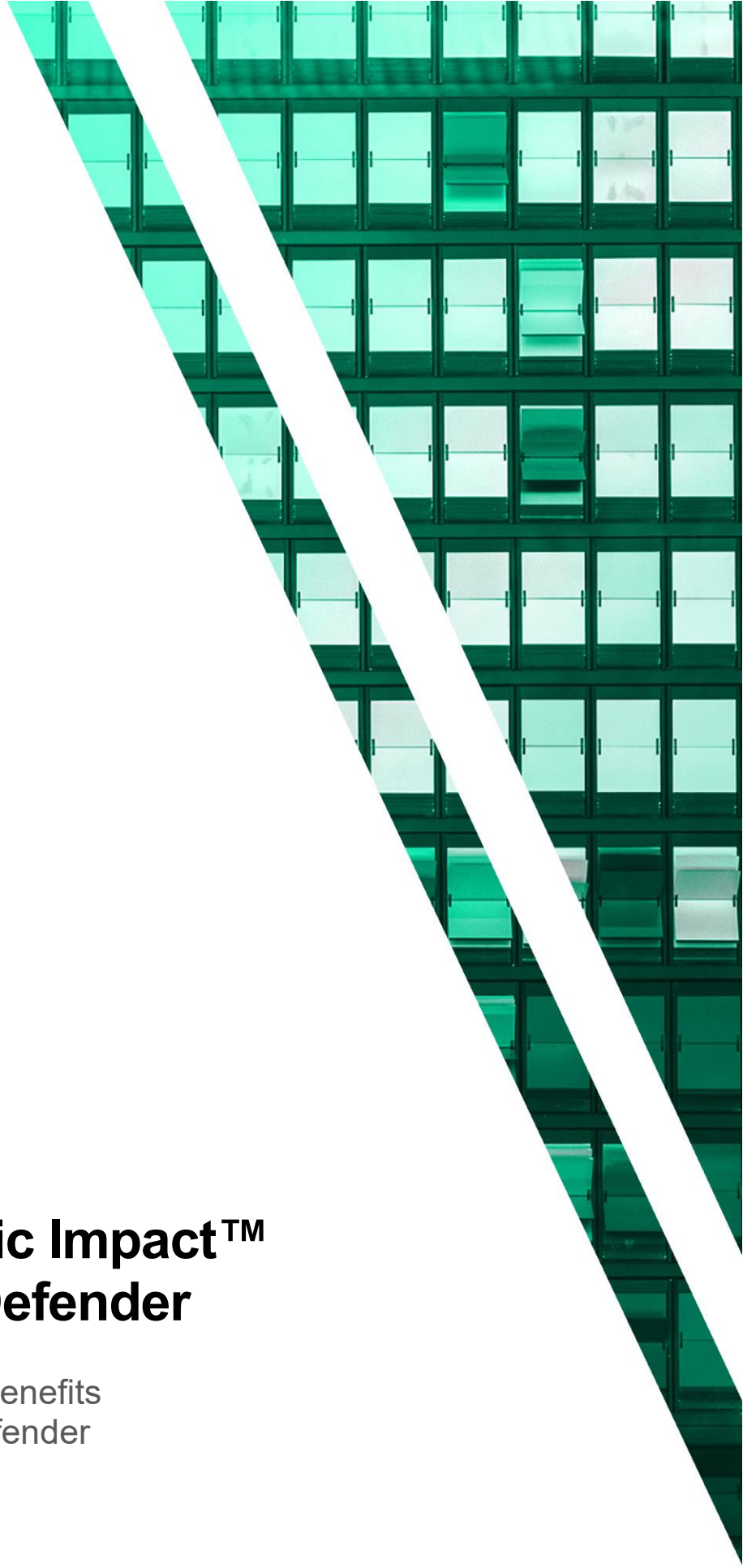
FORRESTER®



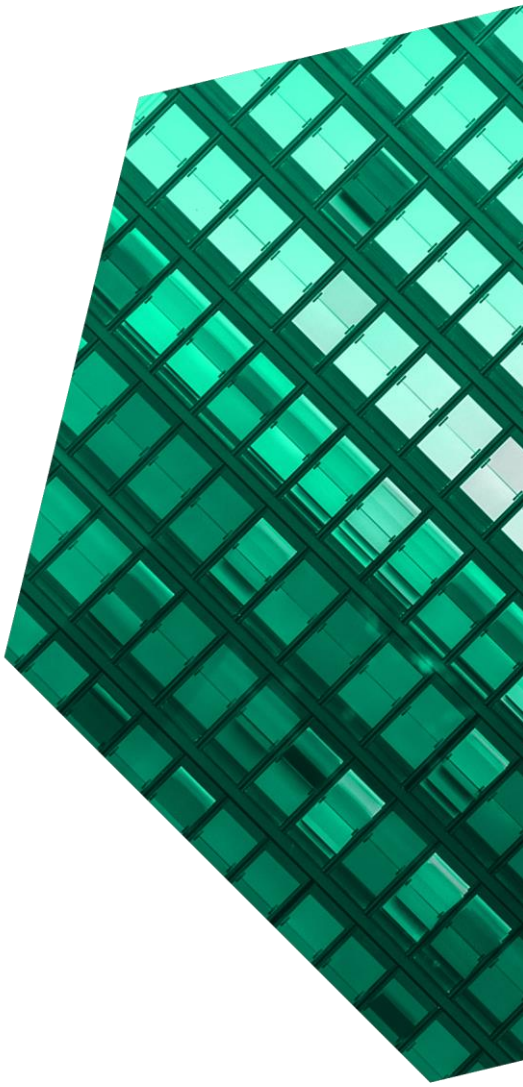
The Total Economic Impact™ Of Microsoft 365 Defender

Cost Savings And Business Benefits Enabled By Microsoft 365 Defender

APRIL 2022

Table Of Contents

Consulting Lead *Kim Finnerty*



Executive Summary

The modern enterprise faces a greater volume and complexity of security challenges than ever before. Microsoft 365 Defender empowers security teams to spend less time investigating and more time acting on proactive security. It combines data from endpoints, identities, applications, email and multiple platforms to highlight cross-platform incidents, automatically address issues, enable advanced hunting, and provide team members with common data to promote more effective collaboration.

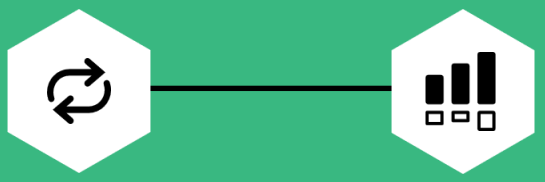
Microsoft 365 Defender protects end-user environments using XDR technology. It uses AI to combine signals from endpoints, identities, applications, data, email and more to automatically analyze threats across domains and build a complete picture of each attack in a single dashboard. As a result, security professionals can easily focus on the most critical threats and hunt for sophisticated attempts to breach defenses.

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 Microsoft 365 Defender.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Microsoft 365 Defender on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed five decision-makers at four organizations with experience using Microsoft 365 Defender. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization.

Prior to using Microsoft 365 Defender, these interviewees noted that their security teams spent much of their time investigating a deluge of security alerts, rather than using their expertise on activities such as hunting and other proactive security measures.

KEY STATISTICS



Return on investment (ROI)
242%

Net present value (NPV)
$17.11M

After the investment in Microsoft 365 Defender, the interviewees found their organizations reduced successful attacks and recovered more quickly from them. Key results from the investment also included enhanced productivity for the security team and the whole organization, as well as reduced investments in the security stack due to rationalization of tools from multiple vendors.

KEY FINDINGS

Quantified benefits. Risk-adjusted present value (PV) quantified benefits over the three years of the financial model include:

- **Increased security team automation and process improvements added $6.0 million to the bottom line.** Interviewees described several ways in which Microsoft 365 Defender improved their teams' efficiency. A single-pane-of-glass security dashboard, common search language,

> **You don't know what you don't know. Microsoft does so much AI behind the scenes. It makes discovery so much easier.**
>
> — Head of global monitoring and alerting, energy

data normalization, correlation of alerts to highlight cross-platform incidents, and autohealing of many incidents all combined to allow analysts the time to put their skills to better use for the organizations.

- **Added automation and process improvements delivered $10.5 million in end-user productivity.** Native integration with Microsoft's widely used productivity, communication, and other applications meant that security teams did not need to physically remove devices to prevent or remediate incidents, so they could address potential security issues without impacting end users' ability to continue working on their devices.
- **Reduced cost of risk due to security breaches avoided over $2.1 million in losses.** Security teams became more proactive in their approach to threats, particularly with the adoption of advanced hunting. This, in conjunction with autohealing and cross-domain visibility, resulted in a more secure environment and lowered the risk of loss from a security breach.
- **Reduced cost of risk due to faster incident response time saved $2.9 million in losses.** Interviewees noted that, when security incidents did happen, Microsoft 365 Defender greatly sped up their ability to find and address the problem. Because alerts were correlated across platforms and analysts did not need to jump from one portal to another, interviewees reported that response times were cut in half with Microsoft 365 Defender.
- **Enhanced IT administration and deployment saved over $1.7 million.** With fewer agents to deploy and maintain, faster provisioning, and

Security analyst time redeployed:

75%

fewer ticketed issues to resolve, Microsoft 365 Defender also improved IT team productivity.

- **Implemented vendor consolidation to save over $1.0 million.** Deploying Microsoft 365 Defender not only allowed participating organizations to terminate their subscriptions to several point solutions, but also freed up the time of those employees charged with monitoring and maintaining them.

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

- **Improved relationships/coordination between security and IT teams.** Interviewees reported that security and IT teams worked together more seamlessly with Microsoft 365 Defender because security was integrated with the operating system (OS) that the technical team knew so well. The deployment also made the IT team's work much easier, as they only had to deal with one familiar solution, rather than several.
- **A more empowered, satisfied security team.** By removing the majority of low value-added tasks analysts need to deal with and freeing them up to use their unique skills on preventing incidents and improving security, Microsoft 365 Defender contributed to a more satisfied workforce.
- **A proactive rather than reactive approach to security.** Interviewees reported that Microsoft 365 Defender gave their analysts the time and information to use their skills in a more proactive approach to security.

Costs. Risk-adjusted PV costs over the three-year period of the model include:

- **Microsoft fees of $6.9 million secured E5 security licenses for workers.** These licenses covered all fees related to Microsoft 365 Defender.
- **Initial deployment costs totaled $25,000.** Deployment was quite simple for these organizations, requiring very little technical intervention (and no professional or third-party services), and training only for the security team.
- **Ongoing administration cost the organization $66,000.** Interviewed executives stated that a minimal level of oversight was required to maintain the solution for their organizations.

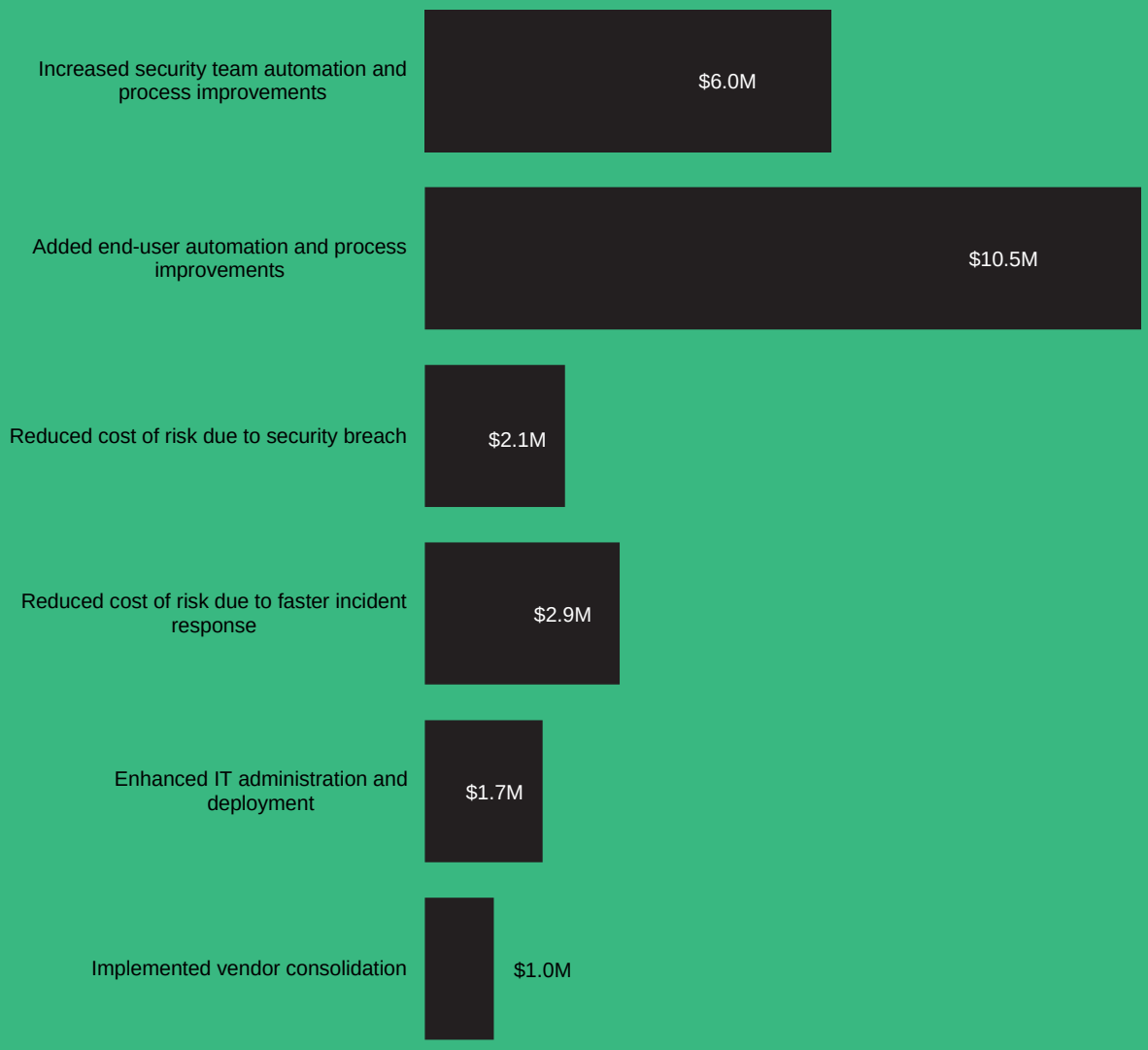
The decision-maker interviews and financial analysis found that a composite organization experiences benefits of $24.17 million over three years versus costs of $7.06 million, adding up to a net present value (NPV) of $17.11 million and an ROI of 242%.

ROI
242%

BENEFITS PV
$24.17M

NPV
$17.11M

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 Microsoft 365 Defender.

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 Microsoft 365 Defender 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 Microsoft 365 Defender.

DECISION-MAKER INTERVIEWS

Interviewed five decision-makers at four organizations using Microsoft 365 Defender to obtain data on costs, benefits, and risks.

COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewees' organizations.

FINANCIAL MODEL FRAMEWORK

Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the decision-makers.

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 Microsoft 365 Defender Customer Journey

Drivers leading to the Microsoft 365 Defender investment

Interviewed Decision-Makers

Interviewee	Industry	Region	Revenues
Cybersecurity operations manager	Manufacturing	Global	$38.5 billion
Manager, cyberthreat and operations	Energy	APAC	$935 million
Lead, security operations	Energy	APAC	$935 million
Senior director, information security	Insurance	Global	$8.5 billion
Head of global monitoring and alerting	Energy	EMEA	$3.5 billion

KEY CHALLENGES

Before deploying Microsoft 365 Defender, most interviewees' organizations were using point solutions from a variety of vendors. These solutions had been acquired over a number of years, often by teams acting in siloes, to address individual domain issues or to respond to new types of threats.

The interviewees noted how their organizations struggled with common challenges, including:

- **Inefficient use of analysts' time and skills.** The security teams dealt each day with an overwhelming amount of security data generated separately by the various tools in use. They spent countless hours reviewing and investigating these alerts, which were often false positives, trying to form a complete picture of the threat with virtually no context to guide them. This resulted in analysts who felt overwhelmed and underutilized.
- **Focusing on remediation rather than prevention.** With limited ability to take a holistic view of the threat activity happening across platforms, low-level signals, which could alert analysts to threats early enough to prevent them, got lost in the noise. Instead, analysts spent more time reviewing problems and piecing together what went wrong rather than responding with a coordinated remediation plan and preventing attacks.
- **Difficulty collaborating across security team silos, resulting in a less effective effort.** The interviewed decision-makers shared the structure of their teams with Forrester. While most of them outlined several subteams and specialty security operations centers (SOCs), most encouraged cooperation across these invisible walls. Such cooperation was very difficult since different teams were using different tools, looking at different types of data, and even using different query languages.

> **"If I got a machine for forensics, I may not even have known how it got infected; it could take anywhere from 5 minutes to several weeks to figure it out. And if I had to restage a machine, it might take me a week to get it shipped from China, or it might get stuck in customs coming from India."**
>
> *Cybersecurity operations manager, manufacturing*

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and a ROI analysis that illustrates the areas financially affected. The composite organization is representative of the four organizations whose decision-makers Forrester interviewed and is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The organization is a $20-billion, multinational energy supplier with operations across multiple sites. Its 15,000 employees work in energy exploration, production, engineering, retail sales and support, B2B sales and support, and corporate management functions. As a provider of critical infrastructure, the composite organization is particularly susceptible to security events, such as ransomware. Its team of 25 security professionals takes the lead in protecting the firm against these intrusions.

Key assumptions

- **Energy provider**
- **$20 billion in revenues**
- **15,000 employees**
- **25 security analysts**

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits

Ref.	Benefit	Year 1	Year 2	Year 3	Total	Present Value
Atr	Increased security team automation and process improvements	$2,404,688	$2,404,688	$2,404,688	$7,214,064	$5,980,102
Btr	Added end-user automation and process improvements	$4,241,309	$4,241,309	$4,241,309	$12,723,927	$10,547,507
Ctr	Reduced cost of risk due to security breaches	$824,484	$824,484	$824,484	$2,473,453	$2,050,371
Dtr	Reduced cost of risk due to faster incident response	$989,381	$1,187,258	$1,286,196	$3,462,834	$2,826,980
Etr	Enhanced IT administration and deployment	$697,950	$697,950	$697,950	$2,093,850	$1,735,698
Ftr	Implemented vendor consolidation	$407,835	$407,835	$407,835	$1,223,505	$1,014,225
	Total benefits (risk-adjusted)	$9,578,277	$9,777,531	$9,877,158	$29,232,966	$24,208,982

INCREASED SECURITY TEAM AUTOMATION AND PROCESS IMPROVEMENTS

Evidence and data. One of the key goals for the interviewed decision-makers was reducing the complexity of interacting with the security software for both analysts and engineers, while increasing the level of collaboration and cooperation between analysts tasked with monitoring different kinds of threats.

"There's a laundry list of things that we need to do here. Every security department has, right? But [Microsoft 365 Defender] has given us back a tremendous amount of bandwidth where we can focus on things that are more proactive in ensuring that we're detecting the right things."

Senior director, information security, insurance

Interviewees related some of the challenges security team members faced on a daily basis. It was their responsibility to review any threats detected and take action to protect the organization. The volume of alerts that were generated daily, however, was overwhelming. As a result, some issues were overlooked or evaded detection while analysts dealt with other alerts.

Microsoft 365 Defender used data and results generated by all of its incorporated security solutions to correlate alerts into incidents, as well as enable autohealing and other capabilities. This allowed all the analysts on the teams to get the holistic view of the situation that is missed when they log in to multiple platforms, look at different screens and reports, and use different query languages or data types from different platforms.

Many interviewees relied on Microsoft 365 Defender's autohealing capability to increase their teams' effectiveness. The autohealing function triggered an investigation in response to well-known threats and automatically recommended appropriate remediation actions for the security team to review

and approve. Using this feature, the teams addressed many issues quickly and easily, freeing up time to use their skills on more complex issues or generate more proactive approaches to threats.

Some executives were unsure about autohealing at first, and their teams continued to keep logs and investigate some or all of the autohealed incidents. As they became more comfortable that the software was handling these situations appropriately, the teams relied on it to address an increasing proportion of incidents and in an increasingly automatic manner.

While interviewees expected to find efficiency improvements with a solution that was more integrated and driven by AI, they were pleasantly surprised to find that this single pane of glass also encouraged collaboration between teams that had previously been siloed. Easy access to a broader set of data, reported in the same familiar way, helped analysts to see how issues they were working on overlapped or were impacted by issues analysts on other teams were investigating.

Modeling and assumptions. Forrester assumes the following in modeling the value of this benefit:

- The composite organization employs 25 FTEs in its security operations team with an average fully burdened annual salary of $135,000.
- Analysts employed on the security team spend approximately 75% of their time on relatively low value/low return activities, such as chasing down alerts — the majority of which are often false. They freed up this time for more valuable tasks.

Risks. Potential risks that could impact the value of this benefit include:

- The size and salary of the security team.
- The amount of time spent on low-value activities before and after Microsoft 365 Defender.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of nearly $6.0 million.

Increased Security Team Automation and Process Improvements

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Security team FTEs	Composite	25	25	25
A2	Average fully burdened salary	TEI standard	$135,000	$135,000	$135,000
A3	Analyst time saved with M365 Defender	Interviews	75%	75%	75%
At	Increased security team automation and process improvement	A1*A2*A3	$2,531,250	$2,531,250	$2,531,250
	Risk adjustment	↓5%			
Atr	Increased security team automation and process improvement (risk-adjusted)		$2,404,688	$2,404,688	$2,404,688
	Three-year total: $7,214,063			**Three-year present value: $5,980,102**	

ADDED END-USER AUTOMATION AND PROCESS IMPROVEMENTS

Evidence and data. Interviewees noted that their organizations delivered a better user experience for employees and, in doing so, increased their satisfaction and productivity by better integrating and simplifying security tools with existing business applications.

Users no longer needed to surrender their devices for restaging after security incidents or for provisioning and security updates during the normal course of business. The solution allowed IT and security to work together to handle these time-consuming tasks virtually while end users continued to work on their devices uninterrupted.

Interviewees reported better performance from their users' devices as a result of the removal of agents for all the point solutions they had been using before, and the overall simplification of the security stack. While these improvements showed up in small increments (e.g., faster boot-up, more response app performance, etc.) they were noticeable to end users and very much appreciated.

> **"We blocked well over 3 million spam messages with Microsoft 365 Defender just last month. From the user experience standpoint, we're trying to push messaging to say security is not a barrier. Security creates a better user experience and here's how."**
>
> *Cybersecurity operations manager, manufacturing*

Finally, Microsoft 365 Defender automated investigation tasks that previously required end-user involvement, therefore increasing productivity for end users. While these interruptions were not a daily occurrence for any particular user, the team needed to ask for this type of input thousands of times a year.

Previously, the requests were annoying at best when required, as they took users' away from their planned work at unexpected times. At worst, one of these interruptions could result in a missed deadline or other commitment. With the deployment of Microsoft 365 Defender, these annoying interruptions became completely unnecessary.

Modeling and assumptions. Forrester assumes the following in modeling the value of this benefit:

- The organization spends 21,600 hours each year restaging machines before deploying Microsoft 365 Defender.
- Productivity drops by 75% for those end users whose devices must be evaluated and restaged.
- After deploying Microsoft 365 Defender, the time spent restaging machines drops to 24 hours per year (interviewees estimated that the new security stack was at least 60% responsible for that improvement).
- The average fully burdened annual salary is $94,500, or $47.25 per hour.
- With fewer, simpler agents running on their devices, each of 15,000 employees also saves 21 hours per year due to improved device performance.
- A conservative 35% of that time savings is recaptured in productive labor.

Risks. Potential risks that could impact the value of this benefit include:

- The proportion of knowledge workers in an organization's workforce.
- The average salary of knowledge workers.
- The rate at which user devices need to be restaged for security purposes, and the impact that has on their ability to perform their jobs.

Results. To account for these risks, Forrester adjusted this benefit downward by 25%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of over $10.5 million.

Added End-User Automation And Process Improvements

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Annual hours to restage machines before M365 Defender	Interviews	21,600	21,600	21,600
B2	Annual hours to restage after M365 Defender	Interviews	24	24	24
B3	Percent attributable to M365 Defender	Interviews	60%	60%	60%
B4	End-user productivity loss during restage	Interviews	75%	75%	75%
B5	Subtotal: End-user productivity improvement from fewer restages	(B1-B2)*B3*B4*B13	$458,760	$458,760	$458,760
B6	Email incidents per year involving end users	Interviews	6,000	6,000	6,000
B7	Hours saved per incident with M365 Defender	Interviews	0.10	0.10	0.10
B8	Subtotal: End-user productivity improvement from better email security	B6*B7*B13	$28,350	$28,350	$28,350
B9	Hours saved annually per user from faster boot/app open times	Interviews	21	21	21
B10	Percent recaptured	Forrester	35%	35%	35%
B11	Number of knowledge workers	Composite	15,000	15,000	15,000
B12	Subtotal: End-user productivity improvement from fewer agents on devices	B9*B10*B11*B13	$5,167,969	$5,167,969	$5,167,969
B13	Average fully loaded hourly employee wage	$70,000+35%/2,000	$47.25	$47.25	$47.25
Bt	Added end-user automation and process improvements	B12+B8+B5	$5,655,078	$5,655,078	$5,655,078
	Risk adjustment	↓25%			
Btr	Added end-user automation and process improvements (risk-adjusted)		$4,241,309	$4,241,309	$4,241,309
	Three-year total: $12,723,927			**Three-year present value: $10,547,507**	

REDUCED COST OF RISK DUE TO SECURITY BREACHES

Evidence and data. According to the interviewees, Microsoft 365 Defender fostered a more secure environment for their organizations. This was primarily due to analysts' ability to quickly identify and take action on the most threatening situations as well as appreciate and deal with the full, cross-platform extent of the threat. Interviewees also noted the solution's autohealing capability was a factor in lowering their organizations' threat risk. To begin with, it dealt effectively and quickly with issues immediately rather than waiting for analysts to get to them. Further, it streamlined the analysts' work to the point where they had time to identify and resolve other threats that required their specific skills.

> **"An obvious benefit is the native aspect — it's native to the Microsoft footprint and built into the tools. We're not granting another organization access to our highly privileged, highly restricted email data to do incident containment and response functions."**
>
> *Lead, security operations, energy*

Modeling and assumptions. Forrester assumes the following in modeling the value of this benefit:

- The average cost of a security breach in an organization the size of the composite is $1,210,600.[2]
- The average organization experiences 2.5 breaches per year.[3]
- A portion of the employee base in the organization also experiences lost productivity during a breach. Affected employees lose 3.6 hours of productive time during the average breach and ensuing downtime.[4]
- A breach affects 10% of the organization's workforce and that the average fully burdened hourly wage in the organization is $47.25.
- The installation of Microsoft 365 Defender, as part of a new or upgraded license, reduces the risk of breach by 25% over the security tools already in place. While customer estimates varied on this point, Forrester uses 25% as a relatively conservative estimate.

Risks. Assigning a value to the avoidance of security breaches is a very difficult exercise. Forrester has used research-based estimates in the assumptions outlined above, but any individual organization will likely not experience an "average breach."

There is a chance an organization will not experience any breaches in a given year, or even during the entire three years the model covers. There is also a very small chance that the organization will experience a catastrophic event costing millions of dollars and damaging the company's reputation.

Potential risks that could impact the value of this benefit include:

- A higher or lower percent of employees being affected by breach-based downtime.
- A different average salary for those impacted.
- A prior situation which would increase or decrease the incrementality of the security enabled by Microsoft 365 Defender.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $2.1 million.

Reduced Cost Of Risk Due To Security Breaches					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Average cost of material breach	Forrester research	$1,210,600	$1,210,600	$1,210,600
C2	Average breaches per year	Forrester research	2.5	2.5	2.5
C3	Hours of user downtime	Forrester research	5,400	5,400	5,400
C4	Average fully burdened hourly wage	TEI standard	$47.25	$47.25	$47.25
C5	Average annual cost of potential security breaches	(C1*C2)+ (C3*C4*C2)	$3,664,375	$3,664,375	$3,664,375
C6	Risk reduction due to M365 Defender stack	Interviews	25%	25%	25%
C7	Reduced cost of risk due to security breaches	C5*C6	$916,094	$916,094	$916,094
	Risk adjustment	↓10%			
Ctr	Reduced cost of risk due to security breaches (risk-adjusted)		$824,484	$824,484	$824,484
	Three-year total: $2,473,453			**Three-year present value: $2,050,371**	

REDUCED COST OF RISK DUE TO FASTER INCIDENT RESPONSE

Evidence and data. Interviewees reported that using Microsoft 365 Defender drastically reduced the number of alerts security analysts needed to investigate each day as a result of its ability to correlate alerts across security platforms into incidents. Analysts had previously spent a typical day investigating hundreds of alerts, trying to piece together how they might be related (and finding that up to 80% of them were false alarms). Microsoft 365 Defender served up a much smaller list of incidents, which involved dozens of alerts rather than hundreds. Because the software presented analysts with stories and solutions, they could quickly get to work remediating the situation rather than spending time trying to construct the story.

An additional benefit of Microsoft 365 Defender's incident-bundling capability was that the time spent assessing and investigating each incident was cut by 50% or more. One interviewee in the energy business told Forrester, "It used to take several hours to investigate an incident once identified, but now it's usually less than an hour." Because alerts from across several domains were correlated into each incident, analysts could get a handle more quickly on the issue.

> **"In some cases, the tool just needs to buy us time to do an adequate review of the risk and take the appropriate action. If it's ransomware or malware, or if it's advanced persistent threats, I have to understand what I'm up against."**
>
> *Cybersecurity operations manager, manufacturing*

Modeling and assumptions. Forrester assumes the following in modeling the value of this benefit:

- While the improved security stack reduces the risk of breach, the organization still experiences security breaches and associated costs as projected by Forrester's research into this topic.[5]
- Eighty percent of the costs associated with these breaches is related to the length of time the issues continue.
- Improved visibility into the nature and extent of the breaches decreases the time to detect and remediate these issues by 50% in the first year, increasing to 65% in the third year as the security team grows more familiar with and skilled in using the Microsoft 365 Defender capabilities.

Risks. Potential risks that could impact the value of this benefit include:

- The number and severity of the organization's security breaches each year.
- The improvement in speed of detection and remediation for any given organization.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of nearly $2.9 million.

Reduced Cost Of Risk Due To Faster Incident Response

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Average annual cost of breaches not avoided	C5-Ct	$2,748,281	$2,748,281	$2,748,281
D2	Improved time to detect and resolve	Interviews	50%	60%	65%
D3	Portion of breach cost impacted by lapsed time	Forrester survey	80%	80%	80%
Dt	Reduced cost of risk due to faster incident response	D1*D2*D3	$1,099,313	$1,319,175	$1,429,106
	Risk adjustment	↓10%			
Dtr	Reduced cost of risk due to faster incident response (risk-adjusted)		$989,381	$1,187,258	$1,286,196
	Three-year total: $3,462,834			**Three-year present value: $2,846,980**	

ENHANCED IT ADMINISTRATION AND DEPLOYMENT

Evidence and data. Interviewees enumerated several ways in which Microsoft 365 Defender not only streamlined the work of the security team, but also the IT organization.

For instance, the technicians responsible for provisioning and updating endpoints were able to let the process run, rather than spending time monitoring and shepherding each device through the upgrade. While the amount of time saved and the specific drivers behind those savings differed, all the interviewees agreed that it was significant across the IT teams.

Microsoft 365 Defender also eliminated a significant portion of help desk tickets, streamlining IT operations. These were security-related issues, such as password resets, failed updates, and decreased system responsiveness due to numerous and/or large security agents running. This time savings allowed management to redeploy technical employees to higher-value tasks and to improve the

job satisfaction of those who continued working on help tickets.

Modeling and assumptions. Forrester assumes the following in modeling the value of this benefit:

- The IT team saves 17,000 hours per year on provisioning-related tickets $16.
- The IT team also saves 11,600 hours each year provisioning and updating devices, assuming an average 10 minutes per device to update/provision after Microsoft 365 Defender vs. the legacy solution.
    - 15,000 employee devices.
    - 1,800 new employees require full 2-hour provisioning protocol each year.
    - 10,000 devices require two 30-minute updates per year.
- Average fully burdened hourly wage of $45 for IT engineers.
- Recapture of 70% of that time in productive work for the organization.

Risks. Potential risks that could impact the value of this benefit include:

- The time spent provisioning and updating endpoints before and after deployment of Microsoft 365 Defender
- The reduction in tickets surrounding provisioning and security-related issues (e.g., password resets, phishing inquiries).
- The average salary of IT engineers.
- The average cost per help desk ticket.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $1.7 million.

Enhanced IT Administration and Deployment

Ref.	Metric	Source	Year 1	Year 2	Year 3
E1	Help desk tickets avoided	Interviews	15,000	15,000	15,000
E2	Cost per ticket	Composite	$16	$16	$16
E3	Total IT hours saved on provisioning and updating devices	Interviews	17,000	17,000	17,000
E4	IT team average fully burdened hourly salary	TEI standard	$45	$45	$45
E5	Percent recaptured	TEI standard	70%	70%	70%
Et	Enhanced IT administration and deployment	(E1*E2)+(E3*E4*E5)	$775,500	$775,500	$775,500
	Risk adjustment	↓10%			
Etr	Enhanced IT administration and deployment (risk-adjusted)		$697,950	$697,950	$697,950
	Three-year total: $2,093,850			**Three-year present value: $1,735,698**	

IMPLEMENTED VENDOR CONSOLIDATION

Evidence and data. All the interviewed decision-makers confirmed their organizations used multiple security solutions before investing in Microsoft 365 Defender. Even though most of them used Microsoft operating systems and productivity applications, they had acquired several security solutions over time as they tried to address emerging threats in an increasingly complex cybersecurity environment.

Interviewees unanimously described Microsoft's security offerings as best in class. They believed Microsoft 365 Defender, in particular, provided strong performance along with the additional benefits of dealing with a single vendor and using a product that integrates with their larger Microsoft estate.

Modeling and assumptions. Forrester assumes the following in modeling the value of this benefit:

- The organization replaces an average of three point solutions made redundant with the deployment of the Microsoft security stack.
- The average cost of each of those subscriptions is $120,000 per year.
- It also redeploys the equivalent of one FTE at a fully burdened annual salary of $93,150, who administers and monitors those solutions.

Risks. Potential risks that could impact the value of this benefit include:

- The number and subscription cost of security software Microsoft 365 Defender replaces.
- The time and salary of any system administrators for those solutions.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a

> **"It does the login and reporting into Sentinel, it has the EDR, it does antivirus. That one agent does so much we just replaced everything with Microsoft 365 Defender. It's less expensive than most of the other things, as well."**
>
> *Head of global monitoring and alerting, energy*

three-year, risk-adjusted total PV of nearly $1.0 million.

Implemented Vendor Consolidation					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
E1	Average point solutions retired	Interviews	3	3	3
E2	Average annual cost of tools	Interviews	$120,000	$120,000	$120,000
E3	FTE to maintain retired tools	Interviews	1.0	1.0	1.0
E4	Average fully burdened annual salary	TEI standard	$93,150	$93,150	$93,150
Et	Implemented vendor consolidation	E1*E2	$453,150	$453,150	$453,150
	Risk adjustment	↓10%			
Etr	Implemented vendor consolidation (risk-adjusted)		$407,835	$407,835	$407,835
	Three-year total: $1,223,505		**Three-year present value: $1,014,225**		

UNQUANTIFIED BENEFITS

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

- **Improved relationships/coordination between security and IT teams.** Several interviewees spoke to the fact that the goals of the security and IT teams were often seen as conflicting.

> **"We partnered with endpoint engineering on this solution, and the fact that they just had to enable settings to deploy it, instead of pushing out a thick client or having another solution to manage, that was a huge win. It really helped build that relationship."**
>
> *Senior director, information security, insurance*

Security's job was to protect the organization, sometimes at the expense of user convenience. IT team's job was to help employees work as productively as possible, and that team sometimes saw the security team's work as a barrier. The improvements made possible by Microsoft 365 Defender made IT team's job easier and fostered more of a team atmosphere between the two groups.

- **A more empowered, satisfied security team.** The search for skilled security analysts is ongoing for most organizations, as this talent can be difficult to find and easily lost to competitors. One way to mitigate this situation is to give analysts a satisfying and challenging work environment. By removing the majority of low value-added tasks analysts need to deal with and freeing them up to use their unique skills on preventing incidents and improving security, Microsoft 365 Defender contributed to a more satisfied workforce.
- **A proactive rather than reactive approach to security.** Interviewees agreed that the ultimate goal of their teams was to prevent intrusions and

other security issues, not simply to chase them down and fix them. By exposing correlations and giving analysts more time to think about “what if,” Microsoft 365 Defender allowed the teams to improve the environment. As the teams saw this, they were more motivated to take a holistic, forward-looking approach. As the cybersecurity operations manager of a manufacturing company stated, “We have really shifted our program from being reactive to proactive and to almost being able to predict the future before an attacker is able to make a move.”

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement Microsoft 365 Defender and later realize additional uses and business opportunities. One interviewee related that having the solution in place made it possible for them to relate to other companies — both customer and vendors — as a modern entity and they experienced business benefits from those more contemporary relationships.

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**
Gtr	Microsoft fees	$0	$2,775,000	$2,775,000	$2,775,000	$8,325,000	$6,901,014
Htr	Deployment costs	$23,968	$0	$0	$0	$23,968	$23,968
Itr	Ongoing administration costs	$0	$54,338	$54,338	$54,338	$163,014	$135,129
	Total costs (risk-adjusted)	$23,968	$2,829,338	$2,829,338	$2,829,338	$8,511,982	$7,060,111

MICROSOFT FEES

Evidence and data. Interviewees agreed that the majority of the cost for the solution was the fee paid to Microsoft. In many cases, organizations already had E5 licenses with Microsoft, so there was no incremental out-of-pocket cost to deploy the Microsoft 365 Defender solution. In other cases, the organizations had E3 licenses and paid an additional fee to upgrade to the E5 security license.

Modeling and assumptions. Forrester assumes the following in modeling the value of this cost:

- The organization is not currently a full E5 license holder, but purchases 15,000 E5 security licenses for its knowledge workers.
- The composite organization pays the full cost of an E4 security license to use the platform.
- The price of an E5 security license is estimated at $185 per year.

Risks. The Microsoft fees associated with Microsoft 365 Defender may vary if the organization has already purchased full E5 licenses for its employees. In this case, the cost of the security platforms is included in that fee.

Results. Since the primary risk for this cost is that it may actually be lower than indicated in the model, Forrester has adjusted it by 0%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of less than $7.0 million.

Microsoft Fees						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
G1	E5 security licenses purchased	Interviews		15,000	15,000	15,000
G2	Cost per license	Microsoft		$185	$185	$185
Gt	Microsoft fees	G1*G2		$2,775,000	$2,775,000	$2,775,000
	Risk adjustment	0%				
Gtr	Microsoft fees (risk-adjusted)		$0	$2,775,000	$2,775,000	$2,775,000
	Three-year total: $8,325,000			**Three-year present value: $6,901,014**		

DEPLOYMENT COSTS

Evidence and data. Interviewed decision-makers stated that the deployment process for the solution was simple and quick compared to other deployments they had experienced. They found the documentation clear and easy to use, and there was ample support from the Microsoft onboarding team. In fact, interviewees did not pay for additional professional services contracts, nor did they need to hire third-party service companies to help them get up and running.

Training needs were minimal and confined to the security team. While the solution was quite intuitive for experienced security analysts, some of the more junior team members required a few weeks to get fully up to speed in using the solution's capabilities.

> **"We experienced almost no deployment costs. The APIs are robust, so it was easy to integrate with other tools. We scaled up using just the onboarding team, with no third-party services, because our IT team was already so familiar with Microsoft."**
>
> *Senior director, information security, insurance*

Modeling and assumptions. Forrester assumes the following in modeling the value of this cost:

- Two technicians spend the equivalent of one week each setting up and integrating the solution.
- The 25 security analysts receive an average of ten hours of training each.

Risks. Other organizations may experience a different cost for deployment based on:

- The familiarity of their IT team with Microsoft software. Less familiarity may imply the need for some training of IT personnel.
- On the security team's side, a more junior team may require more training than is indicated for the composite organization.
- An organization requiring particularly complex integrations may find that they spend more than the composite on this aspect of deployment.

Results. To account for these risks, Forrester adjusted this cost upward by 20%, yielding a three-year, risk-adjusted total PV of less than $24,000.

Deployment Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
H1	Onboarding and integration	Interviews	$1,800			
H2	IT training	Interviews	$0			
H3	Security team training	Interviews	$18,173			
Ht	Deployment costs	H1+H2+H3	$19,973	$0	$0	$0
	Risk adjustment	↑20%				
Htr	Deployment costs (risk-adjusted)		$23,968	$0	$0	$0
	Three-year total: $23,968			**Three-year present value: $23,968**		

ONGOING ADMINISTRATION COSTS

Evidence and data. Interviewees told Forrester that there was little to no ongoing administrative cost associated with their Microsoft 365 Defender solution. They estimated that a systems administrator might spend about a day per week monitoring and maintaining the system's functionality.

Modeling and assumptions. Forrester assumes the following in modeling the value of this cost:

- A systems administrator spends 50% of their time monitoring and maintaining the solution.
- The average systems administrator fully burdened annual salary is $94,500 ($70,000 base and 35% benefit costs).

Risks. Other organizations may experience a different set of costs if IT salaries are higher or lower in their area.

Results. To account for these risks, Forrester adjusted this cost upward by 15%, yielding a three-year, risk-adjusted total PV of $135,000.

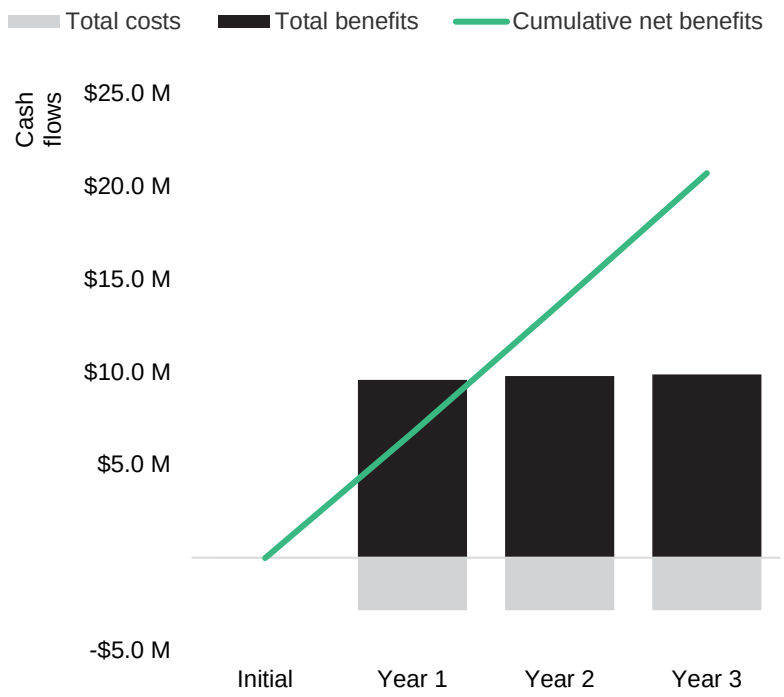
Ongoing Administration Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
I1	Administrator FTEs	Interviews		0.5	0.5	0.5
I2	Administrator fully burdened annual salary	TEI standard		$94,500	$94,500	$94,500
It	Ongoing administration costs	I1*I2		$47,250	$47,250	$47,250
	Risk adjustment	↑15%				
Itr	Ongoing administration costs (risk-adjusted)		$0	$54,338	$54,338	$54,338
	Three-year total: $163,013			**Three-year present value: $135,129**		

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 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	($23,968)	($2,829,338)	($2,829,338)	($2,829,338)	($8,511,982)	($7,060,111)
Total benefits	$0	$9,565,647	$9,763,523	$9,862,461	$29,191,631	$24,174,883
Net benefits	($23,968)	$6,736,309	$6,934,185	$7,033,123	$20,679,649	$17,114,772
ROI						242%

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] 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, Q4 2020.
[3] Ibid.
[4] Ibid.
[5] Ibid.


FORRESTER®