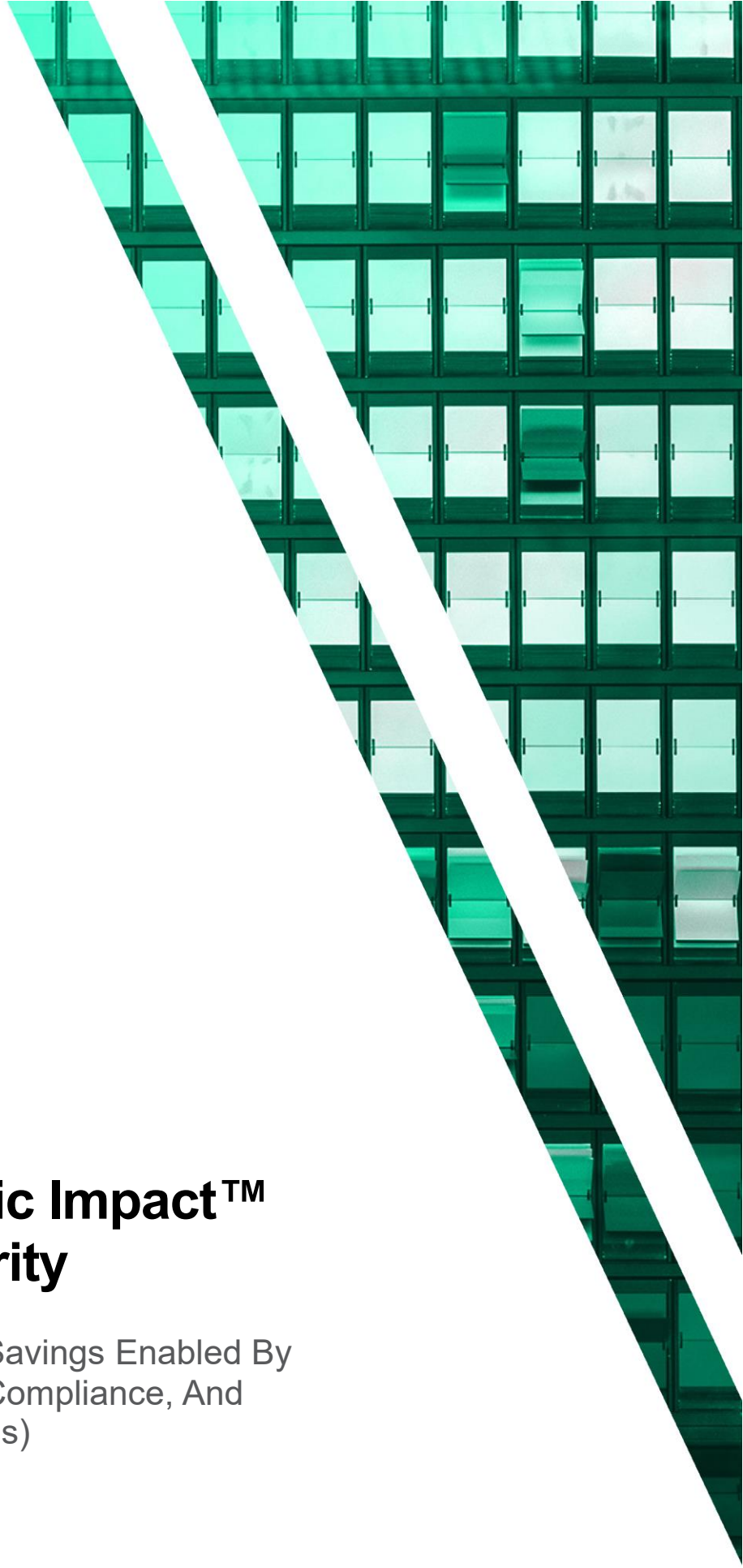
FORRESTER®



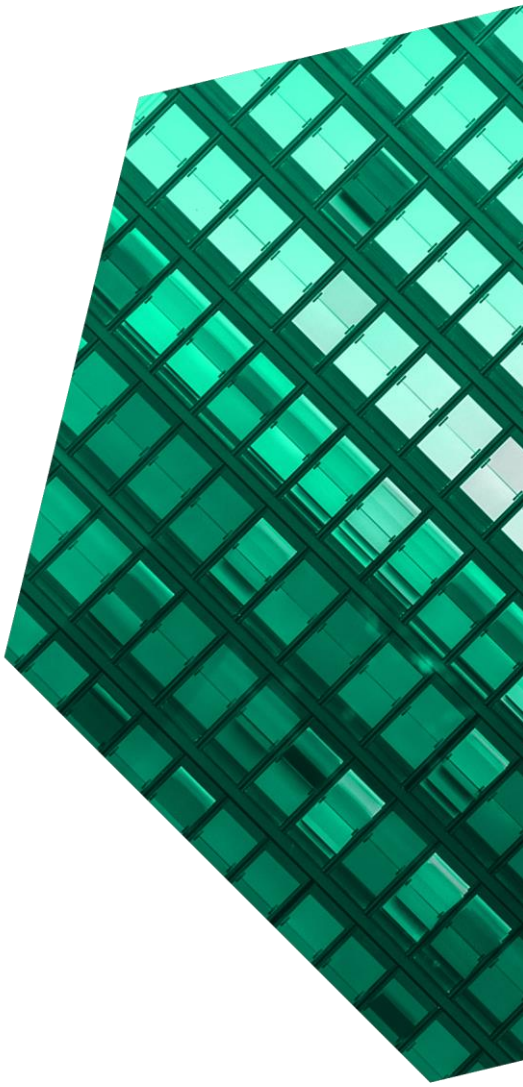
The Total Economic Impact™ Of Microsoft Security

Improved Security And Cost Savings Enabled By Microsoft Security (Security, Compliance, And Identity Management Solutions)

FEBRUARY 2023

Table Of Contents

Consulting Team: Jonathan Lipsitz
Casey Sirotnak



Executive Summary

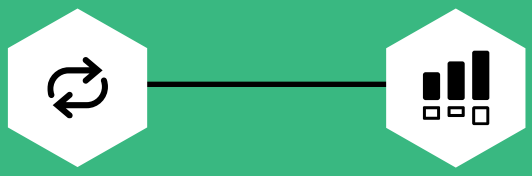
Companies of all sizes and industries are at increased risk of security breaches across multiple vectors, including external and internal actors and compliance violations. Many of these companies are finding that past approaches integrating point solutions led to security gaps as well as too much cost and effort to maintain and improve. Microsoft's suite of threat protection (including SIEM), compliance, and identity solutions natively work together, providing the necessary security without additional cost and complexity.

Microsoft Security includes solutions across six product families designed to manage threat protection (including security information and event management [SIEM]), compliance, and identity.[1] They easily and natively integrate with each other to protect a company's infrastructure and devices. The goal is to provide the necessary security without the added cost and effort of integrating point security solutions and centralize signals and management to improve the overall security posture. Microsoft refers to this as simplified, comprehensive protection to secure more with less.

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 Security solutions.[2] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Microsoft Security on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed five representatives and surveyed 361 respondents with experience using Microsoft Security solutions. For the purposes of this study, Forrester aggregated the experiences of the interviewees and survey respondents and combined the results into a single composite organization with 10,000 employees and 20 IT security professionals.

KEY STATISTICS



Return on investment (ROI)
231%

Net present value (NPV)
$19.29M

Reduced likelihood of a breach
72%

Prior to using Microsoft Security solutions, interviewees and survey respondents noted how their organizations had continual problems creating and maintaining an adequate security posture and that their costs and administrative efforts were growing at an unsustainable pace. These limitations led to increased security, identity, and compliance risks, which impacted the IT organization, business users, and customers.

After the investment in Microsoft Security, the interviewees rationalized their IT security estate while improving the integration and ingestion of signals across more systems to improve security. Key results from the investment include reducing security license

costs and effort while improving the overall security posture and business productivity.

KEY FINDINGS

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

- **Improved security posture, reducing the likelihood of a breach by 72%.** The reduction in breaches covers a wide range of security threats protected with various Microsoft Defender solutions and Sentinel; compliance and privacy threats protected with Microsoft Purview and Priva; and identity threats protected by Microsoft Entra and Intune. Across all of these areas, the composite organization has an improved security posture, reducing the number of successful attacks and making it easier and faster to recover. Additionally, less downtime during breaches means business users continue to do their jobs. The reduction in breaches, combined with business users not being affected, is worth $5.2 million of the three-year study.
- **Vendor consolidation, reducing solution license and consumption costs by 25%.** The composite organization replaces solutions across many areas, including SIEM, endpoint management, single sign-on (SSO), compliance, and threat detection. This study uses the $21 per-user-per-month uplift from the Microsoft 365 E3 to E5 cost as a proxy for the cost of the Microsoft licenses and consumption costs for Microsoft Sentinel and Defender for Cloud. The $21 uplift represents a 25% reduction in what the composite organization previously spends. The total value over the life of the study is $2 million.
- **Affected IT and security teams increasing efficiencies by 50%.** The composite organization's IT and security team benefits from the ease of integration, management, and remediation with Microsoft Security. The composite organization would have to grow security staffing by 50% to achieve the same level of security with point solutions that it achieves with Microsoft Security. In addition to security and IT team savings, internal audit effort is reduced by 22%. The additional headcount not added costs an additional $2.6 million over three years.
- **Business users increasing productivity by, on average, 1 hour per week.** More time available to get work done is taken as a proxy for improved business outcomes because the value someone adds should, at a minimum, be equal to what they are paid. Basic activities, such as easier SSO and device onboarding, save 15 minutes per week. Across a broader range of activities, business users at the composite organization save upwards of 2 hours per week and time to market for a new product is reduced by 20% because better collaboration is enabled. The

"User adoption of Microsoft Security solutions is very easy because people are familiar with Microsoft tools. Additionally, everything works well together, and it brings down our costs."

Global technical lead, professional services

Reduced security license costs

25%

financial model assumes 1 additional hour of productive work per week, which is worth $17.9 million over the life of the study.

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

- **Improved employee satisfaction.** Interviewees and nearly half of the survey respondents said that employee satisfaction is higher because Microsoft Security solutions made it easier for them to collaborate and create value in their jobs. Improved job satisfaction translated into lower attrition rates, which could be very valuable to an organization.
- **Better external collaboration.** Microsoft Security helped the interviewees' and survey respondents' companies collaborate securely with external parties in addition to the previously discussed employee collaboration. This included partners, suppliers, and customers, and the last category can contribute to improved customer satisfaction.
- **Better vendor customer service.** Working with fewer or a single vendor made it easier for the interviewees' companies to get the engineering and customer support they needed from security vendors. Interviewees said that they had close relationships with Microsoft, which helped them roll out better security faster and contributed to IT time savings.

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

- **Internal effort costs $1.0 million.** The internal effort includes a nine-month initial rollout, training the relevant IT and security teams, and ongoing "keeping the lights on" activities.
- **External costs total $7.4 million.** The highest cost is the $21 per-user-per-month Microsoft 365 E3 to E5 uplift that is used as a proxy for the Microsoft Security license costs for the various security, compliance, and identity solutions, including Microsoft Sentinel. There is also upfront professional services to help implement and integrate Microsoft Security, as well as ongoing professional services primarily around security operations center (SOC) management.

The financial analysis, which is based on the interviews and survey, found that a composite organization experiences benefits of $27.66 million over three years versus costs of $8.37 million, adding up to a net present value (NPV) of $19.29 million and an ROI of 231%.

> **"Microsoft Security helps us deal with the massive shortage of security professionals available for hire, better support the business, and keep costs under control."**
>
> *Enterprise infrastructure director, beverage distributor*

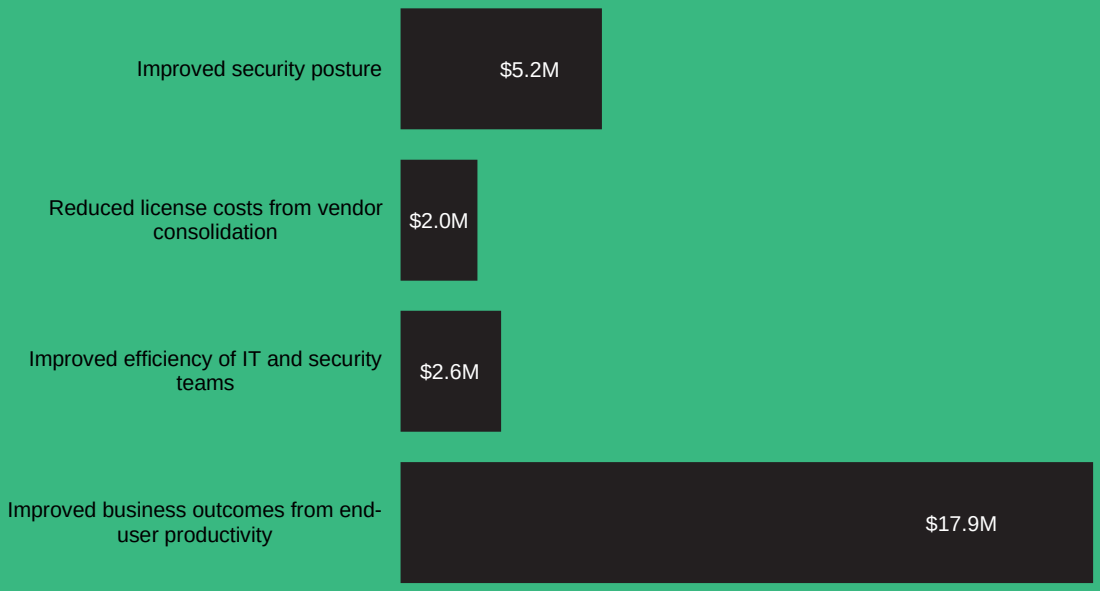
ROI
231%

BENEFITS PV
$27.66M

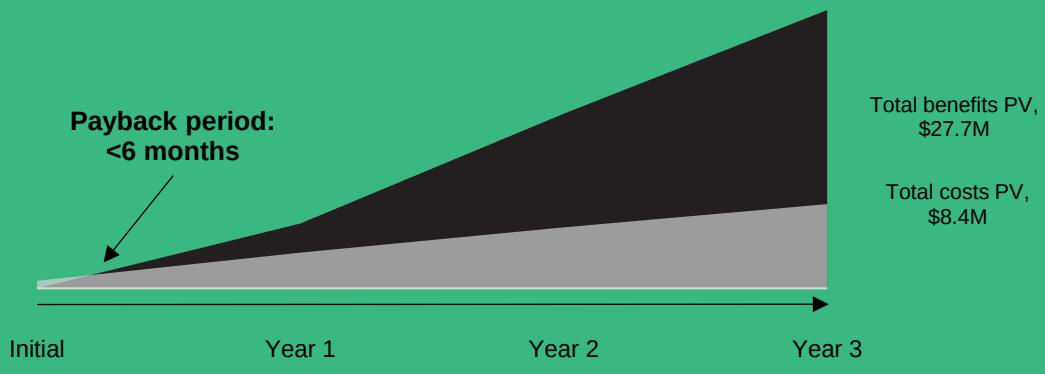
NPV
$19.29M

PAYBACK
<6 months

Benefits (Three-Year)



Financial Summary



TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews and survey, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in Microsoft Security.

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 Security 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.

DISCLOSURES

Readers should be aware of the following:

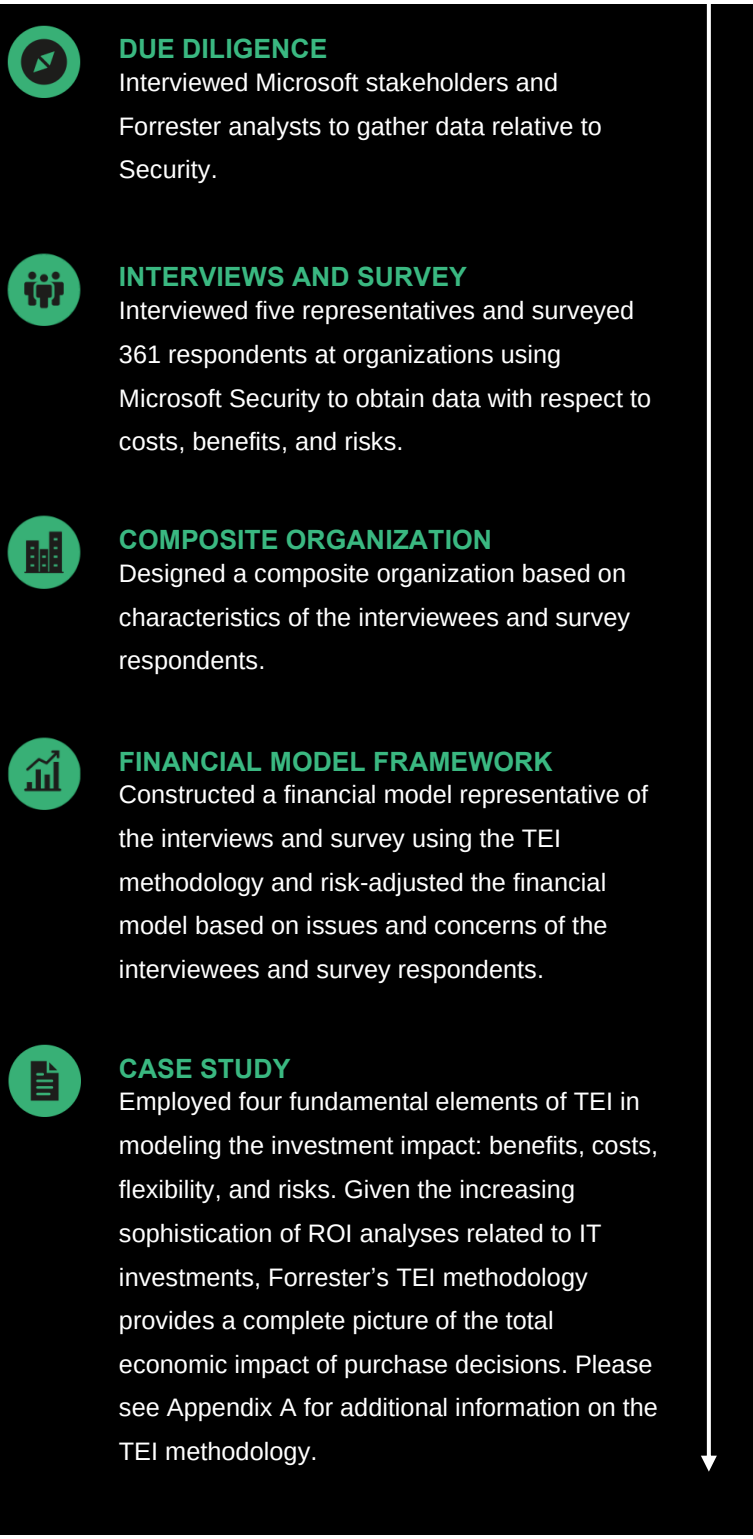
This study is commissioned by Microsoft and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

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

Microsoft reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.

Microsoft provided the customer names for the interviews but did not participate in the interviews.

Forrester fielded the double-blind survey using a third-party survey partner.



The Microsoft Security Customer Journey

Drivers leading to the Microsoft Security investment

KEY CHALLENGES

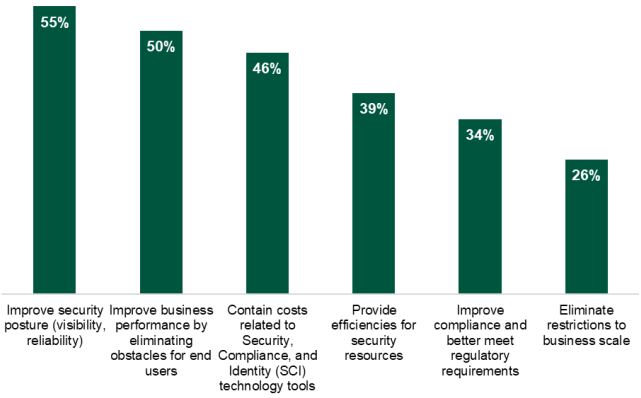
Forrester interviewed five representatives and surveyed 361 respondents with experience using Microsoft Security at their organizations. For more details on these individuals and the organizations they represent, see Appendix B.

Before moving to Microsoft Security, interviewees' organizations used a collection of point solutions for security, compliance, and identity. Additionally, there were solution gaps because of budget and labor constraints. This resulted in too much effort and cost, as well as security gaps due to a lack of integration and incomplete coverage.

Both interviewees and survey respondents noted how their organizations struggled with common challenges, including the following:

- **Prior solutions resulted in increased complexity and associated rising costs.** Interviewees reported that their prior point solution integration approaches required too much effort to set up and maintain the necessary integrations. Additionally, multiple point solutions required more effort to identify and remediate threats. Interviewees also said that they were spending too much on security solution licenses, and those who already had E5 licenses were being asked by CFOs why they were paying for redundant capabilities.
- **It was difficult to respond to the increasing complexity of security threats and compliance requirements.** Vulnerabilities and attacks became more complex, and interviewees said that meeting these threats required better integration and the aggregation of signals across as many systems as possible. The VP and CISO at the financial services organization said that their prior SIEM solution was only ingesting signals from 60% of the systems and that now with Sentinel, they are above 90%.
- **Enabling the business and user productivity was exceedingly difficult with the prior solutions.** All interviewees stressed that they want IT and security to be seen as business enablers rather than as an impediment to collaboration and innovation. Their prior security solutions made it too difficult for employees to collaborate and were a cause of major frustration.

What goals/challenges did your organization hope to address?



Base: 361 decision-makers responsible for security
Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, September 2022

"When I was hired, I inherited a security estate with a lot of best-in-breed point solutions. There seemed to be a lot of opportunity to simplify our security stack. Since I already had E5 licenses, it made sense to go this direction. We have a small IT team, so simplification and cost control are very important."

VP and CISO, financial services

INVESTMENT OBJECTIVES

The interviewees and survey respondents searched for a solution that could:

- Strengthen the security posture through tighter integration across various components and ingest signals from as many sources as possible.
- Be quickly deployed to achieve security benefits faster.
- Control costs through license rationalization.
- Reduce the level of effort because of difficulties in hiring IT security professionals and not require a lot of additional training.

COMPOSITE ORGANIZATION

Based on the interviews and survey, 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 five interviewees and the 361 survey respondents, and it is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The composite organization is a global, business-to-business organization with 10,000 full-time workers. It currently employs 20 security and IT professionals that interact with Microsoft Security solutions on a regular basis.

Deployment characteristics. The composite organization previously followed a point solution integration approach that tied together security, compliance, and identity solutions generally termed "best in class." It also had Microsoft 365 E5 licenses, so it explored moving to the solutions included in the E5 license. It now uses Microsoft solutions across all six product families: Microsoft Defender, Microsoft Sentinel, Microsoft Entra, Microsoft Intune, Microsoft Purview, and Microsoft Priva. Its SOC is built on Microsoft Sentinel, and there is a professional services contract to do threat detection as part of the SOC operation.

The composite organization took a good-better-best approach to implementing Microsoft Security. "Good" consisted of getting better visibility across all systems and reactive response to threats. "Better" consisted of proactive management to address vulnerabilities before an active attack. "Best" consisted of putting more automation and cross-vector protections in place.

Key Assumptions

- **10,000 employees**
- **20 IT and security professionals using Microsoft Security solutions**
- **Using solutions across all six product families**

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits						
Atr	Improved security posture	$1,129,950	$2,620,279	$2,673,311	$6,423,540	$5,201,245
Btr	Reduced license costs from vendor consolidation	$798,000	$798,000	$798,000	$2,394,000	$1,984,508
Ctr	Improved efficiency of IT and security teams	$997,500	$1,047,375	$1,099,744	$3,144,619	$2,598,671
Dtr	Improved business outcomes from end-user productivity	$4,160,000	$8,736,000	$9,152,000	$22,048,000	$17,877,686
	Total benefits (risk-adjusted)	$7,085,450	$13,201,654	$13,723,055	$34,010,159	$27,662,110

IMPROVED SECURITY POSTURE

Evidence and data. Microsoft Security solutions spanning the six product families improved the security posture across a wide range of areas, including better visibility across the IT estate, reduced mean time to detect (MTTD) and mean time to remediate (MTTR), and fewer breaches. Companies' rollout roadmaps varied greatly based on their unique challenges — some began with security threats, some with identity, and some with compliance. Interviewees and survey respondents shared the following examples of how their security postures improved:

- The VP and CISO at a financial services organization said: "Our dwell time is probably 10x less now, although it is hard to know because prior to Microsoft, we did not have good threat detection and visibility capabilities. Now, our capabilities are much stronger using the Defender products and Intune. Additionally, our compliance is improving with Purview."
- The VP and CISO also shared that, since going live in January of 2021, Microsoft Security has helped them get from a 60% "healthy" score to 98%. They estimate that the likelihood of a breach was reduced from once every two years to once every seven years — a 72% improvement.
- The group head of enterprise IT and information security at a retailer shared an example of Defender preventing a password-cracking attack that could have led to the entire network being taken over and millions of dollars in damages.
- At the beverage distributor, compliance improved in the insider-risk area. Microsoft Purview flagged a C-suite employee doing a mass download before announcing they were quitting.
- The global technical lead at the professional services organization noted their organization implemented full identity lifecycle management to deactivate unused accounts, and that they used "the intelligence in Microsoft Graph to identify risky user activities." They explained that "all the security exists in the background without hurting the user experience."
- The principal technologist at an agriculture company stressed the importance of consistency

and the ability to automatically apply security policies to new cloud resources. This was a big part of the reason they moved from on-prem to cloud infrastructure.

- Interviewees' estimates of the cost of a breach ranged from $500,000 to $10 million and up.
- Two-thirds of the survey respondents reported "fewer data breaches/incidents" after moving to Microsoft Security. Additionally, the total cost of a breach was reduced by 33%.
- The survey also found that "noncompliance events related to data retention policies" were reduced by 16.8%.

"Many of the things we do with Microsoft's security solutions we could have done with other vendors, but it would have taken 50% longer with other solutions, which is more time that we would have been at risk."

VP and CISO, financial services

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

- Before Microsoft Security, the composite experiences an annual average of 3.1 material security breaches at an average per-breach cost of $750,000.[3]
- After completing the Microsoft Security deployment, the likelihood of a breach is reduced by 72%. Three-quarters of this benefit is realized in Year One as the rollout is finalized and the composite organization moves through the good-better-best progression.
- Breaches negatively impact 33% of the composite's 10,000 total employees at a time with the average breach-related downtime being 4 hours.
- The average employees' fully burdened hourly rate (including salary, benefits, and payroll taxes) is $40, growing 5% annually.

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

- The prior frequency of breaches and the total cost of a breach.
- Which Microsoft Security solutions are implemented and an IT security organization's maturity as it relates to threat detection and remediation.
- The number of employees affected by a breach and their average fully burdened cost.

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 $5.2 million.

Improved Security Posture

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Average annual number of material breaches before Microsoft Security	Forrester research	3.1	3.1	3.1
A2	Average cost of a breach	Forrester research	$750,000	$750,000	$750,000
A3	Reduced likelihood of a breach with Microsoft Security	Assumption	54%	72%	72%
A4	Subtotal: Reduced risk of a major security breach	(A1*A4)-(A2*A4)	$1,255,500	$1,674,000	$1,674,000
A5	Total employees	Composite	10,000	10,000	10,000
A6	Average percent of employees impacted	Forrester research	33%	33%	33%
A7	Average downtime per employee per breach (hours)	Forrester research	4	4	4
A8	Average fully burdened hourly cost	TEI standard	$40.00	$42.00	$44.00
A9	Subtotal: Reduced employee downtime during a breach	A1*A3*A5*A6*A7*A8	$883,872	$1,237,421	$1,296,346
At	Improved security posture	A4+A9	$2,139,372	$2,911,421	$2,970,346
	Risk adjustment	↓10%			
Atr	Improved security posture (risk-adjusted)		$1,129,950	$2,620,279	$2,673,311
	Three-year total: $6,423,540			**Three-year present value: $5,201,245**	

REDUCED LICENSE COSTS FROM VENDOR CONSOLIDATION

Evidence and data. Moving from a point-solution-integration approach to Microsoft Security stacks lowered license costs for interviewees and survey respondents. For those who already had Microsoft 365 E5 licenses, the savings could be very large if considered a sunk cost for the business case. Interviewees and survey respondents shared the following examples of how they reduced license costs:

- The VP and CISO at the financial services organization noted they retired other SIEM, endpoint, SSO, compliance, and threat detection solutions. Taken all together, these were costing approximately $1 million per year and the VP and CISO estimated that they saved 25% on license costs since moving to Microsoft Security.
- The enterprise infrastructure director at the beverage distributor said that they saved $250,000 a year in the managed detection response (MDR) and SIEM categories.
- The principal technologies noted their agriculture company saved money by turning off other threat detection solutions and using Microsoft for container security.
- The survey found that security license costs were reduced by 13% and necessary hardware costs were reduced by 10%. Additionally, associated management costs were reduced by 20%.

> **"Moving everything to Azure Active Directory will save us license costs across many areas and allow us to decommission applications that we have built."**
>
> *Principal technologist, agriculture*

Modeling and assumptions. For the financial analysis as applied to the composite organization, Forrester assumes the Microsoft Security license costs described in the Costs section of the study are 25% less than the prior point solution license costs. (Note: If a company already has Microsoft 365 E5 licenses and considers that a sunk cost, the savings is the entire prior license spend.)

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

- The prior approach to selecting and integrating security solutions.
- The extent to which an organization consolidates onto Microsoft's stack.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $2.0 million

Reduced License Costs From Vendor Consolidation

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	License costs eliminated/reduced by Microsoft 365 E5	F3/75%-F3	$840,000	$840,000	$840,000
Bt	Reduced license costs from vendor consolidation	B1	$840,000	$840,000	$840,000
	Risk adjustment	↓5%			
Btr	Reduced license costs from vendor consolidation (risk-adjusted)		$798,000	$798,000	$798,000
	Three-year total: $2,394,000			**Three-year present value: $1,984,508**	

IMPROVED EFFICIENCY OF IT AND SECURITY TEAMS

Evidence and data. Improved team efficiency is the area where interviewees saw the greatest "do more with less" impact. They stressed that even if money was not an issue, it was nearly impossible to recruit and retain enough IT security professionals. Interviewees and survey respondents shared the following examples of how they could provide the same or better security without having to significantly grow the size of their IT and security teams:

- The VP and CISO at the financial services organization explained that because of Microsoft Security, they kept the security team the same size despite the employee headcount nearly doubling in the past 2.5 years. They estimated that the current team of eight would need to grow to twelve without Microsoft Security.
- The agriculture company used automation to reduce the amount of security-related work. The principal technologies noted: "I can protect everything in Azure with three clicks. It's pretty awesome. If someone creates a new subscription, all the security policies are automatically applied." They saved 2 hours in configuration effort for each new Azure subscription.
- The principal technologist at the agriculture company also said that Microsoft Security saved money and effort in application development because "implementing Azure policies forces developers to code properly. You can fix things easily when in development compared to fixing them afterwards in production. It's a couple of hundred dollars in testing versus $5,000 to $10,000 once in production."
- At the beverage distributor, the enterprise infrastructure director talked about the difficulty of hiring security professionals and how Microsoft Security helped get everything done with a small team: "Microsoft is building intelligence into all of their products and leveraging their scale so that if one of their customers experiences an attack, our instance knows to look for it. We logged 135 million events in the last ten days. The only way for a small team like mine to manage that is through the AI built into Microsoft solutions. It distilled the millions of events down to 10 that needed to be addressed. That is what doing more with less is." The interviewee estimated that their IT team of 15 with no dedicated security people would need to grow by 50% without Microsoft Security.
- The global technology lead at the professional services organization shared an example of a solution built using Microsoft Security solutions to provide guest access. They estimated that they would have spent approximately $1 million to build and roll out a solution using other tools, several times more than what they spent leveraging existing Microsoft capabilities.
- The group head of enterprise IT and information security at the retailer estimated that their team of four IT security people would need to grow to somewhere between 12 and 18 people if they were not using Microsoft Security: "We are so efficient because of the tight integration between all the Microsoft Security solutions and the productivity solutions, such as Outlook and Teams. Everything comes into Sentinel and we use machine learning to deal with false positives."
- The survey found that 59% less time was spent on event detection and 52% less on event remediation.

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

- There are 20 FTEs on IT and IT security teams that interact with Microsoft Security solutions.

- Without Microsoft Security, the team size would need to increase by 50% to provide the same level of security and service to the organization.
- The average fully burdened cost across the IT and security teams is $140,000, increasing 5% per year.

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

- The prior size of the relevant IT and security teams.
- The extent of consolidation onto Microsoft Security solutions and the degree of automation, artificial intelligence, and machine learning applied.
- The fully burdened cost for these resources.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $2.6 million.

"The best example of doing more with less is our SOC. We have a 24/7 operation with only four people and a $250,000 managed services contract. Without Microsoft's XDR solution and everything working in Sentinel, I would need 12 to 16 people working in the SOC."

Group head of enterprise IT and information security, retail

Improved Efficiency Of IT And Security Teams

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Affected IT and security teams FTEs	Composite	20	20	20
C2	Additional headcount savings because of Microsoft Security	C1*50%	10	10	10
C3	Annual fully burdened cost	TEI standard	$140,000	$147,000	$154,350
C4	Productivity capture	TEI standard	75%	75%	75%
Ct	Improved efficiency of IT and security teams	C2*C3*C4	$1,050,000	$1,102,500	$1,157,625
	Risk adjustment	↓5%			
Ctr	Improved efficiency of IT and security teams (risk-adjusted)		$997,500	$1,047,375	$1,099,744
	Three-year total: $3,144,619			**Three-year present value: $2,598,671**	

IMPROVED BUSINESS OUTCOMES FROM END-USER PRODUCTIVITY

Evidence and data. Creating secure and compliant environments must always be balanced with providing business users with the access and tools they need to be productive. Improved business outcomes could manifest in many ways, such as better user productivity, faster time to market, and increased revenues. Interviewees stressed both the importance and benefits of providing security in ways that improved business productivity and outcomes, including the following examples:

- The VP and CISO at the financial services organization explained that moving to a Zero Trust architecture made employees more productive while also securing important corporate information: “It is not the reason we moved to Microsoft, but the user experience is much better. App response times are much faster than on legacy VPNs. We used to have groups complain a lot. It’s been a big win for security and a big win for user experience.”
- The VP and CISO also shared an example of implementing security at a new headquarters building being built out: “We don’t have to build LANs, which makes everything much simpler and faster to implement. Users have the same experience whether in the office or at home.”
- The enterprise infrastructure director at the beverage distribution company said that business users are more efficient from simple things such as SSO. They estimated that each employee saved 15 minutes per week from better SSO and device onboarding.
- The global technology lead at the professional services firm said that Microsoft Security improved collaboration through better integration with Microsoft Teams and Outlook and by creating intuitive user experiences. A project using Microsoft Security solutions to provide guest access made it easier and faster for employees to collaborate with customers and suppliers.
- Microsoft Security led to increased revenues for 57% of survey respondents.
- Survey respondents also said that time to market for a new product was reduced by 20%.
- The survey found that employees saved, on average, 100 hours per year after moving to Microsoft Security.

> **“Moving to Microsoft creates a lot of new opportunities for us to improve the business. We have made it easier for people to work from home and are now looking at expanding into new areas such as bringing manufacturing systems online.”**
>
> *Enterprise infrastructure director, beverage distributor*

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

- Improved employee productivity is used as a proxy for various forms of improved business outcomes since employees should create value that is, at a minimum, equal to their compensation.
- Each employee saves, on average, 1 hour per week from things such as improved SSO; less time on activities such as onboarding devices; better system performance compared to VPN access; and better support of collaboration tools and processes. Half of this benefit is realized in

Year 1 as the rollout is complete and the organization moves through the good-better-best progression.

- The average hourly fully burdened cost across all 10,000 employees is $40 and this increases by 5% per year.
- A 50% productivity capture is applied.

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

- Prior security systems and processes in place.
- The type of employees and the nature of their work.
- The average fully burdened cost of employees.

Results. To account for these risks and because user productivity may be viewed as a softer benefit, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $17.9 million. It is worth noting that even if this benefit is discounted 100%, the move to Microsoft Security still had a positive ROI for the composite organization.

Improved Business Outcomes From End-User Productivity

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Annual time savings per employee (hours)	Y1: 1 hour*52 weeks*50% Y2 and Y3: 1 hour*52 weeks	26	52	52
D2	Average fully burdened hourly cost	A8	$40	$42	$44
D3	Productivity capture	TEI standard	50%	50%	50%
Dt	Improved business outcomes from end-user productivity	A5*D1*D2*D3	$5,200,000	$10,920,000	$11,440,000
	Risk adjustment	↓20%			
Dtr	Improved business outcomes from end-user productivity (risk-adjusted)		$4,160,000	$8,736,000	$9,152,000
	Three-year total: $22,048,000			**Three-year present value: $17,877,686**	

UNQUANTIFIED BENEFITS

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

- **Improved employee satisfaction.** Interviewees and nearly half of the survey respondents reported that their employees were happier after the move to Microsoft Security. There were several reasons, including better user experiences, less user frustration, improved work-from-home capabilities, and better collaboration/interactions with colleagues. For survey respondents who measured employee satisfaction, the average improvement was 16.7%.
- **Better external collaboration.** Microsoft Security made it easier for the interviewees' and survey respondents' companies to work with their customers, partners, and suppliers. This resulted in more innovation, faster time to market, and improved customer satisfaction. Survey respondents said that customer satisfaction increased by 20.2%.
- **Better vendor customer service.** Interviewees all said that working with fewer vendors was easier and that Microsoft provided very good customer service and support. This included co-engineering and support on new security-related initiatives.

FLEXIBILITY

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

- **Expanding into additional Microsoft Security solution families.** Each interviewee had a unique roadmap matched to their most pressing security issues. They all also had plans to investigate or roll out additional Microsoft Security solutions. For many, compliance was the area that they were moving into as part of a second- or third-phase deployment.
- **Rolling out Microsoft's enhancements.** Interviewees said that Microsoft is continually innovating to bring new security-related solutions and features to market. These were evaluated and implemented based on the fit to an individual organization's needs.

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A). None of these flexibility benefits were included in the financial model.

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Etr	Internal effort	$495,000	$195,800	$205,425	$215,531	$1,111,756	$1,004,705
Ftr	External costs	$262,500	$2,856,000	$2,856,000	$2,856,000	$8,830,500	$7,364,949
	Total costs (risk-adjusted)	$757,500	$3,051,800	$3,061,425	$3,071,531	$9,942,256	$8,369,654

INTERNAL EFFORT

Evidence and data. Interviewees generally said that implementing Microsoft Security was easier than other solutions because of the native integrations across solution families. Smaller companies described the process as “a few flips of switches.” For larger companies, the implementation ranged from two to 10 months with a multidisciplinary team including IT, IT security, compliance, and business users. Some training for IT and security staff took place during this time.

Ongoing effort for “keeping the lights on” activities was also described as relatively small. The level of effort ranged from a few hours per week and 2 FTEs, depending on company size, the breadth of Microsoft Security solutions deployed, and the overall IT estate complexity.

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

- The initial implementation lasts nine months and requires 4 FTEs.
- Ongoing solution management requires 1.25 FTEs.
- Each of the 20 IT and security employees interacting with Microsoft Security solutions receives 20 hours of training during implementation and 2 hours in each subsequent year.
- The average fully burdened cost across the IT and security teams is $140,000.

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

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

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.0 million.

Internal Effort						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Implementation	4 FTEs*9 months*$13,000	$420,000			
E2	Ongoing solution management	1.25 FTEs*C3		$175,000	$183,750	$192,938
E3	Training	Initial: 20 FTEs*20 hours*$75 Y1 to Y3: 20 FTEs*2 hours*$75	$30,000	$3,000	$3,000	$3,000
Et	Internal effort	E1+E2+E3	$450,000	$178,000	$186,750	$195,938
	Risk adjustment	↑10%				
Etr	Internal effort (risk-adjusted)		$495,000	$195,800	$205,425	$215,531
	Three-year total: $1,111,756			**Three-year present value: $1,004,705**		

EXTERNAL COSTS

Evidence and data. External costs primarily consisted of Microsoft licenses and consumption charges for Microsoft Sentinel and Defender for Cloud. Ninety percent of survey respondents accessed the majority of the Microsoft Security solutions through an enterprise Microsoft 365 E5 license. Interviewees also reported using some professional services for implementation, and the group head of enterprise IT and information security at the retailer said they were using ongoing professional services for tier-one SOC support.

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

- $250,000 is spent on deployment professional services. This is in addition to the free support that Microsoft sometimes provides.
- A $200,000 annual contract for SOC tier-one support.
- The $21 per-user-per-month difference in list price between the Microsoft 365 E3 and E5 licenses is used as a proxy for the costs of the Microsoft security, compliance, and identity solutions, including consumption charges for Microsoft Sentinel and Defender for Cloud. The total costs used in this study are consistent with prior TEI studies looking at Microsoft's security solutions (see Appendix C). The reader is encouraged to speak with their Microsoft account manager or partner to understand what their actual costs will be.

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

- The overall size of the organization.
- Any negotiated discounts on licenses.
- The number of professional services required.

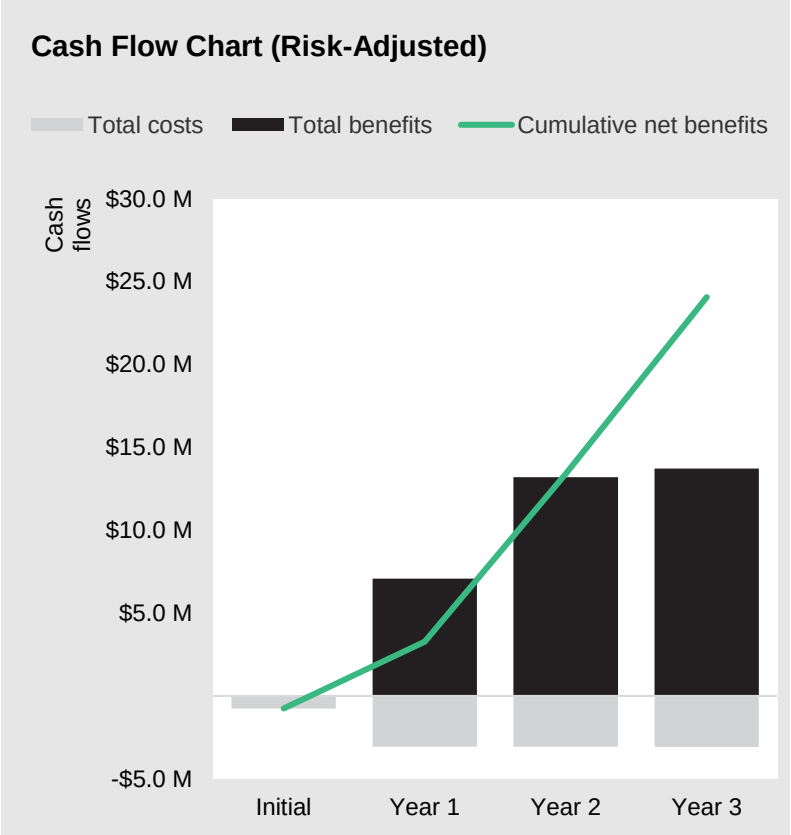
Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $7.4 million.

External Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Professional services	Assumption	$250,000	$200,000	$200,000	$200,000
F2	Microsoft 365 E5 license costs allocated to security, compliance, and identity solutions	A5*($57-$36)*12 months	$0	$2,520,000	$2,520,000	$2,520,000
Ft	External costs	F1+F2	$250,000	$2,720,000	$2,720,000	$2,720,000
	Risk adjustment	↑5%				
Ftr	External costs (risk-adjusted)		$262,500	$2,856,000	$2,856,000	$2,856,000
	Three-year total: $8,830,500			**Three-year present value: $7,364,949**		

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS



The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, 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	($757,500)	($3,051,800)	($3,061,425)	($3,071,531)	($9,942,256)	($8,369,654)
Total benefits	$0	$7,085,450	$13,201,654	$13,723,055	$34,010,159	$27,662,110
Net benefits	($757,500)	$4,033,650	$10,140,229	$10,651,524	$24,067,902	$19,292,456
ROI						231%
Payback period						<6 months

Appendix A: Total Economic Impact

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

TOTAL ECONOMIC IMPACT APPROACH

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

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

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

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

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

PRESENT VALUE (PV)

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

NET PRESENT VALUE (NPV)

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

RETURN ON INVESTMENT (ROI)

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

DISCOUNT RATE

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

PAYBACK PERIOD

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

Appendix B: Interview And Survey Demographics

Interviews

VP and CISO	Financial services	North America	1,500
Principal technologist	Agriculture	North America	10,000
Enterprise infrastructure director	Beverage distributor	North America	1,700
Global technical lead	Professional services	Global, NA HQ	300,000
Group head of enterprise IT and information security	Retail	Global, UK HQ	50,000

Survey Demographics

"Please indicate the region your firm/organization is headquartered in."

Base: 361 decision-makers responsible for security
Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, September 2022

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

Base: 361 decision-makers responsible for security
Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, September 2022

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

Industry	
Retail	7%
Transportation and logistics	7%
Consumer product goods and/or manufacturing	6%
Technology and/or technology services	6%
Financial services	5%
Manufacturing and materials	5%
Media	5%
Electronics	5%
Telecommunications services	5%
Business or professional services	4%
Energy, utilities, or waste management	4%
Government	4%
Chemicals and/or metals	4%
Construction	4%
Property management	4%
Consumer services	4%
Insurance	4%
Healthcare	4%
Higher education	3%
Advertising and/or marketing	3%
Quick-service restaurant/food industry	2%
Travel and entertainment	2%
Agriculture, food, and/or beverage	1%
Gaming (e.g., online casinos, fantasy sports, lotteries)	1%
Legal services	1%

Base: 361 decision-makers responsible for security
Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, September 2022

Appendix C: Other TEI Studies On Microsoft Security Solutions

"The Total Economic Impact™ Of Microsoft Cloud App Security," a commissioned study conducted by Forrester Consulting on behalf of Microsoft, March 2020.

"The Total Economic Impact™ Of Securing Apps With Microsoft Azure Active Directory," a commissioned study conducted by Forrester Consulting on behalf of Microsoft, August 2020.

"The Total Economic Impact™ Of Microsoft Azure Sentinel," a commissioned study conducted by Forrester Consulting on behalf of Microsoft, November 2020.

"The Total Economic Impact™ Of Microsoft Defender for Cloud," a commissioned study conducted by Forrester Consulting on behalf of Microsoft, February 2021.

"The Total Economic Impact™ Of Microsoft 365 E5 Compliance," a commissioned study conducted by Forrester Consulting on behalf of Microsoft, June 2021.

"The Total Economic Impact™ Of Microsoft Azure Network Security," a commissioned study conducted by Forrester Consulting on behalf of Microsoft, October 2021.

"The Total Economic Impact™ Of Zero Trust Solutions From Microsoft," a commissioned study conducted by Forrester Consulting on behalf of Microsoft, December 2021.

"The Total Economic Impact™ Of Microsoft 365 Defender," a commissioned study conducted by Forrester Consulting on behalf of Microsoft, April 2022.

"The Total Economic Impact™ Of Microsoft SIEM And XDR," a commissioned study conducted by Forrester Consulting on behalf of Microsoft, August 2022.

"The Total Economic Impact™ Of Microsoft Entra," a commissioned study conducted by Forrester Consulting on behalf of Microsoft, February 2023.

Appendix D: Endnotes

[1] The Microsoft Security product families include Microsoft Defender and Microsoft Sentinel for security; Microsoft Purview and Microsoft Priva for compliance and privacy; and Microsoft Entra and Microsoft Intune for identity and management.

[2] 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.

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


FORRESTER®