount of data filtered from 150 GB per day to 1 TB per day, a 6.5x increase.
- Alliance Data decreased the number of anomalous events from 28,000 to 4,000 per month, a 7x decrease.
- As one team member said, "If you're seeing such a large reduction in security events, it's because of that shared mission and understanding that we're here as a single team to be as efficient and as effective as we can to protect the castle and keep it from harm."

Modeling and Assumptions.

- The reduction in anomalous events decreased by 1,600 every year.
- The cost to respond is $70 per event.

Risks. The efficiency gains through automation may vary due to:

- The amount of data analyzed.
- The number of anomalous events experienced.

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, rounded, risk-adjusted total PV (discounted at 10%) of $6.2 million.

> **"If you're seeing such a large reduction in security events, it's because of that shared mission and understanding that we're here as a single team to be as efficient and as effective as we can to protect the castle and keep it from harm."**
> *— Team member, Alliance Data*

"At the beginning of the relationship with Deepwatch, we were experiencing upwards of 28,000 to 30,000 alerts per month, and we're now down to 4,000. That is an illustration of something that we say all the time, which is, 'we are one team.' There is no 'us' and 'them' when it comes to Deepwatch radius. We are all in it together. And we are all in it to win it. We all accept accountability collectively, and the results speak for themselves."

— Team member, Alliance Data

Efficiency Gain Through Automation

Ref	Metric	Source	Initial	Year 1	Year 2	Year 3
A1	Anomalous events closed by automation	Interview	28,000	20,000	12,000	4,000
A2	Percentage of anomalous events investigated by analysts	Interview	20%	20%	20%	20%
A3	Anomalous events investigated by analysts	A1*A2	5,600	4,000	2,400	800
A4	Reduced number of events per month	A3 Initial-A3	0	1,600	3,200	4,800
A5	Cost per event	Forrester research		$70	$70	$70
At	Efficiency gain through automation	A4*A5*12 months	$0	$1,344,000	$2,688,000	$4,032,000
	Risk adjustment	↓5%				
Atr	Efficiency gain through automation (rounded* and risk-adjusted)		$0	$1,300,000	$2,600,000	$3,800,000
	Three-year total: $7,700,000			**Three-year present value (rounded): $6,200,000**		

*All model table figures have been rounded in addition to adjustment for risks. This is because these modeled dollar values are not precise calculations of actual value, but rather indicative estimations of the value received.

REDUCED EVENT RESPONSE COST

Evidence and data. Once the Deepwatch squad has done the initial review of anomalous events, if necessary, events are escalated to the customer's own team of security analysts. Alliance Data typically sees about 10% of the events each month. As the total number of events that Deepwatch MDR handles on Alliance Data's behalf has fallen, so then has the number of events that Alliance Data reviews. Because these are more unusual events, they take longer to resolve.

The Alliance Data manager said: "With the free cycles that we've inherited by our time savings, now we can focus on advancing the capabilities of our tools so we can make them better. We can look for new use cases that we are not currently using."

Modeling and assumptions.

- The number of events reviewed by the customer's security operations center (SOC) have fallen from 5,600 per month, before engaging Deepwatch MDR, to 800 events in Year 3.
- The response time per incident is 3.8 hours, per the customer interview.
- The fully loaded cost of a security analyst is $140,000 per year.

Risks. The reduced event response cost may vary due to:

- The amount of data filtered.
- The cost of a security analyst.
- The number of anomalous events experienced.

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, rounded, risk-adjusted total PV (discounted at 10%) of $1.9 million.

A really awesome accomplishment that our team delivered, [by] leveraging Deepwatch, was the phishing automation implementation that we did. The net result was a real dollar savings of $650,000 in cost avoidance and productivity gain. We achieved this just by leveraging the core capabilities coupled with working with the Deepwatch team to come together.

— Director, Alliance Data

Reduced Event Response Cost						
Ref	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
B1	Anomalous events investigated by analysts	A3	5,600	4,000	2,400	800
B2	Percentage of anomalous events escalated to security team	Interview	10%	10%	10%	10%
B3	Number of anomalous events escalated to security team	B1*B2	560	400	240	80
B4	Reduced number of events per month	B3 Initial-B3		160	320	480
B5	Response time per event (hours)	Forrester research		3.8	3.8	3.8
B6	Annual hours saved on event response	B4*B5*12 months		7,296	14,592	21,888
B7	Reduced effort per year measured in FTEs	B6/2,080 hours		3.5	7.0	10.5
B8	Cost per security professional	PayScale		$120,000	$120,000	$120,000
Bt	Reduced event response cost	B7*B8	$0	$420,000	$840,000	$1,260,000
	Risk adjustment	↓5%				
Btr	Reduced event response cost (rounded, risk-adjusted)		$0	$400,000	$800,000	$1,200,000
	Three-year total: $2,400,000			**Three-year present value (rounded): $1,900,000**		

RETIRED LEGACY SYSTEM

Evidence and data. The customer had been maintaining their own SIEM.

The director at Alliance Data reported, "We were sinking about 2.5 full-time employees' worth of time just into managing and maintaining our SIEM."

The director also reported, "What we reported in our giveback from a year-over-year budget savings perspective was an annualized savings of more than $500,000 as a result of the transition over to Deepwatch MDR, and that's all from pure opex."

Modeling and assumptions.

- The number of personnel is conservatively held constant at 2.5 over the three-year period.
- The fully loaded cost of a system administrator is $91,000.
- The opex savings are conservatively held constant over the three-year period.

Risks. The savings in retired legacy systems may vary due to:

- The size and complexity of the SIEM.
- The fully loaded cost of a system administrator.

> **"With Deepwatch that two-and-a-half FTEs worth of time dedicated to managing the SIEM was now completely released for us to put them on different projects."**
>
> *— Director, Alliance Data*

Retired Legacy System						
Ref	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
C1	FTEs redirected	Interview	$0	2.5	2.5	2.5
C2	Cost per system administrator	Interview	$0	$91,000	$91,000	$91,000
C3	Reduced operating expense	Interview	$0	$500,000	$500,000	$500,000
Ct	Retired legacy system	(B1*B2)+B3	$0	$727,500	$727,500	$727,500
	Risk adjustment	↓5%				
Ctr	Retired legacy system (rounded, risk-adjusted)		$0	$700,000	$700,000	$700,000
	Three-year total: $2,100,000			**Three-year present value (rounded): $2,000,000**		

UNQUANTIFIED BENEFITS

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

- **Increased CMMI rating.** The freed resources from the reduced anomalous events were able to work on innovation and threat intervention.
  The director at Alliance Data said: "We saw a lift in our overall CMMI equivalent, or cybersecurity framework score, as measured by one of the Big Four accounting firms of over a full point of improvement. Deepwatch was a catalyst for that improvement, and those are the things that matter. Those are the types of artifacts we were able to produce for our external audits, risk analysis, and for our board of directors to demonstrate an ongoing increase, year over year in our ability to protect the castle."
  The manager at Alliance Data said: "Under the NIST [National Institute of Standards and Technology] cybersecurity framework, we saw significant growth in our detect and response scores after being with Deepwatch for only a year."
- **Named squad model.** Deepwatch operates with the squad model, i.e., it has a dedicated group of analysts who work with each customer to develop deep knowledge and expertise in the customer's data and environment.
  The director at Alliance Data said: "When they shared with us that, our analysts would all be the same folks, we valued that. We would work with them day in and day out. It wouldn't be a group of 50 or 60 analysts, and we'd never know who we'd talk with. That was appealing because that meant our Deepwatch analysts get to know our environment. They now understand what normal and abnormal looks like in our world."
- **Regulatory compliance.** As a banking or financial services company, Alliance Data is subject to regulatory oversight and compliance with the FDIC.
  The director at Alliance Data said: "Another piece that was appealing for us being a large financial services organization is that all of these Deepwatch analysts would be stateside. That was appealing for us from a compliance and regulatory perspective because it meant we didn't have to worry about our data leaving the shores. It made compliance a whole lot easier for us."

- **Partnership and transparency.** Alliance Data sought to develop a partnership with a team that would innovate alongside them.
  The manager at Alliance Data said: “Deepwatch was willing to work with us so that we could do things in a very transparent manner. We would both have access to the tools. We could see what they were doing; they could see what we were doing, so that we could truly collaborate and grow together. To us, that was by far the most appealing piece of what Deepwatch was offering.”
- **Response preparedness.** Development in cybersecurity is happening at a fast and furious pace.
  The director at Alliance Data said: “Deepwatch has also proven incredibly beneficial at times when we need to issue responses quickly to understand how vulnerable are to each unique threat actor. Using tools like the SPOT reports, we can quantify what potential exposure we have, if any, for things that are relevant to the business.”
- **Breadth of experience.** Deepwatch works with customers across industries and uses to build its library of use cases.
  The director at Alliance Data said: “As we look across the threat landscape, there are some threat actors that are only, and have only ever been focused on perhaps, supply chain systems or financial services or insurance, and we tend to silo them. When we start to use partners like Deepwatch, where you have a layer of abstraction, and you start to really look at the bits and bytes of who’s doing what, you start to gain a collective level of visibility across their entire ecosystem and the diverse nature of customers that you can’t get in isolation trying to run this thing by yourself.

Analysis Of Costs

Quantified cost data

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Dtr	Fees paid to Deepwatch	$0	$500,000	$800,000	$1,000,000	$2,300,000	$1,900,000
	Total costs	$0	$500,000	$800,000	$1,000,000	$2,300,000	$1,900,000

FEES PAID TO DEEPWATCH

Evidence and data. Deepwatch charges fees based on the amount of data being filtered. Additionally, there is a flat fee for log retention. It should be noted that discrepancies in data analysis by organizations can vary greatly, even for those with similar team sizes or use cases.

Modeling and assumptions.

- Alliance Data increased the amount of data analyzed by Deepwatch from 150 GB per day in Year 1 to 1,000 GB per day in Year 3.
- As more data was analyzed, the fee per gigabyte decreased from $1,600 to $800 per gigabyte.
- A flat fee of $241,000 per year was charged for log retention.

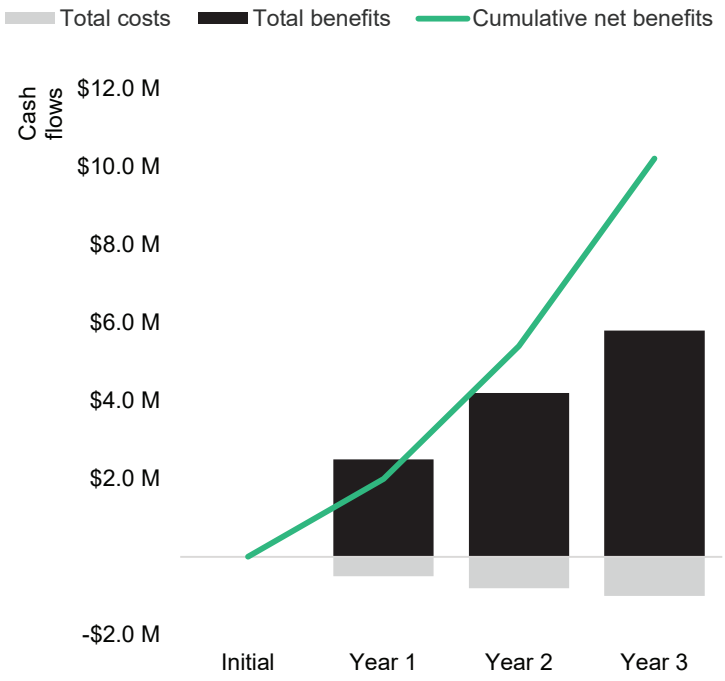
The fees paid to Deepwatch yielded a three-year, rounded, total PV (discounted at 10%) of $1.8 million.

Fees Paid To Deepwatch						
Ref	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
C1	Data filtered per day (GB)	Interview		150	500	1,000
C2	Fee per GB	Interview		$1,600	$1,100	$800
C3	MDR service (log retention)	Interview		$241,000	$241,000	$241,000
Ct	Fees paid to Deepwatch	(C1*C2)+C3	$0	$481,000	$791,000	$1,041,000
	Risk adjustment	0%				
Ctr	Fees paid to Deepwatch (rounded)		$0	$500,000	$800,000	$1,000,000
	Three-year total: $2,300,000			**Three-year present value: $1,900,000**		

Financial Summary

CONSOLIDATED THREE-YEAR RISK ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI, NPV, and payback period values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Analysis (Risk-Adjusted)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	$0	($500,000)	($800,000)	($1,000,000)	($2,300,000)	($1,900,000)
Total benefits	$0	$2,400,000	$4,100,000	$5,700,000	$12,500,000	$10,100,000
Net benefits	$0	$1,900,000	$3,300,000	$4,700,000	$9,900,000	$8,200,000
ROI						432%
Payback period						0 months

Appendix A: Total Economic Impact

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

TOTAL ECONOMIC IMPACT APPROACH

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

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

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

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

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

PRESENT VALUE (PV)

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

NET PRESENT VALUE (NPV)

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

RETURN ON INVESTMENT (ROI)

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

DISCOUNT RATE

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

PAYBACK PERIOD

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

Appendix B: Endnotes

[1]Cybersecurity, Risk & Regulatory, Consulting Solutions

https://www.pwc.com/us/en/services/consulting/cybersecurity-privacy-forensics.html.


FORRESTER®