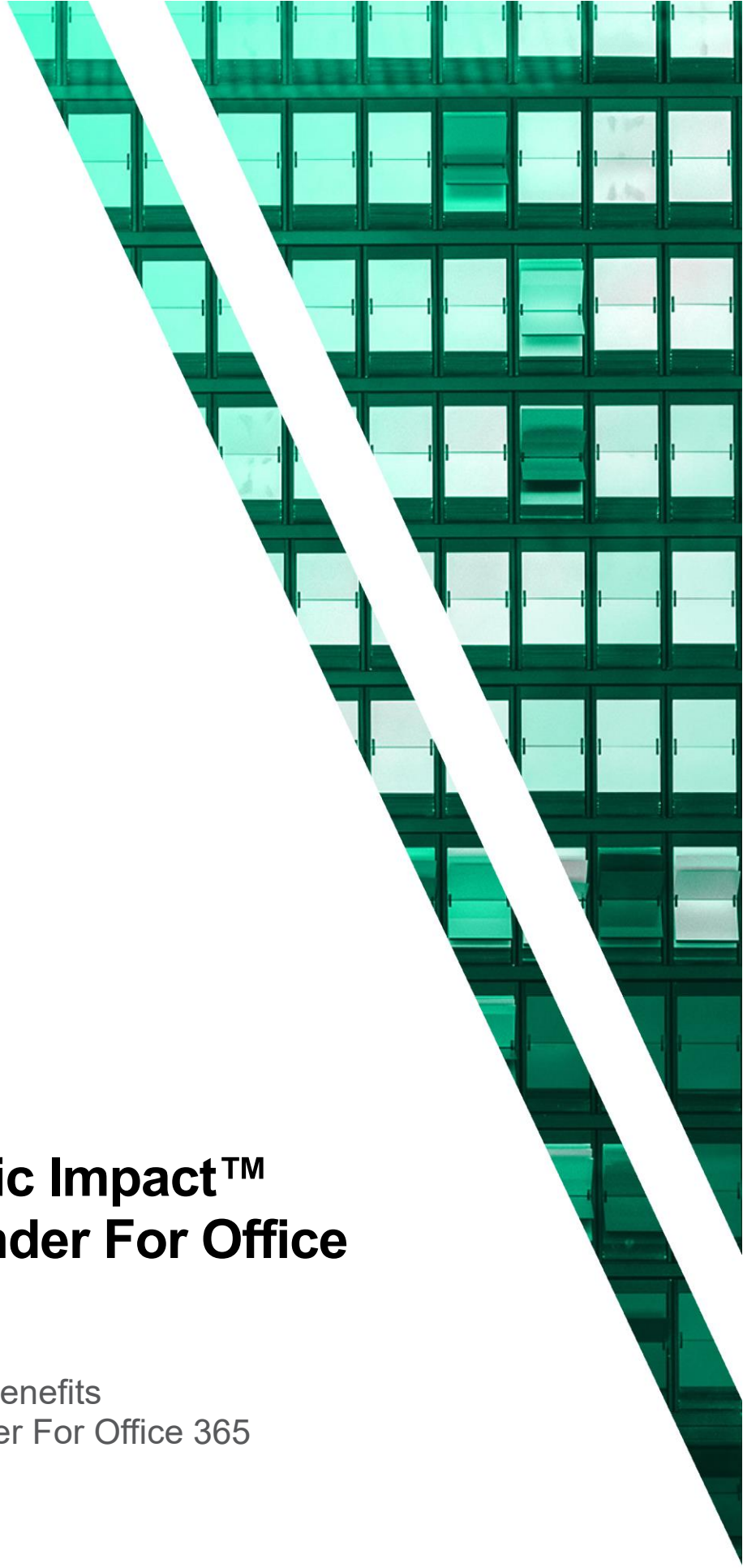
FORRESTER®



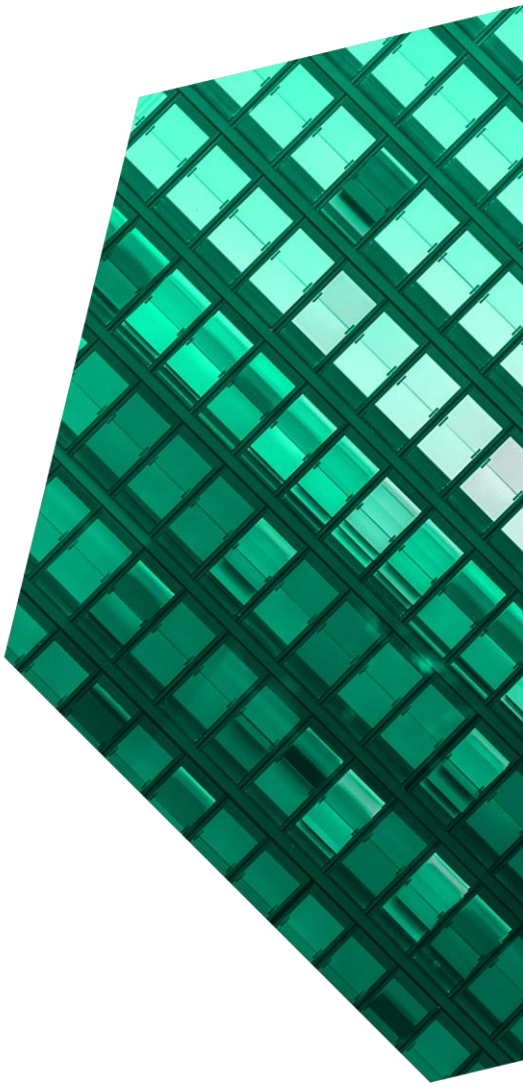
The Total Economic Impact™ Of Microsoft Defender For Office 365

Cost Savings And Business Benefits
Enabled By Microsoft Defender For Office 365

SEPTEMBER 2021

Table Of Contents

Consulting Team: Nick Mayberry



ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. For more information, visit forrester.com/consulting.

Executive Summary

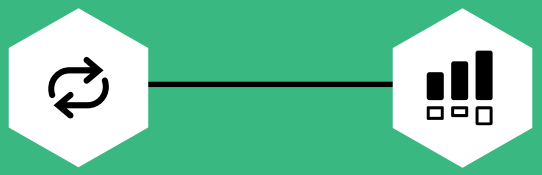
Microsoft Defender for Office 365 enables organizations to defend against malicious threats that come via email and collaboration tools, reducing the risk of a security breach, improving security workflows, and reducing technology expenses. When moving from a competitive solution, customers reduced the time to block links by 95%, the time to investigate threats by 92%, saved $250,000 annually on prior tools, and reduced the risk of a breach by 29%, all while improving their phishing simulations.

Microsoft Defender for Office 365 expands and improves organizations' protection and defense capabilities against threats coming from email and collaboration tools. At its most extensive, the solution prevents broad, volume-based, and known attacks; it protects email and collaboration tools from zero-day malware, phishing attacks, and business email compromise; and it enables attack and threat investigation, hunting, and response, as well as automation of security workflows and improved phishing simulation capabilities.

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

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four customers of different sizes and from different geographies and sectors with experience using Microsoft Defender for Office 365. Before Microsoft Defender for Office 365, most customers used some form of advanced threat protection. In some cases, customers had multiple point solutions, while others had single solutions. In either case, these tools had limited or comparatively lower protection against malware and phishing attacks and limited ability to hunt, investigate, and respond to such threats efficiently. The proliferation of security vendors also increased the complexity of security professional workstreams while increasing potential avenues of attack.

KEY STATISTICS



Return on investment (ROI)
113%

Net present value (NPV)
$3.19M

After the investment in Microsoft Defender for Office 365, customers: 1) improved their security risk posture; 2) realized efficiency gains through the automation of security workflows like link blocking, threat investigation, and threat response; and 3) improved the effectiveness of their phishing simulations while saving costs on prior security tools.

For the purposes of this study, Forrester aggregated the experiences of the interviewed customers and combined the results into a single composite organization that is moving from a previously deployed, competitive solution.

KEY FINDINGS

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

- **Reduced risk of an email or collaboration tool breach when moving from a competitive tool by almost one-third.** Interviewees said Microsoft Defender for Office 365 improved their organizations' security environments by improving visibility, phishing simulations, and the numbers of protected users; by blocking malicious content; and by automating security workflows. This reduced the risk of a breach via email or collaboration tools by 29% and improved employee productivity by 3.3%.
- **Improved link blocking by 95%.** Microsoft Defender for Office 365's automation features improved the efficiency of security teams' protection, detection, and response workstreams. Automated the blocking of malicious links reducing the time needed from 2.5 hours to no time cost because 95% of links were automatically blocked.
- **Improved threat investigation by 92%.** In addition, Microsoft Defender for Office 365 improved averages time to investigate, which decreased from 12 hours to 1 hour. The average time to respond dropped from 8 hours to 30 minutes, of which Defender for Office 365 was partially responsible as the interviewed customers used other SIEM systems for response.
- **Decommissioned prior security tools that cost $250,000 annually.** Lastly, interviewees said their organizations no longer needed some pre-existing security tools after investing in Microsoft Defender for Office 365. Decommissioning these tools saved $200,000 on a gross annual basis, while saving an additional$50,000 gross on services.

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

- **Improved security for work-from-home environment.** Microsoft Defender for Office 365 enabled the interviewees' organizations to flexibly respond to the shifting work environment by providing protection to end users when the organizations implemented work-from-home policies. Interviewees noted that Defender for Office 365 required little to no changes, while protecting vectors like Microsoft Teams made users more secure as they increasingly adopted these tools.
- **Improved visibility.** Interviewees said Microsoft Defender for Office 365 improved visibility into potential threats and provided a better understanding of their organizations' risk profiles. Improved visibility allowed the organizations to further protect against potential threats.
- **Increased annual phishing simulations by 200%.** Microsoft Defender for Office 365 improved the organizations' ability to run additional phishing simulations. Thanks to the efficiencies of Microsoft Defender for Office 365 over prior solutions, customers had extra time to run additional simulations, which increased by 200%, while the number of employees targeted with simulations increased by 50%. This improved employees' awareness and preparedness of malicious email attacks.
- **Platformwide protection.** Interviewees said Microsoft Defender for Office 365 provided protection, detection, and response capabilities across the entire Office 365 suite. Before the investment, the organizations lacked protection in their collaboration environments.
- **Up-leveled security professionals.** Microsoft Defender for Office 365 also enabled organizations' more junior security professionals to take on advanced tasks traditionally handled

by senior team members. After deployment, the junior team members asked more insightful questions, sought out new opportunities and use cases for the technology, and did so without needing the oversight of senior team members.

Costs. Risk-adjusted PV costs include:

- **Licensing fees.** The cost of Microsoft Defender for Office 365 is included in the licenses for Microsoft 365 and Office 365 E5, but customers can also purchase it via two different licenses: Plan 1 and Plan 2. The composite organization uses Plan 2 licensing at $4.25 per user. Volume discounting may apply to certain customers.
- **Cost of implementation, migration, and deployment.** Interviewees said their organizations needed an average of three FTEs to commit 120 hours (or three weeks) for implementation, migration, and deployment. Because the composite switches from a competitive solution, it utilizes a consultant for implementation, migration, and deployment at a cost of $250 per hour for 100 hours. Organizations currently on Microsoft Exchange Online Protection (EOP) can take advantage of free migration services from Microsoft.
- **Internal cost of training and ongoing management.** On average, security operation center (SOC) employees needed 8 hours for training. Interviewees also said their organizations needed an average of 38% of 1 FTE to manage and maintain Microsoft Defender for Office 365.

The customer interviews and financial analysis found that a composite organization experiences benefits of $6.03 million over three years versus costs of $2.84 million, adding up to a net present value (NPV) of $3.19 million and an ROI of 113%.

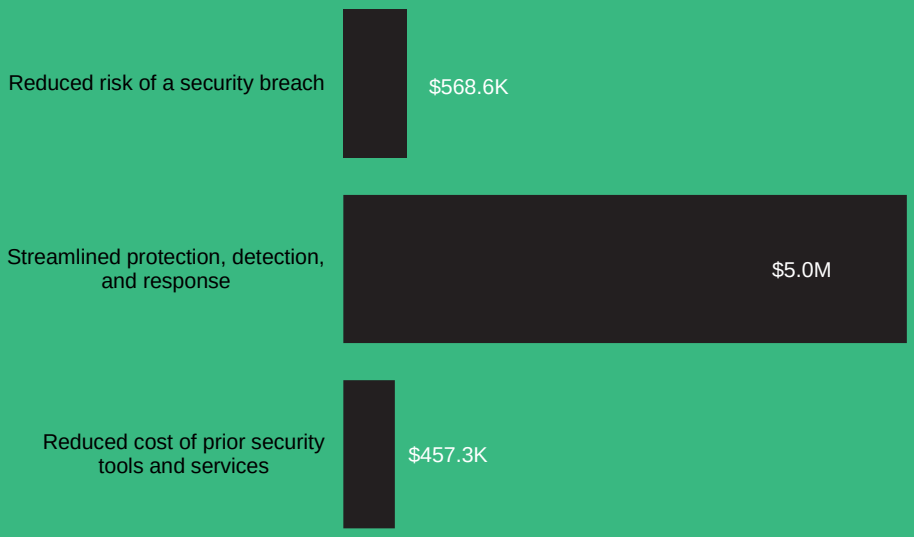
ROI
113%

BENEFITS PV
$6.03M

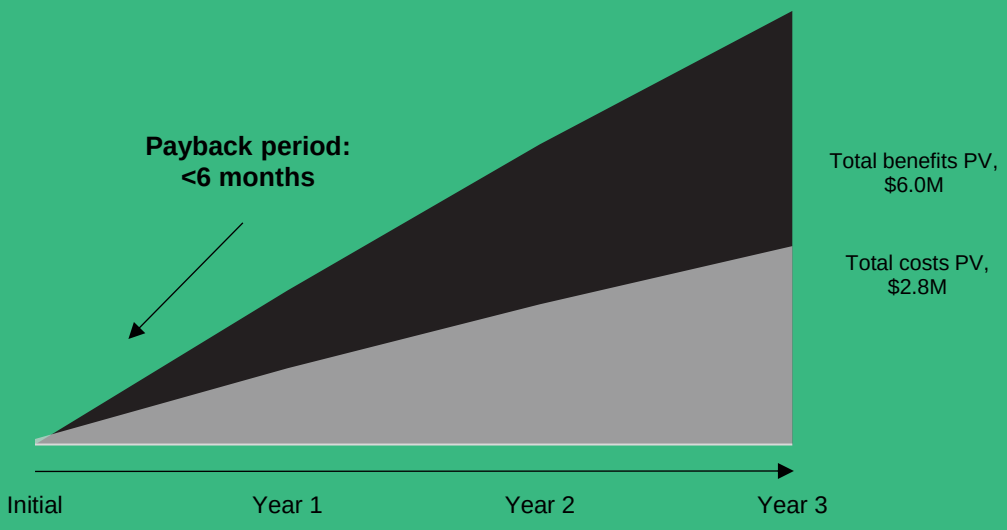
NPV
$3.19M

PAYBACK
<6 months

Benefits (Three-Year)



Financial Summary



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 Defender for Office 365.

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 Defender for Office 365 can have on an organization.

DUE DILIGENCE

Interviewed Microsoft stakeholders and Forrester analysts to gather data relative to Microsoft Defender for Office 365.

CUSTOMER INTERVIEWS

Interviewed four decision-makers at organizations using Microsoft Defender for Office 365 to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

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

FINANCIAL MODEL FRAMEWORK

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

CASE STUDY

Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

The Microsoft Defender For Office 365 Customer Journey

Drivers leading to the Microsoft Defender for Office 365 investment

Interviewed Organizations

Industry	Region	Interviewee	Total employees MDO use cases
Professional services	Global	CTO	12,000 Protection and detection
Financial services	North America	VP of SOC	17,000 Phishing simulation
Professional services	APAC	Head of IT systems and processes	20,000 Phishing simulation, protection, and detection
Food and beverage	Global	Head of global SOC	275,000 Protection, detection, and response

KEY CHALLENGES

Before investing in Microsoft Defender for Office 365, the interviewees' organizations had limited security against threats from email messages, links, and collaboration. This typically consisted of anti-spam, anti-malware, and occasionally anti-phishing tools. Where there were tools in place, the organizations used a variety of vendors to protect their end users from such threats. Regardless, the organizations still lacked an integrated solution with zero-day protection, collaboration tool protection, and the ability to easily investigate, hunt, and respond to threats.

The interviewees' organizations struggled with common challenges, including:

- **Limited capabilities.** Although the organizations had deployed various security tools before investing in Microsoft Defender for Office 365, those tools lacked important capabilities that could further protect their data from a breach. For example, some interviewees said their prior tools lacked desired features that could defend against more complex or sophisticated attacks as well as zero-day protection that could remediate vulnerabilities that were not yet widely known. Additionally, the organizations did not have any means to hunt, investigate, or respond to threats stemming from email or collaboration tools. Lastly, the organizations also used phishing simulation tools that were not trustworthy to end users because they lacked the ability to use brand names.

> **"Having multiple vendors complicated our security environment and left us open to different supply-chain attacks. This actually left us open to more attacks than consolidating under a single vendor would."**
>
> *VP of SOC, financial services*

- **Vendor proliferation.** Interviewees said their organizations used multiple point solutions provided by different vendors to protect their previous environments. One interviewee noted that this created risk by introducing multiple points of attack into their organization's security chain. Other interviewees said reducing vendors saved them both time on vendor management

and the costs associated with multiple licenses. Some said their organizations also found consolidation under Microsoft to be particularly attractive because they were already paying for licenses that included Defender for Office 365.

"We have a very strong desire to maximize the value we get out of our various vendor licenses. We would [typically] take on an additional licensing costs for a substantially better product, but we did not have to [do that] in this case. We already were on an E5 license, and Defender for Office 365 met our needs."

CTO, professional services

COMPOSITE ORGANIZATION

Based on the interviews, 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 four companies that Forrester interviewed and is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The composite is a B2B organization that operates globally and generates $5 billion in revenue. It has 20,000 full-time employees, and six are messaging professionals and six are security professionals who work in the SOC. The organization already invested in a handful of tools including anti-spam, anti-malware, and anti-phishing tools to bolster its security against threats from email and links. Decision-makers choose to switch to Microsoft Defender for Office 365 to bolster these capabilities and to add protection to the organization's collaboration tools like Microsoft Teams and Microsoft SharePoint. This gives the SOC the ability to hunt, investigate, and respond to threats that come from email and collaboration tools.

Deployment characteristics. Decision-makers choose to switch from a competitive security offering to Microsoft Defender for Office 365. Because the solution is not already included in the organization's existing licenses, decision-makers opt for the Plan 2 license, which includes protection against malicious links, attachments, and phishing. The plan also includes the ability hunt, detect, and respond to potential threats. It takes three to four weeks for the composite to implement and deploy Microsoft Defender for Office 365 across its 20,000-employee user base, and those employees spend approximately 90% of their work time in applications like Microsoft Outlook and Microsoft Teams, which are protected by Defender for Office 365. It takes just more than one additional week for the organization's SOC team to get up to speed with the hunting, investigation, and response features of the tool.

Key assumptions

- **$5 billion in revenues**
- **20,000 employees**
- **6 messaging professionals**
- **6 SOC professionals**

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	Reduced risk of a security breach	$228,625	$228,625	$228,625	$685,875	$568,557
Btr	Streamlined protection, detection, and response	$2,012,470	$2,012,470	$2,012,470	$6,037,411	$5,004,716
Ctr	Reduced cost of prior security tools and services	$112,500	$225,000	$225,000	$562,500	$457,269
	Total benefits (risk-adjusted)	$2,353,595	$2,466,095	$2,466,095	$7,285,786	$6,030,542

REDUCED RISK OF A SECURITY BREACH

Evidence and data. Interviewees said Microsoft Defender for Office 365 reduced their organizations' risks of potential security breaches. Their security risk profiles improved because the solution:

- Improved visibility into security environments and potential threats.
- Improved quality and value of phishing simulations as seen by user awareness improvements.
- Increased the numbers of protected users.
- Improved the blocking of malicious content.
- Improved SOC teams' abilities to hunt, investigate, and respond to potential threats.
- Reduced complexity by establishing a single-vendor environment.

"Microsoft Defender for Office 365 improved protection for our whole company between 20% and 30%."

Head of global SOC, food and beverage

Interviewees noted that Microsoft Defender for Office 365 improved their visibility into potential threats compared to their prior environments. For example, the head of global SOC in the food and beverage industry said their organization now had visibility into more potential threats, with between 50% to 75% of such threats going unseen in their prior environment. Others noted that Defender for Office 365 helped them to identify the types of threats they were seeing and the sources of these threats. This enabled the interviewees to plan and take actions to prevent such threats in the future.

"Microsoft Defender for Office 365 helped us to zero in and identify what apps or vectors were most susceptible to threats so that we could plug them proactively."

Head of IT systems and processes, professional services

Defender for Office 365 also bolstered visibility by increasing the number of employees who were protected. One interviewee said their organization improved in this area by between 10% and 12%. Additionally, Defender for Office 365 includes

protection across the Office 365 suite, which means it also protected employee activity in collaboration tools like Microsoft Teams and Microsoft SharePoint, where no protection existed in the prior environment.

> **"Deploying Microsoft Defender for Office 365 helped us increase the number of protected employees by between 10% and 12%."**
>
> *Head of IT systems and processes, professional services*

Phishing simulations also improved after deployment. Before using Defender for Office 365, the effectiveness of the organizations' phishing simulations was limited by a lack of features, including no targeting capabilities and no permission to use real-world brand names. With Defender for Office 365, the interviewees' organizations gained the ability to target specific internal groups (e.g., the finance department, specific delivery teams), and the solution improved the credibility of phishing simulations by legally leveraging real-world brand names. As a result, the organizations saw evidence that employees had more awareness of the content coming through email and collaboration tools and that they displayed more positive, security-conscious behaviors than before.

> **"With Microsoft Defender for Office 365, not only can we cover all of our employees, but we can also target certain groups. If we want to target the procurement group or finance or HR, I can do it. I can do much more than before."**
>
> *Head of IT systems and processes, professional services*

Interviewees also said they saw positive impacts from Microsoft Defender for Office 365's automation capabilities. Activities automated by Defender for Office 365 included:

- Blocking of malicious links.
- Reducing the mean time to detect a potential threat.
- Reducing the mean time to investigate a potential threat.
- Reducing the mean time to respond to a potential threat.

Automation impacted the organizations' security in several key ways. This included protecting against more malicious content, removing the risk of human error in security workflows, and allowing security professionals to spend more time focused on threats that Defender for Office 365did not automatically handle. Interviewees said reducing workflows reduced the effort needed to block malicious links by 95% and the time to investigate and respond to potential threats by 59%.

> **"There has been a positive impact in terms of both mean time-to-detect and mean time-to-resolve. From my perspective, the real power is the automation and the intelligence both for the end user and for our SecOps team."**
>
> *CTO, professional services*

Modeling and assumptions. For the composite organization, Forrester estimates:

- The average number of material breaches is 3.1 per year.

- The average total internal and external costs of a material breach is $657,494.
- Microsoft Defender for Office 365 covers 25% of breaches.
- End users spend 90% of their time in Office 365 applications.
- Microsoft Defender for Office 365 improves the organization's risk profile compared to the prior environment by 29%.
- Each material breach has the potential to cause 12.4 hours of downtime to 8,548 employees.
- The average fully burdened hourly rate of these employees is $35.
- These employees recapture productivity at a rate of 50%.

Risks. The reduced risk of a security breach will vary with:

- The average number of material breaches each year.
- The total internal and external costs of a breach.
- The prior employee downtime hours caused by a material breach.
- The average number of employees affected by a breach.
- The fully burdened hourly rates of these employees.
- The amount of employee productivity able to be recaptured by preventing a material breach.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $568,600.

Reduced Risk Of A Security Breach					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Average number of material breaches	Forrester data	3.1	3.1	3.1
A2	Average total internal and external costs of a material breach	Forrester data	$657,494	$657,494	$657,494
A3	Percentage of material breaches seen by Microsoft Defender for Office 365 versus other Microsoft Defender solutions	Assumption	25%	25%	25%
A4	Percentage of end-user activity protected by Microsoft Defender for Office 365	Interviews	90%	90%	90%
A5	Percentage risk improvement from Microsoft Defender for Office 365	Interviews	29%	29%	29%
A6	Subtotal: Reduced risk of a security breach	A1*A2*A3*A4*A5	$132,995	$132,995	$132,995
A7	Previous downtime hours from breach per employee	A1*4 hours per breach	12.4	12.4	12.4
A8	Number of employees affected	Forrester data	8,548	8,548	8,548
A9	Average fully burdened hourly rate per employee	Composite	$35	$35	$35
A10	Productivity recapture rate	Assumption	50%	50%	50%
A11	Subtotal: Improved productivity from reduced downtime	A7*A8*A9*A10*A3*A4*A5	$121,033	$121,033	$121,033
At	Reduced risk of a security breach	A6+A11	$254,028	$254,028	$254,028
	Risk adjustment	↓10%			
Atr	Reduced risk of a security breach (risk-adjusted)		$228,625	$228,625	$228,625
	Three-year total: $685,875			**Three-year present value: $568,557**	

STREAMLINED PROTECTION, DETECTION, AND RESPONSE

Evidence and data. Interviewees said their organizations saved time with protection, detection, and response processes associated with email and collaboration-tool security after deploying Microsoft Defender for Office 365. They said that before deployment, their organizations leveraged highly manual processes to accomplish many of the SOC team's regular activities. After deploying Defender for Office 365, the organizations were able to implement automation as part of these activities. This reduced the time costs of protection, detection, and response processes, even though the frequency of those processes increased due to improved visibility and detection capabilities provided by Defender for Office 365.

To protect against malicious links before deployment, the organizations had to use an average of five different firewalls or proxies and manually enter the malicious link or URL. Entering a link in each location took approximately 30 minutes, and the organizations needed to do this with an estimated 60 to 70 links each month.

After deploying Microsoft Defender for Office 365, the organizations used safe links to automate the vast majority of this process. One customer even stated that the entirety of this work was displaced via automation with Microsoft Safe Links. Customers saved an average of 1,750 hours annually from Safe Links alone.

Improved link-blocking process

95%

Microsoft Defender for Office 365 also helped to automated investigation and response processes. Interviewees said it previously took their organizations between one day and several days to investigate each alert in their prior environments. Such alerts happened between five and 10 times daily in this environment. After deploying Defender for Office 365, the organizations reduced the time needed for alert investigations to between a few minutes and one hour. Interviewees also said Defender for Office 365 caught more potential threats than their prior solutions, which meant they could conduct 20 investigations daily instead of five to 10.

Improved threat investigation

92%

Regarding response, although Microsoft Defender for Office 365 does come with response capabilities, the interviewed organizations were using third-party SIEMs for response. These interviewees said that Microsoft Defender for Office 365 provided data that allowed security teams to be notified of potential threats requiring response without any need to open an IT ticket. Security teams previously required about one day to respond to a potential threat, but this time later shrunk to minutes. Interviewees estimated that the data provided by Microsoft Defender for Office 365 to their third-party SIEMs was at least partially responsible for this improvement in response.

Improved threat response process

9%

Modeling and assumptions. For the composite organization, Forrester estimates:

- The previous time required to protect against a malicious link was 2.5 person-hours.
- The number of annual malicious links is 780.
- There's a 95% reduction in links needing manual intervention to protect them from Microsoft Defender for Office 365.
- The fully burdened hourly rate of a security professional is $68.
- The previous time needed to investigate an alert decreases from 12 person-hours to 1 person-hour.
- The number of annual alerts investigated rises from 2,738 to 7,300.
- The time required to respond to a threat is reduced from 8 person-hours to 30 minutes.
- The organization responds to 7,300 threats each year.
- Microsoft Defender for Office 365 is responsible for 10% of the improvement to threat response

Risks. The benefits of streamlining protection, detection, and response will vary with:

- The time previously needed to protect against a malicious link.

- The number of links that require such protection.
- The time previously needed to investigate an alert and the increase in the number of such alerts.
- The time previously needed to respond to a threat and the number of threats that require a response.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $5 million.

Streamlined Protection, Detection, And Response

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Person-hours previously needed to protect against a malicious link	Interviews	2.5	2.5	2.5
B2	Previous number of malicious links	Interviews	780	780	780
B3	Reduction from Microsoft Defender for Office 365	Interviews	95%	95%	95%
B4	Average fully burdened hourly rate for a security professional	Composite	$68	$68	$68
B5	Subtotal: Cost savings from Safe Links	B1*B2*B3*B4	$125,970	$125,970	$125,970
B6	Person-hours previously needed to investigate an alert	Interviews	12	12	12
B7	Number of alerts previously investigated	Interviews	2,738	2,738	2,738
B8	Person-hours to investigate an alert with Microsoft Defender for Office 365	Interviews	1	1	1
B9	Number of alerts investigated with Microsoft Defender for Office 365	Interviews	7,300	7,300	7,300
B10	Subtotal: Cost savings from improved threat investigation	((B6*B7)-(B8*B9))*B4	$1,737,808	$1,737,808	$1,737,808
B11	Person-hours previously spent responding to a threat	Interviews	8	8	8
B12	Person-hours spent responding to a threat with Microsoft Defender for Office 365	Interviews	0.5	0.5	0.5
B13	Number of threats responded to	Interviews	7,300	7,300	7,300
B14	Percentage of responsibility of Microsoft Defender for Office 365	Interviews	10%	10%	10%
B15	Subtotal: Cost savings from improved threat response	(B11-B12)*B13*B14*B4	$372,300	$372,300	$372,300
Bt	Streamlined protection, detection, and response	B5+B10+B15	$2,236,078	$2,236,078	$2,236,078
	Risk adjustment	↓10%			
Btr	Streamlined protection, detection, and response (risk-adjusted)		$2,012,470	$2,012,470	$2,012,470
	Three-year total: $6,037,411			**Three-year present value: $5,004,716**	

REDUCED COST OF PRIOR SECURITY TOOLS AND SERVICES

Evidence and data. The interviewees said their organizations reduced the costs of security tools and services after deploying Microsoft Defender for 365. Each organization was able to decommission the use of at least one tool related to email security, and the value of these tools varied. One interviewee said their organization saved approximately $70,000 annually while another reported saving approximately $250,000. Some tools also required using a vendor's services, and this increased annual costs by as much 13%. Although they could not estimate the total time savings, some interviewees said their organizations spent less time on vendor management because the number of vendors in their security portfolios decreased.

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

- It spent $200,000 annually on a previous email security tool.
- The email security tool required an annual investment of $50,000 in associated services.
- The organization partially decommissions its previous email security in Year 1, and it fully decommissions it by Year 2.

Annual costs saved on prior tools

$250,000

Risks. The reduced cost of prior security tools and services will vary with:

- Whether or not the organization decommissions any previous security tools.
- The annual cost of the previous tools and any associated services.
- The rate at which the tools are decommissioned.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $457,300.

Reduced Cost Of Prior Security Tools And Services

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Previous annual cost of email security tool	Interviews	$200,000	$200,000	$200,000
C2	Previous annual cost of email security services	Interviews	$50,000	$50,000	$50,000
C3	Percentage of decommissioned tools and services	Composite	50%	100%	100%
Ct	Reduced cost of prior security tools and services	(C1+C2)*C3	$125,000	$250,000	$250,000
	Risk adjustment	↓10%			
Ctr	Reduced cost of prior security tools and services (risk-adjusted)		$112,500	$225,000	$225,000
	Three-year total: $562,500			**Three-year present value: $457,269**	

UNQUANTIFIED BENEFITS

Additional benefits that interviewees said their organizations experienced but were not able to quantify include:

- **Improved visibility.** Interviewees said Microsoft Defender for Office 365 improved their organizations' visibility into potential threats and provided a better understanding of their risk profiles. In addition to the reduced risk metrics and improved phishing reporting rates, interviewees also said their organizations saw additional click-throughs that were not caught before by as much as 41%. A head of IT systems and processes in the professional services industry stated: "The added visibility from Microsoft Defender for Office 365 provides us with a lot more information on threats, such as how many threats are coming from different vectors. It helps us identify these risks and protect against them accordingly."
- **Improved phishing simulation process.** The interviewees' organizations were able to improve their processes for deploying phishing simulations, but interviewees were unable to quantify the impact of this improvement. Because their organizations saved time setting up and deploying these simulations, they were able to run more of them, increasing annual simulations by at least 200% (from once per quarter to once or twice per month). Running phishing simulations with Microsoft Defender for Office 365 also increased the number of employees targeted with simulations by 50%.

Increase in annual phishing sims

200%

- **Platformwide protection.** Interviewees noted that Microsoft Defender for Office 365 provided protection, detection, and response capabilities across the entire Office 365 suite, which they said was missing in their prior environments. A CTO in the professional services industry said: "At the end of the day, we work across a distribution ecosystem across Microsoft 365. Defender for Office 365 creates a lot of benefit because of this."

  The VP of SOC in the financial services industry said: "Defender for Office 365 modernized our environment. As Microsoft adds more products, we'll continue to get more agility from it."
- **Up-leveled security professionals.** Interviewees said Microsoft Defender for Office 365 allowed their organizations' junior security professionals to take on more advanced tasks that senior team members traditionally handled. The CTO in the professional services industry said: "We're starting to see more and more professionals asking insightful questions or seeking out new opportunities with the solutions. They're not necessarily waiting for technical permission to advance new solutions, do things differently, or really take advantage of the various features of Defender for Office 365."
- **Access to Microsoft support.** Interviewees said their organizations had great experiences working with Microsoft support. The VP of SOC in the financial services industry said: "One of the really good benefits of this tool is Microsoft's support. Working with [Microsoft's] customer success team has been great! If our rep is online and we ping them, we get a response back in 3 minutes."

FLEXIBILITY

The value of flexibility is unique to each organization. There are multiple scenarios in which a customer might implement Microsoft Defender for Office 365

and later realize additional uses and business opportunities, including:

- **Improved security for work-from-home environment.** Interviewees said Microsoft Defender for Office 365 enabled their organizations to flexibly respond to the shifting work environment by providing protection to end users when the organizations implemented work-from-home policies. The head of IT systems and processes in the professional services industry said: “After implementing work-from-home [policies], we would have struggled to provide security and safety to end users outside of our firewalls or proxies that protect in-office workers. However, with Microsoft Defender for Office 365, features like Safe Links and protection for SharePoint and Teams allowed us to protect work-from-home employees just as effectively as those in the office.”
- **Increased ownership by the SOC team.** Interviewees said Microsoft Office 365 added operational flexibility because security teams felt they gained more ownership of security across the Office 365 suite compared to in their prior states. The CTO in the professional services industry said: “I’ve heard feedback from our security teams that their new ability to self-govern spam has improved their sense of control over protecting our company. They’ve modulated the configurations and sensitivity to get to a sweet spot that they weren’t in before.”
- **Custom rules.** The interviewees said their organizations plan to deploy custom rules with Microsoft Defender for Office 365 in the future. This would provide added protection from threats that might be unique to their businesses. The head of global SOC from the food and beverage industry stated, “We plan to implement custom rules in the future to enable more complex detections — particularly for unique scenarios for our business.”

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**
Dtr	Cost of Microsoft Defender for Office 365 licensing	$0	$1,071,000	$1,071,000	$1,071,000	$3,213,000	$2,663,418
Etr	Cost of implementation, migration, and deployment	$27,500	$0	$0	$0	$27,500	$27,500
Ftr	Internal costs of training and ongoing management	$3,590	$57,446	$57,446	$57,446	$175,930	$146,451
	Total costs (risk-adjusted)	$31,090	$1,128,446	$1,128,446	$1,128,446	$3,416,430	$2,837,369

COST OF MICROSOFT DEFENDER FOR OFFICE 365 LICENSING

Evidence and data. There are several ways to license Microsoft Defender for Office 365. Three of the interviewees' organizations already had Microsoft 365 E5 licenses, while one licensed Microsoft Defender for Office 365 directly with a Plan 2 license. Those organizations with an E5 license did not incur any additional licensing costs from deploying Microsoft Defender for Office 365 because it is already a part of that license. Because of this, Forrester modeled the composite organization with a Plan 2 license so as to more accurately measure the isolated benefits and costs of Microsoft Defender for Office 365 from other benefits and costs that an E5 licensee would receive.

A Plan 2 license includes:

- Safe Attachments
- Safe Links
- Safe Attachments for SharePoint, OneDrive, and Microsoft Teams
- Anti-phishing in Defender for Office 365 protection
- Integration with Microsoft 365 Defender (XDR)
- Priority Account Protection
- Threat Explorer
- Automated investigation and response
- Attack simulation training
- Campaign Views

Forrester based the composite organization's pricing on list price, although volume discounting could apply in the real world.

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

- All 20,000 employees are covered by Microsoft Defender for Office 365.
- The per-user pricing is $4.25 per month.

Risks. The cost of licensing will vary with:

- The number of employees who need protection with Microsoft Defender for Office 365.
- The monthly fee per user.

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 less than $2.7 million.

Cost Of Microsoft Defender For Office 365 Licensing						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
D1	Number of FTEs protected	Composite		20,000	20,000	20,000
D2	Price per user per month	Composite		$4.25	$4.25	$4.25
Dt	Cost of Microsoft Defender for Office 365 licensing	D1*D2*12	$0	$1,020,000	$1,020,000	$1,020,000
	Risk adjustment	↑5%				
Dtr	Cost of Microsoft Defender for Office 365 licensing (risk-adjusted)		$0	$1,071,000	$1,071,000	$1,071,000
	Three-year total: $3,213,000			**Three-year present value: $2,663,418**		

COST OF IMPLEMENTATION, MIGRATION, AND DEPLOYMENT

Evidence and data. Interviewees said their organizations incurred internal time costs to implement and deploy Microsoft Defender for Office 365. They needed an average of three FTEs to commit 120 hours (or 3 weeks) for implementation, migration, and deployment.

Organizations moving from a competitive solution to Microsoft Defender for Office 365 may choose to use a consultant for implementation, migration, and deployment. Forrester used this scenario to model the composite organization's cost of implementation, migration, and deployment.

Organizations currently on EOP can take advantage of free migration services from Microsoft.

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

- The composite chooses to use an implementation consultant for deployment.
- A consultant spends a total of 100 hours to implement Defender for Office 365.
- The hourly rate of a consultant is $250.

Risks. The cost of implementation, migration and deployment will vary with:

- Whether or not the organization uses a consultant or internal teams for implementation, migration, and deployment.
- The hourly rate of a consultant.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $27,500.

Cost Of Implementation, Migration, And Deployment						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Consultant hours for implementation	Microsoft	100			
E2	Consultant hourly rate	Microsoft	$250			
Et	Cost of implementation, migration, and deployment	E1*E2	$25,000	$0	$0	$0
	Risk adjustment	↑10%				
Etr	Cost of implementation, migration, and deployment (risk-adjusted)		$27,500	$0	$0	$0
	Three-year total: $27,500			**Three-year present value: $27,500**		

INTERNAL COSTS OF TRAINING AND ONGOING MANAGEMENT

Evidence and data. Interviewees said their organizations incurred internal costs related to training and ongoing management. They said only SOC employees needed to be trained on the hunting, investigation, and response features of Microsoft Defender for Office 365. Each SOC employee required an average of 8 hours to complete training. For ongoing management, interviewees said their organizations needed 38% of one FTE to manage and maintain Microsoft Defender for Office 365.

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

- Each of its six SOC professionals require training.
- One additional SOC professional requires training each year to account for turnover.
- It takes an average of 8 hours to complete training.
- Ongoing management requires approximately 38% of one FTE's time.

Risks. The internal cost of training and ongoing management will vary with:

- The number of SOC professionals who require training.
- The average time needed to train each SOC employee.

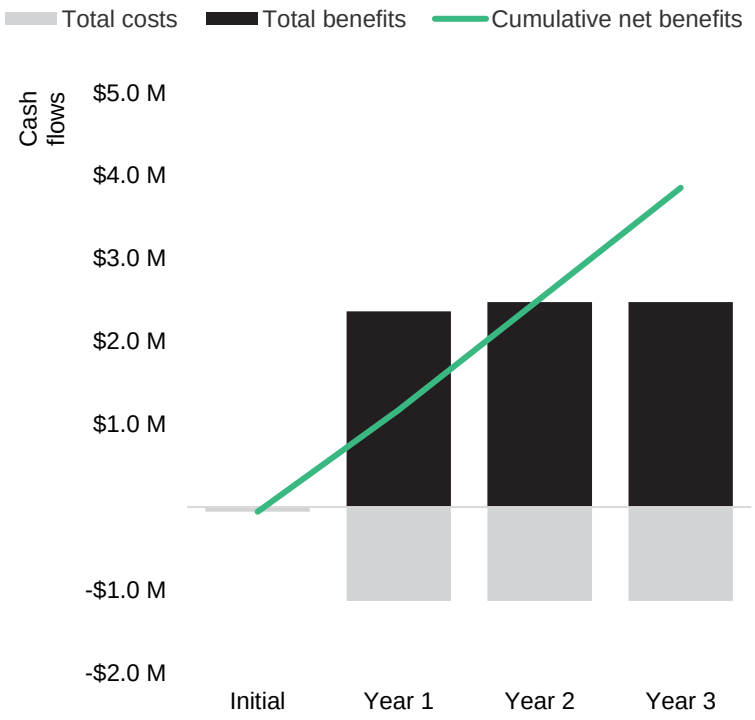
Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of less than $147,000.

Internal Costs Of Training And Ongoing Management						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
F1	FTEs who need training	Interviews	6	1	1	1
F2	Hours required for training	Interviews	8	8	8	8
F3	Total person-hours required for ongoing management	Interviews	0	760	760	760
F4	Average fully burdened hourly rate per FTE	Composite	$68	$68	$68	$68
Ft	Internal costs of training and ongoing management	((F1*F2)+F3)*F4	$3,264	$52,224	$52,224	$52,224
	Risk adjustment	↑10%				
Ftr	Internal costs of training and ongoing management (risk-adjusted)		$3,590	$57,446	$57,446	$57,446
	Three-year total: $175,930			**Three-year present value: $146,451**		

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



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

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

Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($31,090)	($1,128,446)	($1,128,446)	($1,128,446)	($3,416,430)	($2,837,369)
Total benefits	$0	$2,361,062	$2,473,562	$2,473,562	$7,308,185	$6,049,109
Net benefits	($31,090)	$1,225,149	$1,337,649	$1,337,649	$3,869,356	$3,193,173
ROI						113%
Payback period (months)						<6

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.


FORRESTER®