FORRESTER®

NEW TECH

New Technology: The Projected Total Economic Impact™ Of Microsoft Defender Experts For XDR

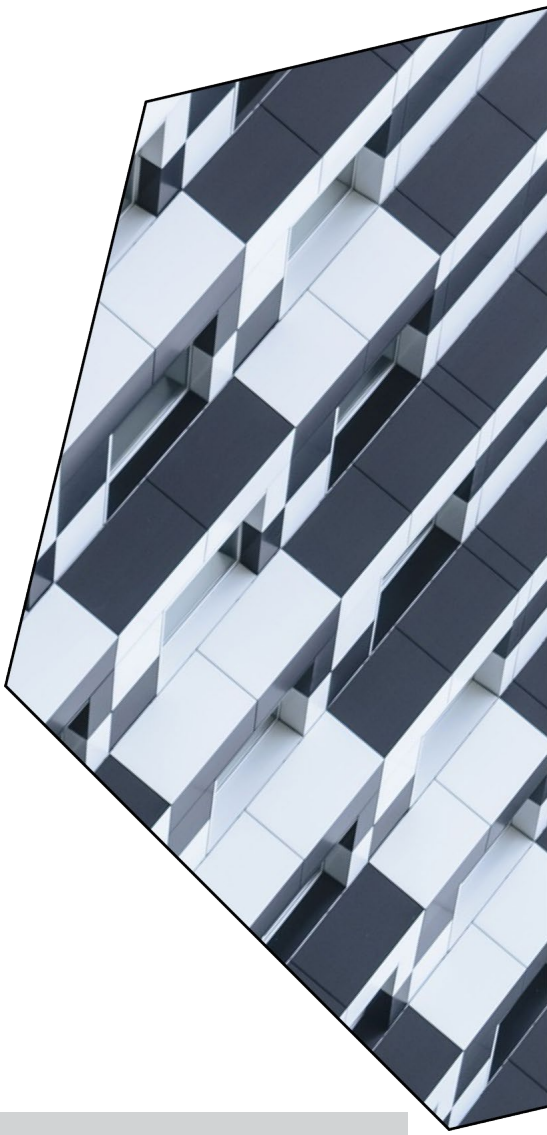
Improved Security Posture, Cost Savings, And Business Benefits Enabled By Defender Experts For XDR

JULY 2023

A FORRESTER NEW TECHNOLOGY PROJECTED TOTAL ECONOMIC IMPACT™ STUDY COMMISSIONED BY MICROSOFT

Table Of Contents

Consulting Team: Sarah Lervold
Jonathan Lipsitz



ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key transformation outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute on their priorities using a unique engagement model that tailors to diverse needs and ensures lasting impact. For more information, visit forrester.com/consulting.

Executive Summary

The rise of cloud adoption and anywhere work, as well as an increase in ransomware attacks, underscore the greater need for security teams to protect their enterprises against increasingly frequent and complex cyberthreats. Yet hiring skilled, around-the-clock IT security talent proves challenging. Microsoft Defender Experts for XDR complements security teams by proactively detecting and guiding incident response through analysts whose visibility and expertise spans many environments at risk of compromise.

The Microsoft Defender Experts for XDR service unites human expertise with automation to investigate Microsoft 365 Defender incidents across endpoints, Office 365, cloud applications and identity. Microsoft Defender Experts for XDR analysts provide security operations teams with actionable guidance to remediate threats and, if granted access, will perform response actions on behalf of an organization. Through proactive extended detection and response, Defender Experts for XDR partners with teams to improve overall security posture without the need to hire additional internal resources.

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

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed seven representatives with experience using Defender Experts for XDR and surveyed 263 respondents with experience using managed detection and response services and at least one Microsoft security product. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the survey results into a single composite organization with 5,000 employees and 15 IT and security professionals who interact with Defender Experts for XDR.

KEY STATISTICS

Projected return on investment (ROI)
43% to 254%

Projected net present value (NPV)
$1.0M to $6.1M

Prior to piloting Defender Experts for XDR, interviewees shared how their organizations responded to security threats in a reactive manner, dedicated thinly resourced teams to manual detection and response activities, and faced integration pains with existing managed service security providers (MSSPs). Interviewees also noted the lack of 24/7 security coverage. These limitations led to increased vulnerability, lengthier incident response times, and delayed response on evenings and weekends. They also required teams to navigate various dashboards to effectively report on their organizations' overall security posture.

After an investment in Defender Experts for XDR, interviewees expected to reduce the likelihood of security breaches and improve their overall security

posture. Interviewees also expected to reduce licensing and professional services costs while eliminating the need for additional IT and security resources. Additional key results from the investment included improving end-user productivity and overall business outcomes from enhanced brand reputation and customer retention.

KEY FINDINGS

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

- **Improved security posture, reducing the likelihood of a breach by up to 20%.** Through earlier and more accurate incident detection, proactive response, and an overall more comprehensive investigation strategy beyond just the traditional endpoint, the composite organization improves its security posture by reducing the likelihood of encountering a material security breach. This is an additional benefit on top of the composite organization's current security measures. The reduction in the likelihood of breaches is worth $261,000 to $522,000 over three years.
- **Reduced license and professional service cost savings up to 100%.** The composite organization realizes value in consolidating vendors and in comanaging its security environment with a team of analysts that built the Defender tooling. This can allow the composite organization to retire its existing managed detection and response (MDR) solution. The reduction in licenses and professional service costs is worth up to $249,000 over three years.
- **Internal IT and security team efficiencies, saving up to 50% additional headcount.** For the composite organization to achieve the same level of security as it achieves with Defender Experts for XDR, it would need to dedicate up to 50% more resources to internal IT and security professionals. The additional headcount avoided is worth up to $2.0 million over three years.
- **Improved business outcomes, including up to a 50% reduction in employee downtime and an incremental operating margin increase up to 3%.** An improved security posture leads to less business user downtime and more time spent on productive work. Additionally, the composite organization realizes an increase in operating margin because of enhanced brand reputation, leading to improvement in customer retention and decreased insurance premiums. Together, these benefits are worth up to $5.7 million over three years.

Additional IT and security team headcount avoided

Up to 50%

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

- **Enhanced talent recruitment and upskilling.** The skills around Microsoft's security stack are more common when compared to competitive vendors, which in turn allows hiring teams to more easily recruit and train professionals. Additionally, the intimate interaction with Defender Experts for XDR analysts upskills internal teams who ask questions of and learn from their peers.
- **Use of human logic alongside automation.** Security operations professionals respect the validation of human logic in their assessments as well as in the open communication channel humans provide. By not strictly relying on an algorithm to investigate, detect, and remediate incidents, cyber incidents are tested through an additional layer of detection.

- **Attentive customer support.** The ability and willingness for Microsoft to directly impact a change (e.g., correct an error or make an improvement) in the Defender stack further enhances security posture.

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

- **License cost.** The license list price is $14 per employee per month.
- **Internal effort.** The internal effort includes a one-week period to configure policies and grant Microsoft access to internal systems, as well as ongoing management activities including meeting with Microsoft to discuss incident activity.

Forrester modeled a range of projected low-, medium-, and high-impact outcomes based on evaluated risk. This financial analysis projects that the composite organization accrues the following three-year net present value (NPV) for each scenario by enabling Microsoft Defender Experts for XDR:

- Projected high impact of a $6.1 million NPV and projected ROI of 254%.
- Projected medium impact of $3.5 million NPV and projected ROI of 147%.
- Projected low impact of a $1.0 million NPV and projected ROI of 43%.

“We’ve gone all in with the Microsoft security tools. We looked at what Defender could give us for endpoint, which allowed alerts related to people and devices together. Then we played with Cloud App security at which point we turned on the identity. We saw how all the data enriches itself in one console. The next step is putting the experts on the ground actually looking at it.”

CIO, legal

NEW TECH TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a New Technology: Projected Total Economic Impact™ (New Tech TEI) framework for those organizations considering an investment in Defender Experts for XDR.

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

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

DUE DILIGENCE

Interviewed Microsoft stakeholders and Forrester analysts to gather data relative to Defender Experts for XDR.

EARLY IMPLEMENTATION INTERVIEWS AND SURVEY

Interviewed seven representatives at organizations using Defender Experts for XDR in a pilot or beta stage and surveyed 263 respondents using managed detection and response (MDR) services and at least one Microsoft Security product to obtain data with respect to projected costs, benefits, and risks.

COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewees and survey respondents.

PROJECTED FINANCIAL MODEL FRAMEWORK

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

CASE STUDY

Employed four fundamental elements of New Tech TEI in modeling the investment's potential 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

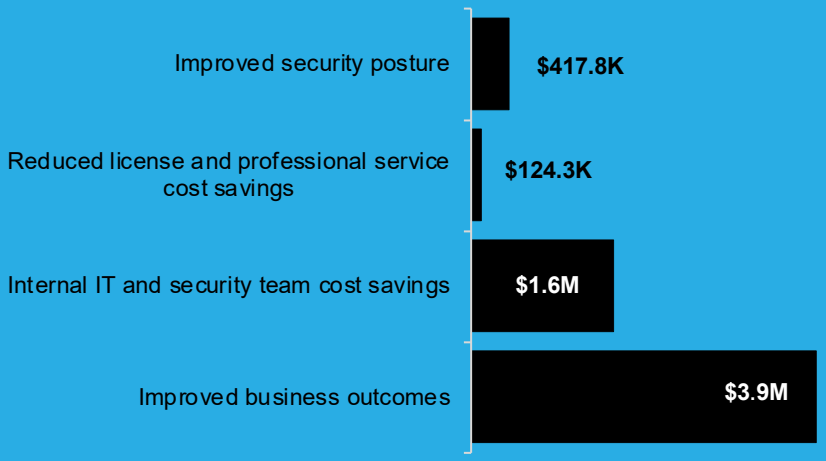
PROI
43% to 254%

PROJECTED BENEFITS PV
$3.4M to $8.5M

PROJECTED NPV
$1.0M to $6.1M

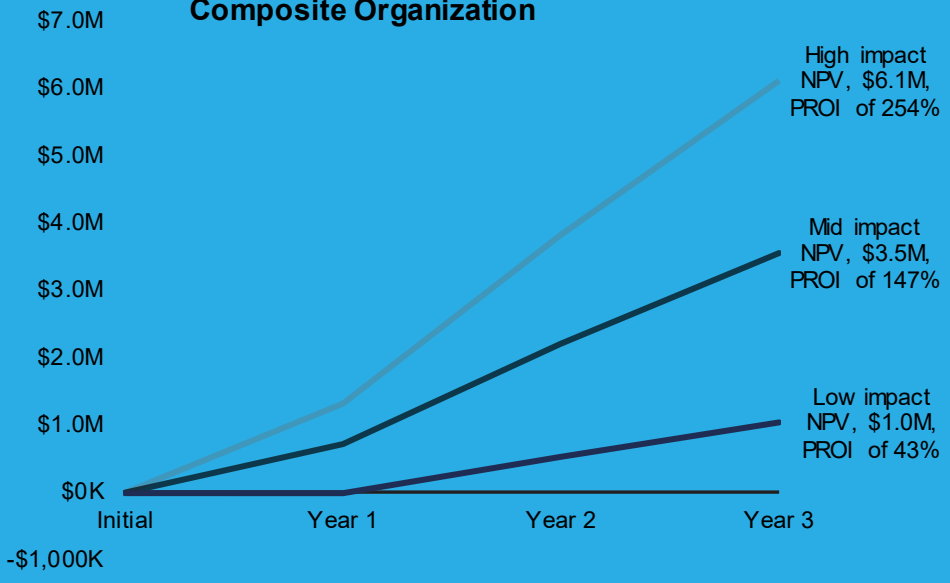
TOTAL COSTS
$2.4M

Projected Benefits (Three-Year)



Figures in chart are projections for the mid-case scenario

Three-Year Projected Financial Analysis For The Composite Organization



The Microsoft Defender Experts For XDR Customer Journey

Drivers leading to the Defender Experts for XDR investment

KEY CHALLENGES

Forrester interviewed seven representatives using Microsoft Defender Experts for XDR and surveyed 263 respondents using managed detection and response (MDR) services and at least one Microsoft security product. For more details on these survey respondents and the organizations they represent, see Appendix B.

Before deploying Defender Experts for XDR, interviewees' organizations investigated and remediated security threats by employing a combination of internal security resources, staff augmentation, and specialized tools from vendors, including MDRs.

In an environment where security threats are increasing in both number and sophistication, interviewees and survey respondents noted how their organizations struggled with common challenges, including the following:

- **Lack of 24/7 security coverage.** Interviewees without a fully staffed internal security team described the need to extend threat detection coverage to after hours and weekends. Without 24/7 resources, the interviewees stressed the urgency at the beginning of each week to sift through outstanding security alerts, acting in a reactive manner to the alerts that required action. Despite their knowledge of this talent gap, interviewees noted the current labor market proves difficult to internally hire skilled security talent to fulfill 24/7 coverage.
- **Internal resources whose time was focused on reactive detection and response activities.** Interviewees described how security resources were strictly reactive in nature to security incidents due to the increasing volume and complexity of incoming threats. This allowed little to no time for proactive threat hunting or for junior-level resources to assess current events more in depth and analyze such incidents.
- **Integration pains with existing managed service provider.** Interviewees reported that prior MSSPs resulted in integration pains due to intricacies in allowing security analysts access to their suite of disparate security tools both in the cloud and on-premises. The time required to configure permission settings accordingly demanded substantial operational overhead each time a new analyst was onboarded. This ultimately delayed the time to operation for detection and response.

> **"The urgency to make sure I'm not missing a threat is suddenly a lot higher than it was a year ago given [recent geopolitical developments]."**
>
> *Principal security analyst, veterinary*

INVESTMENT OBJECTIVES

The interviewees' organizations searched for a solution that could:

- Monitor their security environment 24/7.
- Meet fast SLAs for detection and response at an increasing scale.
- Apply human logic in addition to automation.
- Upskill internal resources to promote proactive — rather than reactive — threat hunting.
- Tap Microsoft's expertise and insight into global account activity and benchmarks.

- Maintain a high level of confidence with clients and auditors from a security standpoint.

COMPOSITE ORGANIZATION

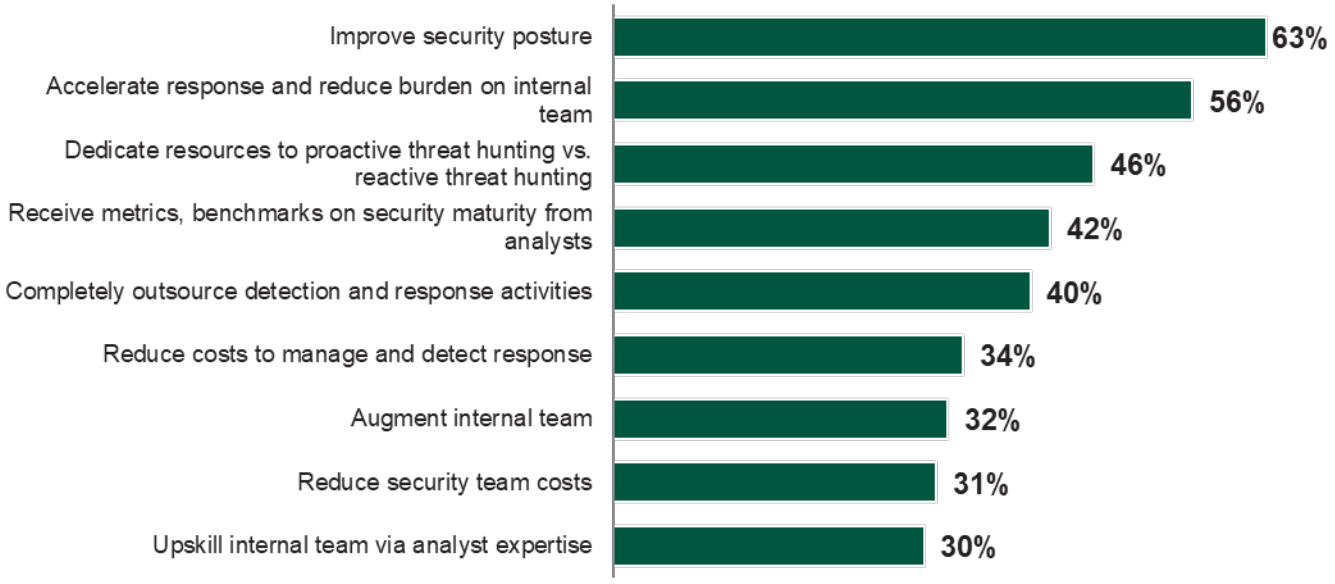
Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of the seven interviewees and 263 survey respondents and has the following characteristics:

Description of composite. The composite organization is a global, business-to-business company with 5,000 full-time workers and annual revenues of $1 billion. It currently employs 15 security and IT professionals that interact with Microsoft Defender Experts for XDR on a regular basis.

Before deploying Defender Experts for XDR, the composite organization invested in a non-Microsoft MDR to address threat detection and response.

Deployment characteristics. The composite organization deploys Defender Experts for XDR across all Microsoft Defenders: endpoints, identities, cloud apps, and email. In Year 1, the composite organization grants Defender Experts for XDR triage and investigation capabilities only, allowing Microsoft to report on threats detected across the composite organization and provide guided response recommendations. In Years 2 and 3, the composite organization grants triage, investigation, and remediation capabilities, allowing Microsoft to take threat remediation action on behalf of the composite organization.

"What goals did your organization hope to address with the implementation of managed detection and response (MDR) service?"



Base: 263 users of managed detection and response (MDR) services, using at least one Microsoft Security product
Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, April 2023

Key Assumptions

- **5,000 employees**
- **$1B revenue**
- **15 IT and security professionals using Defender Experts for XDR**
- **Year 1: Triage and investigation capabilities**
- **Year 2 and Year 3: Triage, investigation, and remediation capabilities**

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Projected Benefits					
Benefit	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Total projected benefits (low)	$955,500	$1,630,500	$1,630,500	$4,216,500	$3,441,176
Total projected benefits (mid)	$1,752,500	$2,765,000	$2,765,000	$7,282,500	$5,955,691
Total projected benefits (high)	$2,425,000	$4,000,000	$4,000,000	$10,425,000	$8,515,589

IMPROVED SECURITY POSTURE

Evidence and data. Interviewees shared that deploying Defender Experts for XDR would improve their organizations' security either as a result of earlier detection compared to their previous vendor solution or from the ability to proactively identify alerts otherwise undetected from thinly resourced internal staff. Because Microsoft receives security-related telemetry from so many companies around the world using Microsoft products, the Defender Experts for XDR analysts have unique access to data and insights into emerging threats and vulnerabilities. This enhances Defender Experts for XDR's ability to detect and remediate threats. Interviewees and survey respondents illustrated the following examples of how their security postures have improved during early implementation:

- The principal security analyst at the veterinary organization said: "Last fiscal year, we recorded 19 breaches in the tenancy that Defender Experts for XDR are monitoring now. We are on track to see approximately 14 breaches in the same calendar duration for this year. Given the volume of alerts processed by the system, confidence is fairly high that this is a direct result of the service."

  The principal security analyst also shared an example of an endpoint exposure to the internet for remote desktop access that resulted in multiple low and medium alerts that the organization's internal team was not resourced enough to investigate.

- The director of information technology at the legal organization added, "Comparing Defender Experts for XDR with our prior solution, Microsoft is much better at getting real alerts versus false positives, at least twice as good."

- The CIO at the same legal organization stated their cybersecurity risk score is 9.6 out of 10:

> **"I see a benefit in correlation. For example, if an incident happens and a machine is infected with malware and credentials are stolen, then you see the login with those credentials from a location that is unfamiliar. Microsoft has all the data in one place, which is easier for us to correlate the whole picture."**
>
> *Incident response team lead, travel*

"Microsoft has a much more global view of account activity, traversing the globe and ensuring my account doesn't become compromised. Whereas our prior vendor was focused on investigating current activities such as downloading a malicious file."

CIO, legal

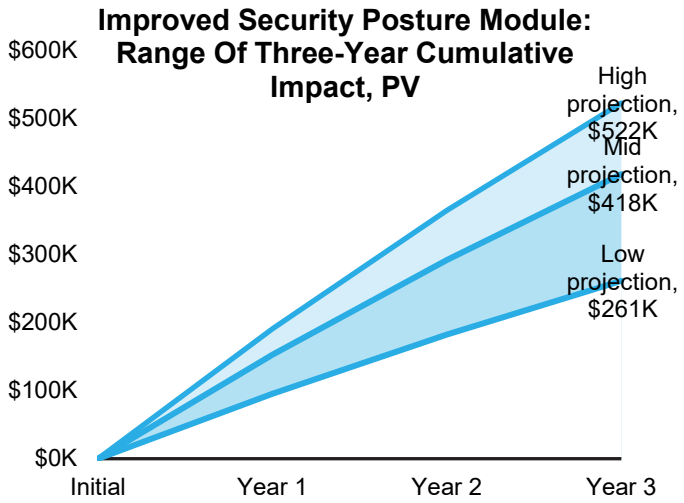
"Microsoft impacts that score. If we were to do it ourselves, I don't think we'd get seven or eight. Microsoft is a huge part of that score."

- The CIO also said that compared to their previous vendor, the organization has realized 5 hours of savings in mean time to detect (MTTD) from the ability of Defender Experts for XDR to detect threat instances earlier.
- Survey respondents reported an average of a 16% decrease in risk of a breach since implementing an MDR service.
- Survey respondents whose organizations are a similar size to the composite reported an average annual total cost of a breach before implementing an MDR service of $322,776.
- The survey also found a 16% decrease in MTTD security breaches and a 17% decrease in mean time to recover (MTTR) from security breaches for organizations using an MDR service.

Modeling and assumptions. For the financial analysis as applied to the composite organization, Forrester assumes:

- Before Defender Experts for XDR, the composite experiences an annual average of three material security breaches.[2]
- Each security breach costs an average of $350,000.[3] The breach is responded to fully in-house and includes response and notification to affected parties, regulatory fines, audit and security compliance costs, and customer compensation.
- In the low-impact scenario, the composite reduces the likelihood of a breach by 10%, which is an additional reduction to the risk of a breach the composite realizes from its current managed service provider.
- In the mid-impact scenario, the composite reduces the likelihood of a breach by 16%, which is an additional reduction to the risk of a breach the composite realizes from its current managed service provider.
- In the high-impact scenario, the composite reduces the likelihood of a breach by 20%, which is an additional reduction to the risk of a breach the composite realizes from its current managed service provider.

Results. This yields a three-year projected PV ranging from $261,000 (low) to $522,000 (high).



Improved Security Posture					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Average annual number of security breaches before Defender Experts for XDR	Forrester research	3	3	3
A2	Average cost of a breach	Survey	$350,000	$350,000	$350,000
$A3_{Low}$	Reduced likelihood of a breach with Defender Experts for XDR	Composite	10%	10%	10%
$A3_{Mid}$			16%	16%	16%
$A3_{High}$			20%	20%	20%
At_{Low}	**Improved security posture**	**A1*A2*A3**	**$105,000**	**$105,000**	**$105,000**
At_{Mid}			**$168,000**	**$168,000**	**$168,000**
At_{High}			**$210,000**	**$210,000**	**$210,000**
Three-year projected total: $315,000 to $630,000		**Three-year projected present value: $261,119 to $522,239**			

REDUCED LICENSE AND PROFESSIONAL SERVICE COST SAVINGS

Evidence and data. Interviewees unanimously shared that Microsoft played an important role as a provider of tools in their security stack and explained the benefit of a consolidated technology stack under one vendor. Some interviewees anticipated a complete replacement of their previous MDR vendor solution while others assumed a portion of the licenses would not be replaced for personal preferences or because the solution provided functionality not included in Defender Experts for XDR's scope. Interviewees and survey respondents illustrated the following examples of how each expects to rationalize their external costs dedicated to threat detection and response:

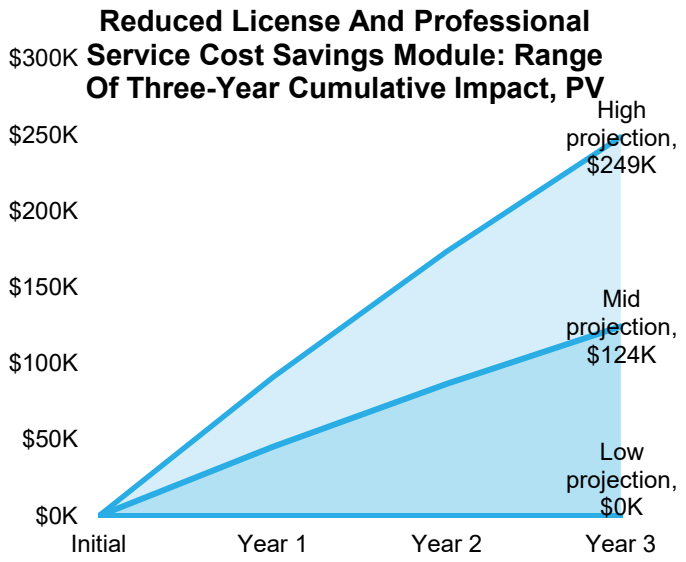
- The director of information technology at the legal organization said: "One of our goals is to consolidate vendors. We don't like to pay for two vendors. We would rather work with a vendor to make them understand our vertical and provide a product that is truly tailored. Microsoft would be a replacement for our product."
- The CIO and director of information technology expected to retire $105,000 in MDR-related solutions comparable to the Defender Experts for XDR offering if fully replaced.
- The director of security operations and response at the travel organization reported using two separate MSSPs. If the interviewee's organization decided to deploy Defender Experts for XDR across the organization, it would retire $100,000 in license cost from one of the MSSPs and leave the second solution in place.
- Survey respondents reported an average annual cost savings from retiring subscription licenses of $75,000 after implementing an MDR service.
- Survey respondents also reported a 17% decrease in professional service costs each year since implementing an MDR service.

Modeling and assumptions. For the financial analysis as applied to the composite organization, Forrester assumes:

- Before Defender Experts for XDR, the composite invests in a MDR service which costs $100,000 annually.

- In the low-impact scenario, the composite organization retains all costs of its current MDR service.
- In the mid-impact scenario, the composite organization retires 50% of its current MDR service.
- In the high-impact scenario, the composite organization retires 100% of its current MDR service.

Results. This yields a three-year projected PV ranging from $0 (low) to $249,000 (high).



Reduced License And Professional Service Cost Savings

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	License and professional service cost eliminated from retired MDR vendor solution	Composite	$100,000	$100,000	$100,000
$B2_{Low}$			0%	0%	0%
$B2_{Mid}$	Annual savings with Defender Experts for XDR	Composite	50%	50%	50%
$B2_{High}$			100%	100%	100%
Bt_{Low}			**$0**	**$0**	**$0**
Bt_{Mid}	**Reduced license and professional service cost savings**	**B1*B2**	**$50,000**	**$50,000**	**$50,000**
Bt_{High}			**$100,000**	**$100,000**	**$100,000**
Three-year projected total: $0 to $300,000		**Three-year projected present value: $0 to $248,685**			

INTERNAL IT AND SECURITY TEAM COST SAVINGS

Evidence and data. In addition to saving on external costs, interviewees shared how Defender Experts for XDR would save the need to hire additional IT and security professionals to service around-the-clock coverage. Full deployment of the service would also allow internal staff to dedicate their time to customer-facing issues and more strategic level tasks. Interviewees and survey respondents illustrated the following examples of internal IT and security team cost savings during early implementation:

- The director of security operations and response at the travel organization said: “This service is working 24/7. We don’t have the headcount to support the organization 24/7.” The interviewee continued that the organization would need to hire three times the staff to meet the 24/7 objective of Defender Experts for XDR.
- The principal security analyst at the veterinary organization shared an example of a recent particularly busy three-day weekend holiday, “Three days of no service and having the knowledge if anything major happened, Microsoft would have emailed me, which takes a couple hours of workload off my team.”
- The principal security analyst continued, “I would love to build an in-house SOC [security operations center], but I have no confidence I would be able to recruit enough people.”
- The CIO and the director of information technology at the legal organization shared the need to hire three additional team members, including a chief information security officer (CISO), to reach a level equivalent to Defender Experts for XDR. This equates to a 37.5% increase in staff.
- The CIO and director of information technology also shared that compared to their prior MDR solution, they expected to save 75% on investigation and remediation with Defender Experts for XDR.
- Survey respondents found that time available to spend on nonsecurity-related activities increased by 20% for IT teams since implementing an MDR service.
- The survey also reported 42% fewer FTE hours needed amongst the security team and a 49% decrease in help desk tickets received per month after implementing an MDR service.

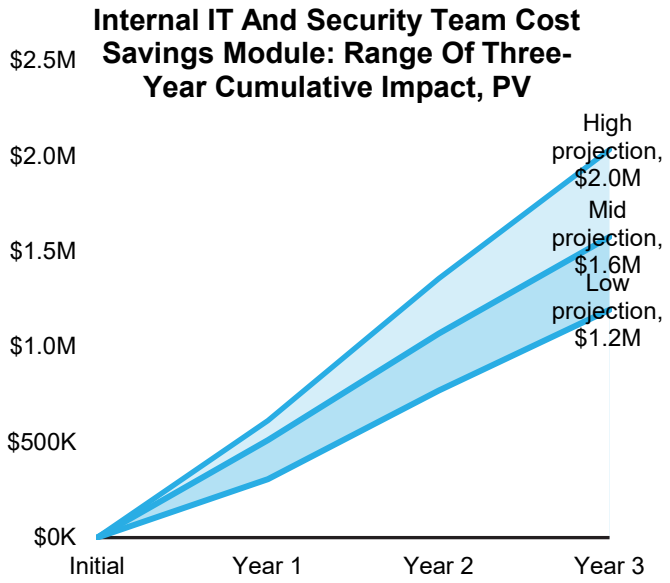
Modeling and assumptions. For the financial analysis as applied to the composite organization, Forrester assumes:

- There are 15 FTEs on IT and security teams that interact with Defender Experts for XDR.
- The average fully burdened cost across the IT and security teams is $150,000. This salary assumes a mid-level professional with a few years of security-related experience and includes salary, benefits, and payroll taxes.

> **“My target state is to have my internal security team to be on hand for escalations and let the managed service take care of not just the detection but also first line containment actions. If somebody needs to reach out to the customer, that would be where we could escalate the internal security team.”**
>
> *Principal security analyst, veterinary*

- Forrester applies a 75% productivity capture rate. The remaining time saved is allocated to nonwork activities.
- In the low-impact scenario, without Defender Experts for XDR, the team size would need to increase by 20% in Year 1 to provide the same level of threat detection service to the organization. In Years 2 and 3, the team size would need to increase to 30% to accommodate the additional responsibility of remediation that would have been covered by Microsoft.
- In the mid-impact scenario, without Defender Experts for XDR, the team size would need to increase by 30% in Year 1 to provide the same level of threat detection service to the organization. In Years 2 and 3, the team size would need to increase to 40% to accommodate the additional responsibility of remediation that would have been covered by Microsoft.
- In the high-impact scenario, without Defender Experts for XDR, the team size would need to increase by 40% in Year 1 to provide the same level of threat detection service to the organization. In Years 2 and 3, the team size would need to increase to 50% to accommodate the additional responsibility of remediation that would have been covered by Microsoft.

Results. This yields a three-year projected PV ranging from $1.2 million (low) to $2.0 million (high).



Internal IT And Security Team Cost Savings

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Affected IT and security teams FTEs	Composite	15	15	15
$C2_{Low}$	Avoided headcount addition with Defender Experts for XDR	Y1: C1*20% Y2 and Y3: C1*30%	3	5	5
$C2_{Mid}$		Y1: C1*30% Y2 and Y3:C1*40%	5	6	6
$C2_{High}$		Y1: C1*40% Y2 and Y3:C1*50%	6	8	8
C3	Annual fully burdened cost	TEI standard	$150,000	$150,000	$150,000
C4	Productivity capture	TEI standard	75%	75%	75%
Ct_{Low}	**Internal IT and security team cost savings**	**C2*C3*C4**	**$337,500**	**$562,500**	**$562,500**
Ct_{Mid}			**$562,500**	**$675,000**	**$675,000**
Ct_{High}			**$675,000**	**$900,000**	**$900,000**
Three-year projected total: $1,462,500 to $2,475,000			**Three-year projected present value: $1,194,309 to $2,033,621**		

IMPROVED BUSINESS OUTCOMES

Evidence and data. An enhanced security posture has further impact on end-user productivity, brand reputation, customer retention, and time to market. Together, these benefits advance an organization's ability to conduct and expand business outcomes. Interviewees and survey respondents illustrated the following examples of improved business outcomes during early implementation:

- The CIO at the legal organization said, "The brand reputation will really have a tremendous impact on our operations." This included the ability to tie third-party risk scores to business development. The interviewee continued: "There is a direct impact to our insurance premium. We're able to keep it low because of nondirect threats or exposures."
- The CIO also stated a 35% to 40% reduction in end-user downtime related to events that impacted their lawyers.
- The cybersecurity operations manager at the manufacturing organization said, "If we can say we've got Microsoft hunting in our environment, this might carry weight with auditors and help with our cybersecurity insurance." This interviewee also noted how their joint ventures may benefit from an investment in Defender Experts for XDR.

"Microsoft is giving us enough leverage to compete against a larger competitor in the market without losing a lot of sleep or investing a lot of money into cybersecurity."

CIO, legal

"Ninety percent of our data is coming from our clients. The future of what we do as a practice will be based on how secure we can protect our client's data."

CIO, legal

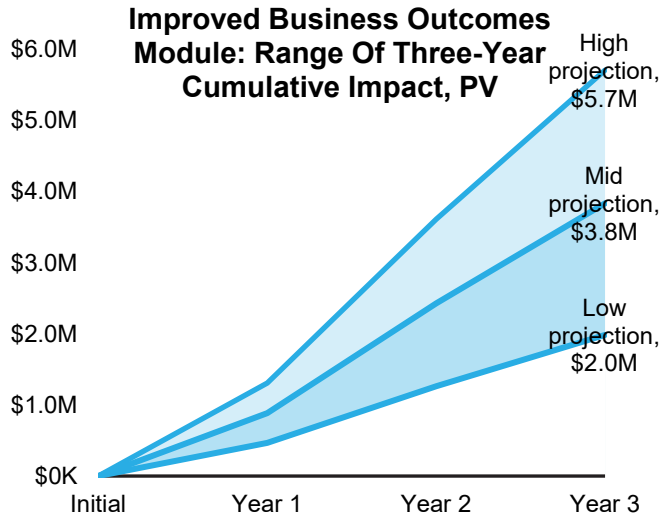
- Survey respondents reported 222 hours annually in time savings per non-IT employee and 15% decrease in employee downtime annually since implementing an MDR service.
- The survey also found that annual revenue increased by 4% annually, citing 20% in customer retention and 34% faster time to market for new products.

Modeling and assumptions. For the financial analysis as applied to the composite organization, Forrester assumes:

- Prior to Defender Experts for XDR, the composite experiences 3 hours of downtime related to material security incidents annually.
- In the low-impact scenario, employees save 35% of hours impacted by downtime annually.
- In the mid-impact scenario, employees save 40% of hours impacted by downtime annually.
- In the high-impact scenario, employees save 50% of hours impacted by downtime annually.

- The fully burdened average hourly cost of an employee is $40.
- Forrester assumes 60% of employees are impacted by downtime related to a material security breach.
- Forrester applies a 50% productivity capture rate. The remaining time saved is reallocated to nonwork activities.
- The composite has an operating margin of 9%.
- In the low-impact scenario, the composite realizes a 0.5% increase in incremental operating profit in Year 1 and a 1.0% increase in Years 2 and 3.
- In the mid-impact scenario, the composite realizes a 1.0% increase in incremental operating profit in Year 1 and a 2.0% increase in Years 2 and 3.
- In the high-impact scenario, the composite realizes a 1.5% increase in operating profit in Year 1 and a 3.0% in Years 2 and 3.

Results. This yields a three-year projected PV ranging from $2.0 million (low) to $5.7 million (high).



Improved Business Outcomes

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Employee downtime prior to Defender Experts for XDR (hours)	Composite	3	3	3
$D2_{Low}$			35%	35%	35%
$D2_{Mid}$	Annual time savings per employee (hours)	Composite	40%	40%	40%
$D2_{High}$			50%	50%	50%
D3	Average fully burdened hourly cost	TEI standard	$40	$40	$40
D4	Productivity capture	TEI standard	50%	50%	50%
D5	Employee headcount	Composite	5,000	5,000	5,000
D6	Affected employees	Composite	60%	60%	60%
$D7_{Low}$			$63,000	$63,000	$63,000
$D7_{Mid}$	Subtotal: Increased end-user productivity	D1*D2*D3*D4*D5*D6	$72,000	$72,000	$72,000
$D7_{High}$			$90,000	$90,000	$90,000
D8	Annual revenue	Composite	$1,000,000,000	$1,000,000,000	$1,000,000,000
D9	Operating margin	Composite	9%	9%	9%
D10	Operating profit	Composite	90,000,000	90,000,000	90,000,000
$D11_{Low}$			0.5%	1.0%	1.0%
$D11_{Mid}$	Incremental margin increases with Defender Experts for XDR	Composite	1.0%	2.0%	2.0%
$D11_{High}$			1.5%	3.0%	3.0%
$D12_{Low}$			$450,000	$900,000	$900,000
$D12_{Mid}$	Subtotal: Incremental profit increase	D10*D11	$900,000	$1,800,000	$1,800,000
$D12_{High}$			$1,350,000	$2,700,000	$2,700,000
Dt_{Low}			**$513,000**	**$963,000**	**$963,000**
Dt_{Mid}	**Improved business outcomes**	**D7+D12**	**$972,000**	**$1,872,000**	**$1,872,000**
Dt_{High}			**$1,440,000**	**$2,790,000**	**$2,790,000**
Three-year projected total: $2,439,000 to $7,020,000			**Three-year projected present value: $1,985,748 to $5,711,044**		

UNQUANTIFIED BENEFITS

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

- **Enhanced talent recruitment and upskilling.** Interviewees noted that it is easier to attract talent that has knowledge of the Microsoft Defender stack, as compared to other MDR vendors, given its global presence and prevalence. In a similar vein, deepening the relationship and frequency of conversation with Microsoft upskills employees. The CIO at a legal organization noted: "Security engineers and other specialists are learning from their counterparts at Microsoft. There's a real person on the other side."
- **Use of human logic alongside automation.** Interviewees stressed how, with Defender Experts for XDR, their organizations appreciated the idea of a comanaged detection and response environment. It was important for the interviewees' organizations to be reassured that humans were a part of their threat hunting environment. The cybersecurity operations manager at the manufacturing organization said: "Some of the other vendors are very big into AI and machine learning. Microsoft is applying human logic and I respect this." The interviewee continued, "Other services are staffed so light the only way they're doing it is pumping through a script or algorithm whereas Microsoft is chipping through a brutal volume."
- **Attentive customer support.** Interviewees recognized the advantage of receiving support from the team that built the tools in the Defender stack. Microsoft's ability to identify and directly influence an improvement to the tool (e.g., a false positive) was appreciated. The cybersecurity manager at the manufacturing organization said: "Our service delivery manager is phenomenal. They've got us thinking in terms of how the tool would work. They bring analysts to the table. It's beneficial to talk to the people doing the hunts or triaging the alerts."

"This kind of service is from the vendor that is responsible for most of your tooling. You get an expertise that does not exist in the market. If there is a false positive, they can fix it on the fly."

Director of security operations and response, travel

FLEXIBILITY

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

- **Enhancements to reporting and insights.** Interviewees shared anticipation for more advanced reporting capabilities displayed in a dashboard format rather than reporting via email. This step in the product roadmap will allow organizations to effectively keep track of live metrics and slice the data to share findings with leadership.
- **Learning from peer organizations.** Microsoft's depth of work across organizations in varying industries and geographies opens opportunity for peer-based groups to learn security-related findings from one another. Interviewees noted examples like sharing use cases, hunting rules, and hunting queries. Ultimately, Microsoft's managed service can foster continued collaboration for organizations that hold a

common mission: to keep their business secure. As the cybersecurity operations manager at the manufacturing organization stated, “This type of world is too real, too stressful, too intimate.”

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

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Etr	License cost	$0	$882,000	$882,000	$882,000	$2,646,000	$2,193,403
Ftr	Internal effort	$8,640	$82,500	$82,500	$82,500	$256,140	$213,805
	Total costs (risk-adjusted)	$8,640	$964,500	$964,500	$964,500	$2,902,140	$2,407,208

LICENSE COST

Evidence and data. Interviewees were not aware of pricing for the Defender Experts for XDR service. Microsoft has since announced the list price, which is based on a license fee per user per month.

Modeling and assumptions. For the financial analysis as applied to the composite organization, Forrester assumes:

- The composite organization pays Microsoft's list price of $14 per user per month.
- Licenses are granted to all 5,000 employees.
- Pricing may vary. The reader is encouraged to speak with Microsoft for additional pricing options.

Risks. The size of this cost can vary because of:

- The overall size of the organization.
- Any negotiated discounts on licenses.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $2.2 million.

License Cost						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Number of licenses	Composite		5,000	5,000	5,000
E2	Defender Experts for XDR license cost	$14/month*12 months		$168	$168	$168
Et	License cost	E1*E2		$840,000	$840,000	$840,000
	Risk adjustment	↑5%				
Etr	License cost (risk-adjusted)		$0	$882,000	$882,000	$882,000
Three-year total: $2,646,000			**Three-year present value: $2,196,403**			

INTERNAL EFFORT

Evidence and data. Interviewees said they anticipate little difficulty on the technical side to fully deploy Defender Experts for XDR across their organization. The upfront effort would entail granting access to the Microsoft team, training Microsoft on any specific organizational tooling, and configuring telemetry.

- The cybersecurity manager at the manufacturing organization shared regarding early implementation: "The onboarding was very simple; they have a prerequisite guide. There was very little from our end we had to change." The interviewee estimated a one-hour meeting to complete the prerequisite guide and maintained biweekly touchpoints with the Microsoft team for ongoing management.
- The director of information technology at the legal organization indicated that implementation involved three engineers over 30 days. No additional professional services were required.

Modeling and assumptions. For the financial analysis as applied to the composite organization, Forrester assumes:

- The initial implementation lasts one week and requires three FTEs.
- Ongoing solution management requires 0.5 FTEs for maintenance of the platform and meetings with Microsoft.
- The average fully burdened cost across the IT and security teams is $150,000.

Risks. The size of this cost can vary because of:

- The size of deployment based on organization size and the prior solutions replaced.
- The average fully burdened cost of these resources.

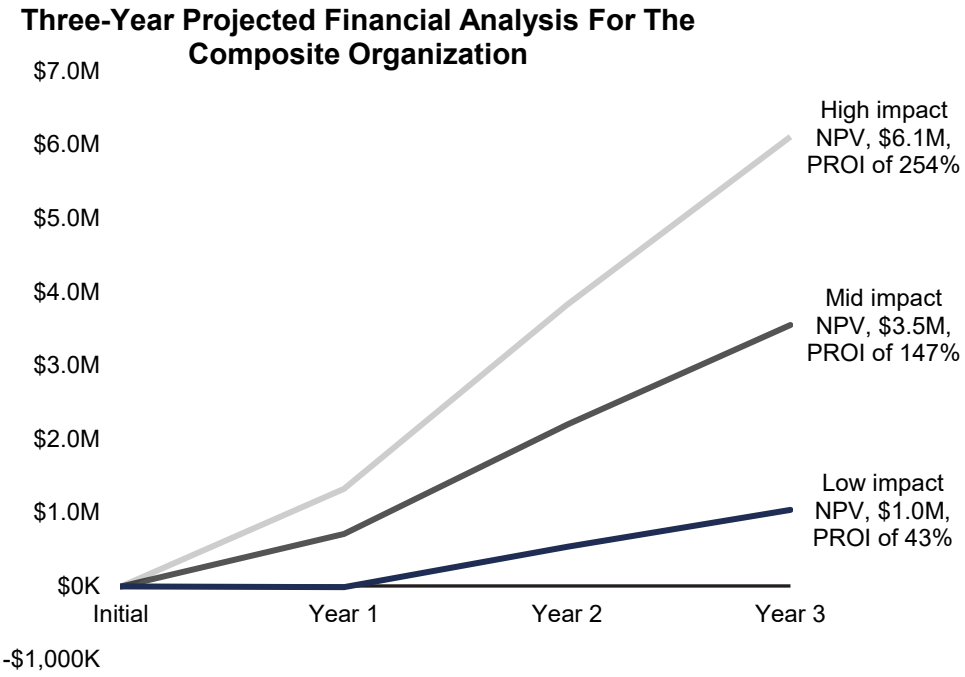
Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $213,000.

Internal Effort

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Implementation	3 FTEs*C3/2,080*40 hours	$8,640			
F2	Ongoing management	0.5 FTE*C3		$75,000	$75,000	$75,000
Ft	Internal effort	F1+F2	$8,640	$75,000	$75,000	$75,000
	Risk adjustment	↑10%				
Ftr	Internal effort (risk-adjusted)		$8,640	$82,500	$82,500	$82,500
	Three-year total: $256,140			**Three-year present value: $213,805**		

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS



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

These risk-adjusted PROI and projected NPV 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	($8,640)	($964,500)	($964,500)	($964,500)	($2,902,140)	($2,407,208)
Total benefits (low)	$0	$955,500	$1,630,500	$1,630,500	$4,216,500	$3,441,176
Total benefits (mid)	$0	$1,752,500	$2,765,000	$2,765,000	$7,282,500	$5,955,691
Total benefits (high)	$0	$2,425,000	$4,000,000	$4,000,000	$10,425,000	$8,515,589
Net benefits (low)	($8,640)	($9,000)	$666,000	$666,000	$1,314,360	$1,033,968
Net benefits (mid)	($8,640)	$788,000	$1,800,500	$1,800,500	$4,380,360	$3,548,483
Net benefits (high)	($8,640)	$1,460,500	$3,035,500	$3,035,500	$7,522,860	$6,108,381
PROI (low)						43%
PROI (mid)						147%
PROI (high)						254%

Appendix A: New Technology: Projected Total Economic Impact

New Technology: Projected Total Economic Impact (New Tech TEI) is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value of their products and services to clients. The New Tech TEI methodology helps companies demonstrate and justify the projected tangible value of IT initiatives to senior management and key business stakeholders.

TOTAL ECONOMIC IMPACT APPROACH

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

Projected Costs consider all expenses necessary to deliver the proposed value of the product. The projected cost category within New Tech TEI captures incremental ongoing costs over the existing environment that are 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.

PROJECTED NET PRESENT VALUE (PNPV)

The projected 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.

PROJECTED RETURN ON INVESTMENT (PROI)

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

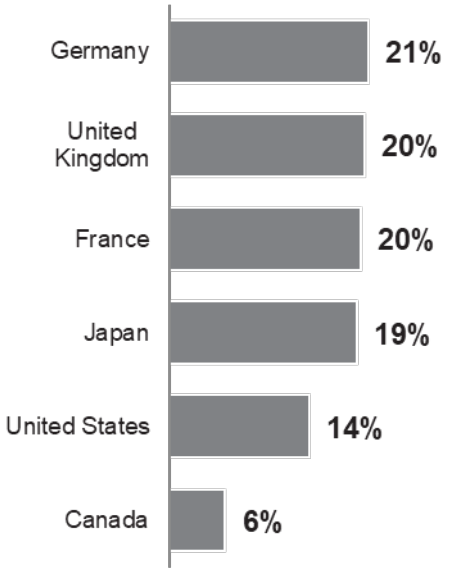
DISCOUNT RATE

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%.

Appendix B: Interviewees And Survey Demographics

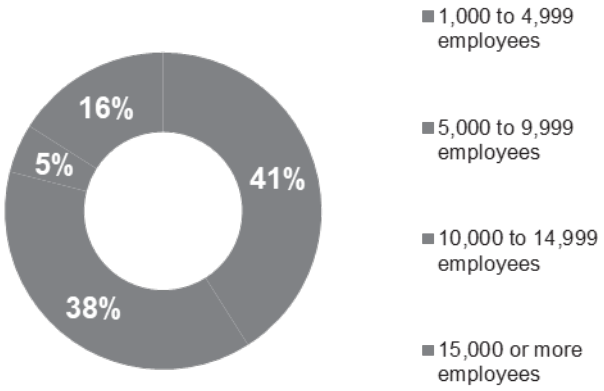
Interviews			
Role	**Industry**	**Region**	**Employees**
CIO	Legal	United States	300
Director of information technology	Legal	United States	300
Cybersecurity manager	Manufacturing	Global, US HQ	36,000
Cybersecurity operations manager	Manufacturing	Global, US HQ	36,000
Director of security operations and response	Travel	Global, Singapore HQ	8,000
Incident response team lead	Travel	Global, Singapore HQ	8,000
Principal security analyst	Veterinary	Global, UK HQ	28,000

"In which country are you located?"



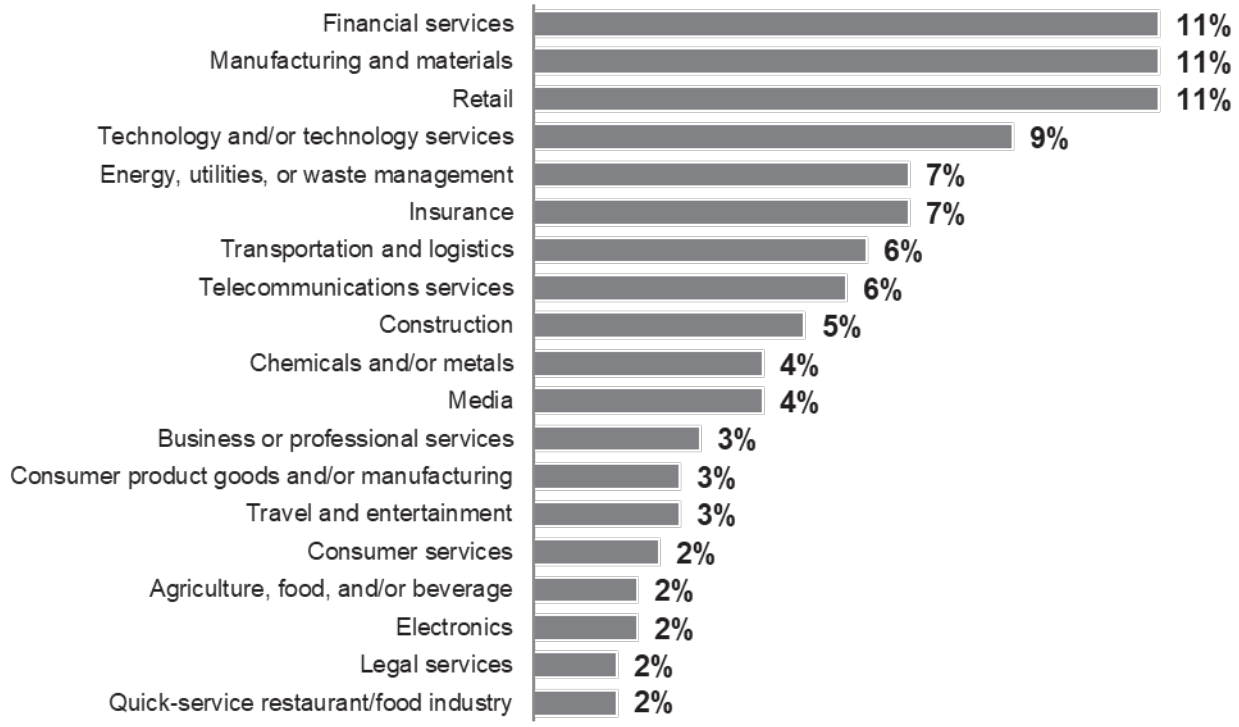
Base: 263 users of managed detection and response (MDR) services, using at least one Microsoft Security product
Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, April 2023

"Using your best estimate, how many employees work for your firm/organization worldwide?"



Base: 263 users of managed detection and response (MDR) services, using at least one Microsoft Security product
Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, April 2023

"Which of the following best describes the industry to which your company belongs?"



Base: 263 users of managed detection and response (MDR) services, using at least one Microsoft Security product
Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, April 2023

Appendix C: Endnotes

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

[2] Source: Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q1 2021.

[3] Base: 66 users of managed detection and response (MDR) services, using at least one Microsoft Security product; Source: A commissioned study conducted by Forrester Consulting, April 2023


FORRESTER®