FORRESTER®

# The Total Economic Impact™ Of Microsoft Defender Experts For Hunting

**September 2023**

## Introduction

Microsoft Defender Experts for Hunting is Microsoft's managed threat hunting service that augments a company's in-house security operations center (SOC) capabilities. It combines human and AI-based proactive threat hunting and analysis, and it includes Defender Experts notifications within Microsoft 365 Defender, Experts on Demand service, and detailed reporting. Defender Experts for Hunting analyzes signals across Microsoft Defender for Identity, Microsoft Defender for Endpoints, Microsoft Defender for Cloud Apps, Microsoft Entra AD, and Microsoft Defender for Office 365 (email and data).

Microsoft commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the return on investment (ROI) enterprises may realize by deploying Defender Experts for Hunting.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Defender Experts for Hunting on their organizations. Microsoft Defender Experts for Hunting is both a stand-alone service offering and a component of Defender Experts for XDR. Additional information regarding the detection-related benefits from Defender Experts for Hunting and the expanded Defender Experts for XDR benefits can be found in the original Defender Experts for XDR TEI study.[2]

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed six representatives from three organizations with experience using Defender Experts for Hunting (either as a stand-alone tool or as part of Defender Experts for XDR) and surveyed 263 respondents with experience using managed detection and response services and at least one Microsoft security product.

Return on investment (ROI)
**96%**

Net present value (NPV)
**$449K**

Interviewees included:

- The CIO and the director of information technology at a large US law firm.
- The cybersecurity manager and the cybersecurity operations manager at a global manufacturer.
- The director of security operations and response and the incident response team lead at a global travel company.

Prior to using Defender Experts for Hunting, interviewees shared how their detection activities were very manual and sometimes failed to identify complex, multivector threats. They also said that the

> **"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*

mean time to detect (MTTD) was often too long. These limitations led to increased vulnerabilities and lengthier incident response times.

### INVESTMENT DRIVERS

The interviewees' organizations searched for a solution that could:

- Monitor their security environment 24/7.
- Meet fast SLAs for detection 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 threats and how to respond.

### 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 six interviewees and 263 survey respondents and has the following characteristics:

The composite organization is a global B2B company with 5,000 full-time workers and an annual revenue of $1 billion. In an IT organization of 100 employees, there are 15 FTEs who are heavily involved in IT security. They represent a mix of representatives from the security team and IT teams such as networking. Out of this group, five FTEs spend a part of their time on threat hunting and interact with Microsoft Defender Experts for Hunting on a regular basis to better understand identified threats and how to improve the organization's overall security posture.

## Benefits

### BENEFIT 1: IMPROVED SECURITY POSTURE

**Evidence and data.** Interviewees shared that deploying Defender Experts for Hunting improved their organizations' security because of faster MTTD compared to their previous external solutions or thinly resourced internal staff. Interviewees also said that the Defender Experts for Hunting analysts had unique access to data and insights into emerging threats and vulnerabilities because Microsoft analyzes trillions of security signals from their worldwide ecosystem of products and services every day. This means the Microsoft teams found vulnerabilities that would otherwise be missed. The following examples of improved security posture were shared:

- The director of information technology at the legal firm said, "Microsoft is much better at getting real alerts versus false positives, at least twice as good."
- The CIO at the same legal firm estimated that its MTTD has improved by 5 hours. They also estimated that upwards of 85% of the total security posture improvement realized with Defender Experts for XDR was attributable to the threat hunting component that makes up Defender Experts for Hunting. Additionally, Microsoft gave them "response instructions on how to remediate a threat."
- The cybersecurity manager at the manufacturer said, "Microsoft picked up false positives very fast, often faster than we could."
- The incident response team lead at the travel company said, "Threat hunting can be a thankless job, but an important one." They also shared that Microsoft found a leftover file on a server from a red-team hunting activity six months prior. The existing team and tools had not detected it.
- Interviewees also benefited from regular conversations and interactions with Microsoft's threat hunters as part of the Experts on Demand service that is included in the Defender Experts for Hunting offering. The director of information technology at the law firm explained that

Microsoft's team helped theirs understand how to configure Exchange to improve security while minimizing false positives and noise.

- Survey respondents reported an average 16% reduction in the risk of a breach after adopting a managed detection and response (MDR) service.
- Survey respondents also reported a 16% reduction in MTTD and a 15% reduction in false positives.

> **"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*

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

- Before Defender Experts for Hunting, the composite experiences an annual average of three material breaches.[3]
- Each security breach costs the organization an average of $350,000.[4] The breach is responded to by in-house staff and includes response and notification to affected parties, regulatory fines, audit and security compliance costs, and customer compensation.
- The composite organization reduces the likelihood of a breach by 17% in Year 1. This is 85% of the total 20% reduction achieved with both external detection and remediation services included in the Defender Experts for XDR TEI study.[5] The reduced likelihood of a breach improves 20% per year as Defender Experts for Hunting improves and the IT team becomes better at implementing the recommendations.

**Risk and result.** The size of this benefit can vary based on how good and fast an organization previously was at threat hunting. To account for this risk, Forrester adjusted this benefit down by 5%, yielding a three-year, risk adjusted total PV (discounted at 5%) of $505,800.

**Improved Security Posture**

| Ref. | Metric | Source | Year 1 | Year 2 | Year 3 |
|---|---|---|---|---|---|
| A1 | Average annual number of security breaches before Defender Experts for Hunting | Forrester research | 3 | 3 | 3 |
| A2 | Average cost of a breach | Survey | $350,000 | $350,000 | $350,000 |
| A3 | Reduced likelihood of a breach with Defender Experts for Hunting | Composite | 17.0% | 20.4% | 24.5% |
| At | Improved security and compliance posture | A1*A2*A3 | $178,500 | $214,200 | $257,040 |
| | Risk adjustment | ↓5% | | | |
| Atr | Improved security and compliance posture (risk-adjusted) | | $169,575 | $203,490 | $244,188 |
| | **Three-year total: $617,253** | | | **Three-year present value: $505,795** | |

## BENEFIT 2: INTERNAL IT AND SECURITY TEAM COST SAVINGS

**Evidence and data.** In addition to improving security posture, Defender Experts for Hunting helped the interviewees' and respondents' organizations achieve better security with less effort. This freed up previously overworked IT security professionals to focus on other activities and to more quickly remediate threats using the recommendations and instructions provided by Defender Experts for Hunting. Examples of how teams became more efficient included:

- The director of information technology at the law firm explained that his team previously spent too much time analyzing logs and telemetry. Much of the time was spent analyzing false and benign alerts. Across the team, the team saved 10% of its time with Defender Experts for Hunting.
- The CIO at the same organization said, "The number and complexity of alerts will definitely go up over the next year as bad actors increase their use of generative AI." Without Defender Experts for Hunting, the team would struggle to keep up with the additional workload.
- The cyber security operations manager at the manufacturer said, "Analysts can save a fair amount of time."
- The survey found a 36% decrease in hours spent on event detection.

> **"Defender Experts for Hunting saves us 40 hours per month across a team of three people."**
>
> *Director of information technology, legal*

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

- Across the IT and security teams, there are five FTEs engaged in threat hunting activities. Prior to Defender Experts for Hunting, they spent one-third of their time on threat hunting activities.
- The time spent on threat hunting is reduced by 36% in Year 1. The time savings improves 20% per year in line with the organization's improved security posture.
- The average fully burdened cost of these FTEs, including salary, benefits, and payroll taxes, is $150,000. There are 2,080 working hours in a year.
- Forrester applies a 90% productivity capture rate. The remaining time saved is allocated to nonwork activities.

**Risk and result.** The size of this benefit can vary based on the team size and level of experience as well as their fully burdened cost. To account for this risk, Forrester adjusted this benefit down by 5%, yielding a three-year, risk adjusted total PV of $229,500.

| Internal IT And Security Team Cost Savings | | | | | |
|---|---|---|---|---|---|
| **Ref.** | **Metric** | **Source** | **Year 1** | **Year 2** | **Year 3** |
| B1 | IT and security teams FTEs engaged in threat hunting | Composite | 5.0 | 5.0 | 5.0 |
| B2 | Time previously spent on threat hunting (hours) | B1*52 weeks*40 hours*1/3 | 3,467 | 3,467 | 3,467 |
| B3 | Hunting activity time savings (hours) | B2*36% (improving 20% per year) | 1,248 | 1,498 | 1,797 |
| B4 | Hourly fully burdened cost | $150,000/2,080 hours | $72.12 | $72.12 | $72.12 |
| B5 | Productivity capture | TEI standard | 90% | 90% | 90% |
| Bt | Internal IT and security team cost savings | B3*B4*B5 | $81,005 | $97,206 | $116,647 |
| | Risk adjustment | ↓5% | | | |
| Btr | Internal IT and security team cost savings (risk-adjusted) | | $76,955 | $92,346 | $110,815 |
| | **Three-year total:$280,116** | | **Three-year present value: $229,535** | | |

**BENEFIT 3: IMPROVED BUSINESS OUTCOMES FROM END-USER PRODUCTIVITY**

**Evidence and data.** For the interviewees' and survey respondents' organizations, an enhanced security posture from better and faster detections, along with clear guidance on how to remediate the threats, resulted in fewer breaches and less downtime for business users. Less downtime meant employees could create more value for an organization. Interviewees and survey respondents shared how Defender Experts for Hunting contributed to less downtime:

- The CIO at the law firm estimated that every 10-minute reduction in detection time is worth $16,000 in lawyer billables. They also estimated that, between the threat detection capabilities of Defender Experts for Hunting and the remediation capabilities of Defender Experts for XDR, there was a 35% to 40% reduction in end-user downtime for lawyers.
- Survey respondents reported 222 hours annually in time savings per non-IT employee and a 15% decrease in employee downtime annually since implementing an MDR service.

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

- Prior to Defender Experts for Hunting, the composite experiences 3 hours of annual downtime related to material security incidents.
- Three-quarters of the overall 50% reduction in end-user downtime realized from implementing Defender Experts for XDR is attributable to Defender Experts for Hunting's improved threat detection and its remediation recommendations. The reduction in downtime improves 20% per year along with the overall improved security posture.
- The fully burdened average hourly cost of an employee is $40.
- Forrester assumes that 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.

**Risk and result.** The size of this benefit can vary based on the amount of previous downtime and the

fully burdened cost of business users. To account for this risk, Forrester adjusted this benefit down by 10%, yielding a three-year, risk adjusted total PV of $181,200.

| Improved Business Outcomes From End-User Productivity | | | | | |
|---|---|---|---|---|---|
| **Ref.** | **Metric** | **Source** | **Year 1** | **Year 2** | **Year 3** |
| C1 | Employee downtime prior to Defender Experts for Hunting (hours) | Composite | 3 | 3 | 3 |
| C2 | Annual time savings per employee (hours) | Composite | 37.5% | 45.0% | 54.0% |
| C3 | Average fully burdened hourly cost | TEI standard | $40 | $40 | $40 |
| C4 | Productivity capture | TEI standard | 50% | 50% | 50% |
| C5 | Employee headcount | Composite | 5,000 | 5,000 | 5,000 |
| C6 | Affected employees | Composite | 60% | 60% | 60% |
| Ct | Improved business outcomes from end-user productivity | C1*C2*C3*C4*C5*C6 | $67,500 | $81,000 | $97,200 |
| | Risk adjustment | ↓10% | | | |
| Ctr | Improved business outcomes from end-user productivity (risk-adjusted) | | $60,750 | $72,900 | $87,480 |
| | **Three-year total: $221,130** | | **Three-year present value: $181,200** | | |

## UNQUANTIFIED BENEFITS AND FLEXIBILITY

Interviewees mentioned the following additional benefits that their organizations experienced but were not able to quantify, or that may be realized in the future:

- **Upgrading to Defender Experts for XDR.** Interviewees' organizations that utilized Defender Experts for Hunting may be able to expand their services agreements so that Microsoft does some or all of the managed response and remediation work. This can deliver additional benefits, which were explored in the full Defender Experts for XDR TEI study.
- **Enhanced talent recruitment and upskilling.** Interviewees noted that it was easier to attract talent that had knowledge of the Microsoft Defender stack, as compared to other security vendors, because of its global presence and prevalence. In a similar vein, organizations that deepened the relationship and frequency of conversation with Microsoft saw upskilling in 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 their organizations appreciated the idea of a comanaged detection 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."
- **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.

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement Defender Experts for Hunting and later realize some of the above-mentioned additional uses and business opportunities. None of these future opportunities were included in the financial analysis.

# Costs

### COST 1: LICENSE COSTS

**Evidence and data.** The list price for Defender Experts for Hunting is $3 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 $3 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.

**Risk and result.** No risk adjustment was made because the list price is used. The three-year total PV is $447,600.

**License Costs**

| Ref. | Metric | Source | Year 1 | Year 2 | Year 3 |
|---|---|---|---|---|---|
| D1 | Number of licenses | Composite | 5,000 | 5,000 | 5,000 |
| D2 | Annual license cost | $3/month*12 | $36 | $36 | $36 |
| Dt | License costs | D1*D2 | $180,000 | $180,000 | $180,000 |
| | Risk adjustment | 0% | | | |
| Dtr | License costs (risk-adjusted) | | $180,000 | $180,000 | $180,000 |
| | **Three-year total: $540,000** | | | **Three-year present value: $447,633** | |

### COST 2: INTERNAL EFFORT

**Evidence and data.** Interviewees said there was little effort on the technical side to fully deploy Defender Experts for Hunting across their organizations. The upfront effort entailed turning on Defender Experts for Hunting and configuring telemetry. Similarly, ongoing management effort was very low.

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

- The initial effort to go live 16 hours to understand how the service works, reporting, etc.
- Ongoing effort outside of threat hunting requires 8 hours per month. This time is spent on modifying and adding new telemetry and using the Experts on Demand service to improve security and the use of Defender Experts for Hunting.
- The average fully burdened cost across the IT and Security teams is $150,000.

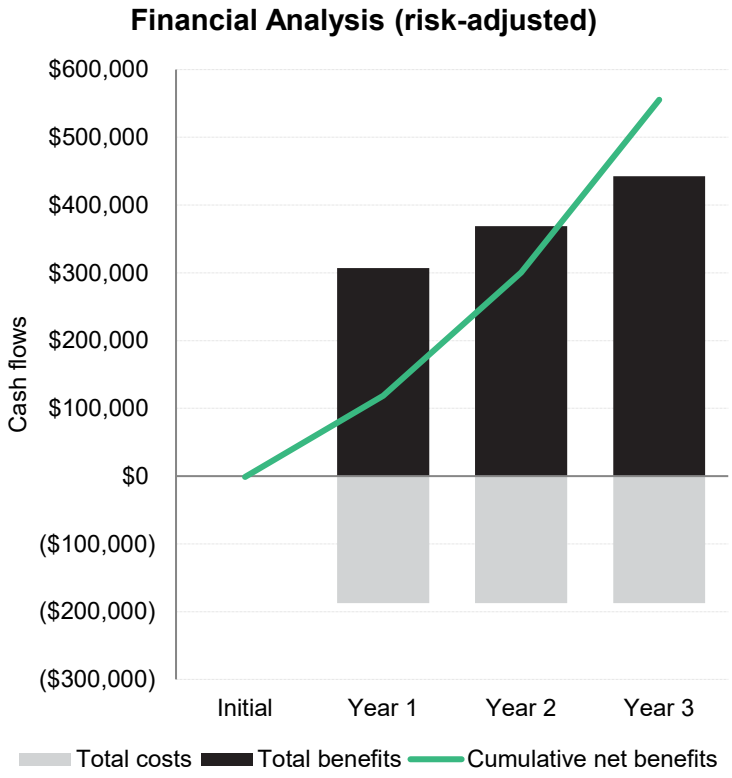
**Risk and result.** The size of this cost can vary based on the size of the organization and the average fully burdened cost of these resources. To account for this risk, Forrester adjusted this cost up by 5%, yielding a three-year, risk adjusted total PV of $19,300.

**Internal Effort**

| Ref. | Metric | Source | Initial | Year 1 | Year 2 | Year 3 |
|---|---|---|---|---|---|---|
| E1 | Implementation | B4*16 hours | $1,154 | | | |
| E2 | Ongoing management | B4*96 hours | | $6,923 | $6,923 | $6,923 |
| Et | Internal effort | E1+E2 | $1,154 | $6,923 | $6,923 | $6,923 |
| | Risk adjustment | ↑5% | | | | |
| Etr | Internal effort (risk-adjusted) | | $1,212 | $7,269 | $7,269 | $7,269 |
| | **Three-year total: $23,019** | | | **Three-year present value: $19,289** | | |

# Financial Summary

## CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS




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

**These risk-adjusted ROI and 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 | ($1,212) | ($187,269) | ($187,269) | ($187,269) | ($563,019) | ($466,922) |
| Total benefits | $0 | $307,280 | $368,736 | $442,483 | $1,118,499 | $916,530 |
| Net benefits | ($1,212) | $120,011 | $181,467 | $255,214 | $555,480 | $449,608 |
| ROI | | | | | | 96% |

## Appendix A: 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: "New Technology: The Projected Total Economic Impact Of Microsoft Defender Experts for XDR," a commissioned study conducted by Forrester Consulting on behalf of Microsoft, July 2023.

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

[4] 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

[5] Source: "New Technology: The Projected Total Economic Impact Of Microsoft Defender Experts for XDR," a commissioned study conducted by Forrester Consulting on behalf of Microsoft, July 2023.


FORRESTER®