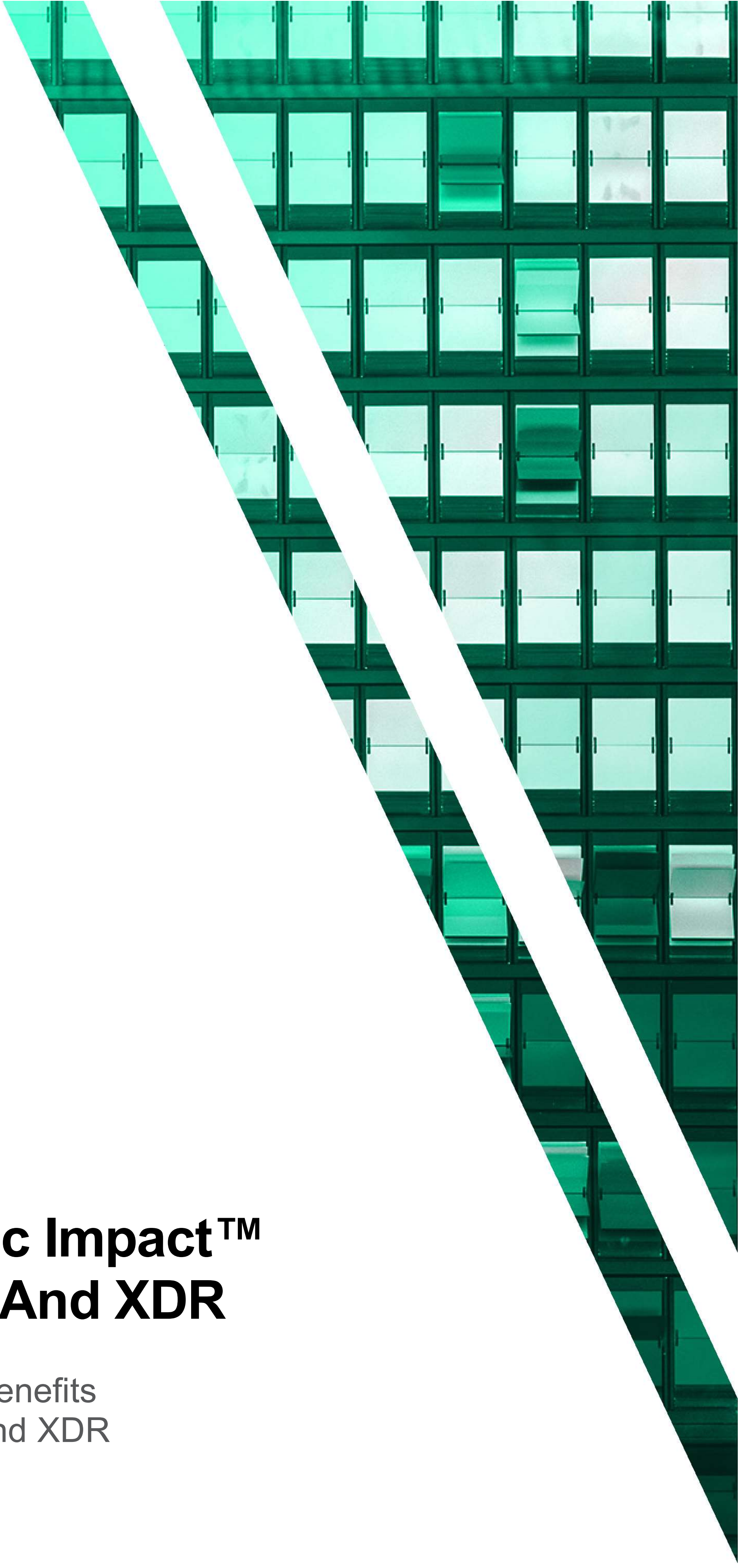
FORRESTER®



The Total Economic Impact™ Of Microsoft SIEM And XDR

Cost Savings And Business Benefits
Enabled By Microsoft SIEM and XDR

AUGUST 2022

A FORRESTER TOTAL ECONOMIC IMPACT™ STUDY COMMISSIONED BY MICROSOFT

Table Of Contents

Consulting Team: Nick Mayberry

Executive Summary 1

The Microsoft SIEM And XDR Customer Journey 6

Key Challenges 6

Solution Requirements 7

Composite Organization 7

Analysis Of Benefits 9

Reduced Time Of Threat Investigation And Response 9

Improved Efficiency Of Other Security Professional Work 11

Reduced Cost Of Material Security Breaches......13

Improved Efficiency And Productivity Of Other Employees...14

Reduced Costs From Vendor Consolidation........16

Unquantified Benefits 18

Flexibility...19

Analysis Of Costs 20

Microsoft SIEM And XDR Fees 20

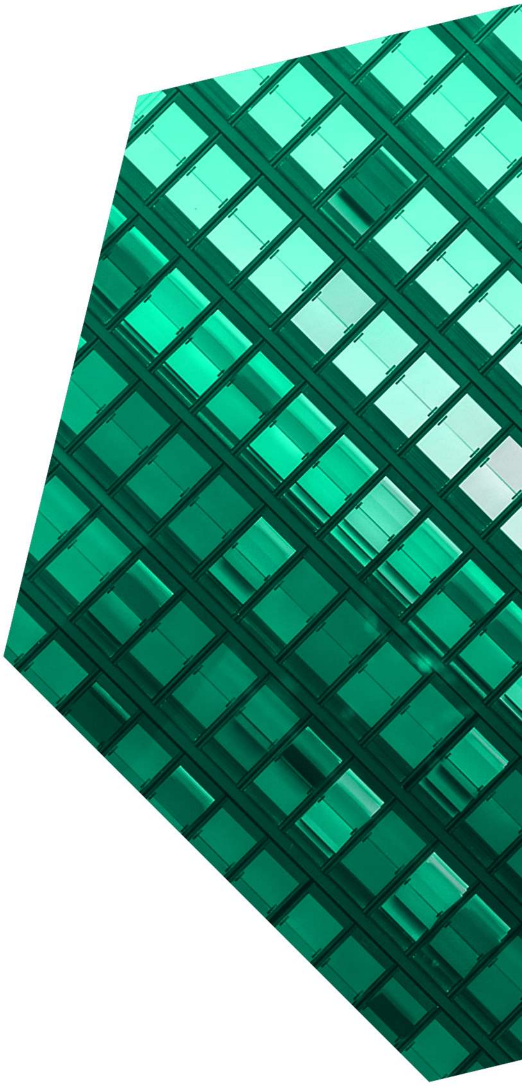
Cost Of Deployment And Implementation 22

Time Cost Of Training And Ongoing Management 23

Financial Summary 24

Appendix A: Total Economic Impact 25

Appendix B: Endnotes 26



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.

© Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on the best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies.

Executive Summary

> Organizations are realizing that past approaches to security tooling have failed both their security professionals and their overall security posture. The focus on best-of-breed point solutions reduces security professionals' ability to rapidly identify and respond to potential threats, while increasing IT spend and productivity costs to end users. Microsoft SIEM and XDR offers a natively integrated approach to security tooling, the costs of which are potentially already incorporated into existing Microsoft licenses.

Microsoft offers unified security information and event management (SIEM) and extended detection and response (XDR) tools aimed at providing security professionals with an integrated experience, preventing breaches across the entirety of an organization. SIEM and XDR combines Microsoft Sentinel, Microsoft 365 Defender, and Microsoft Defender For Cloud into an integrated suite of solutions protecting on-premises, multicloud, and hybrid environments. At the same time, Microsoft's integrated approach enables efficiencies for both security team workflows and IT budgets.

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

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four representatives with experience using Microsoft SIEM and XDR. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization with 8,000 total employees and 10 security professionals.

Prior to using Microsoft SIEM and XDR, interviewees' organizations lacked efficient means of identifying, investigating, and responding to potential threats. Prior best-of-breed tooling created added time costs to security professionals, budget costs to the organizations, and productivity costs to organizations' wider employee bases.

After the investment in Microsoft SIEM and XDR, the interviewees noted that they reduced their mean times to investigate and respond to threats, reduced the risk of a material security breach, enabled additional productivity for general employees, and reduced their IT organizations' spend on security point solutions.

KEY STATISTICS

Return on investment (ROI)
207%

Net present value (NPV)
$11.92M

Total benefits:

$17.68M

KEY FINDINGS

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

- **Reducing time to investigate threats by 65% and reducing time to respond to threats by 88%.** Microsoft SIEM and XDR's integrated approach to security threat investigation and response makes these workflows more efficient for the composite organization's security professionals. They no longer need to jump through multiple tools to identify threats, while security automation features further enhance response workflows.
- **Reducing the time to create a new workbook by 90% and the time to onboard new security professionals by 91%.** Microsoft SIEM and XDR's integrated approach makes additional security professional workflows more efficient as well. As SIEM logs are integrated throughout the suite of solutions, workbook creation is nearly automated, while a singular login enables new security professionals to onboard nearly 16 weeks faster.
- **Reducing the risk of a material breach by 60%.** With more efficient security investigation and response workflows, improved security response automation, and the increased ability to protect all computing environments, including multicloud protection, the composite reduces the risk of breaches with an annual impact of $1.6 million saved.
- **Improving productivity of other employees by almost 68,000 total hours annually.** Microsoft SIEM and XDR also prevents negative impacts to other employees from inefficient security processes. For example, the composite saves 4,000 hours annually thanks to IT professionals' new ability to self-serve regarding security updates and recommendations. It also enables remote security-based troubleshooting on employee machines and reduces the number of security agents running on them, saving nearly 64,000 hours annually in end-user productivity.
- **Saving almost $1.6 million annually from vendor consolidation.** The Microsoft SIEM and XDR investment also enables the composite to reduce the cost of its prior SIEM ($560,000), the associated on-premises infrastructure (over $360,000), three XDR point solutions ($192,000), and the ongoing labor cost to manage these ($480,000).

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

- **Improved visibility.** Microsoft SIEM and XDR's integration also improves the composite's visibility into its security environment, enabling a better cross-organizational understanding of its security posture and enabling it to perform better at penetration tests.
- **Improved compliance.** Microsoft SIEM and XDR also allows compliance teams to leverage self-service in their compliance checks and provides additional visibility into where customer data is flowing and how it is being used, enabling the composite to improve its compliance.
- **Improved IT asset management.** The composite also improves its IT asset management practices thanks to Microsoft SIEM and XDR's enablement of active asset discovery and visibility into groups of assets by function.
- **Microsoft support.** Lastly, the composite benefits from its relationship with Microsoft support, enabling it to provide feedback and early suggestions for feature requests, which would go on to improve the functionality of Microsoft SIEM and XDR.

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

- **Microsoft SIEM and XDR fees.** Microsoft SIEM and XDR is a combination of Microsoft 365 Defender, Microsoft Sentinel, and Microsoft Defender For Cloud. Each of these solutions is priced according to different metrics, which can be referenced fully in the Analysis Of Costs section.
- **Cost of deployment and integration.** The composite incurs partner costs associated with the deployment ($50,000) and implementation ($100,000) of Microsoft SIEM and XDR. Importantly, Microsoft's integrated SIEM and XDR tools require less time to deploy and implement, enabling a faster time-to-value of investment than otherwise possible.
- **Time cost of training and ongoing management.** The composite incurs time costs associated with training (three full days per security professional) and ongoing management (0.38 FTEs) for the three solutions in the Microsoft SIEM and XDR suite.

The representative interviews and financial analysis found that a composite organization experiences benefits of $17.68 million over three years versus costs of $5.76 million, adding up to a net present value (NPV) of $11.92 million and an ROI of 207%.

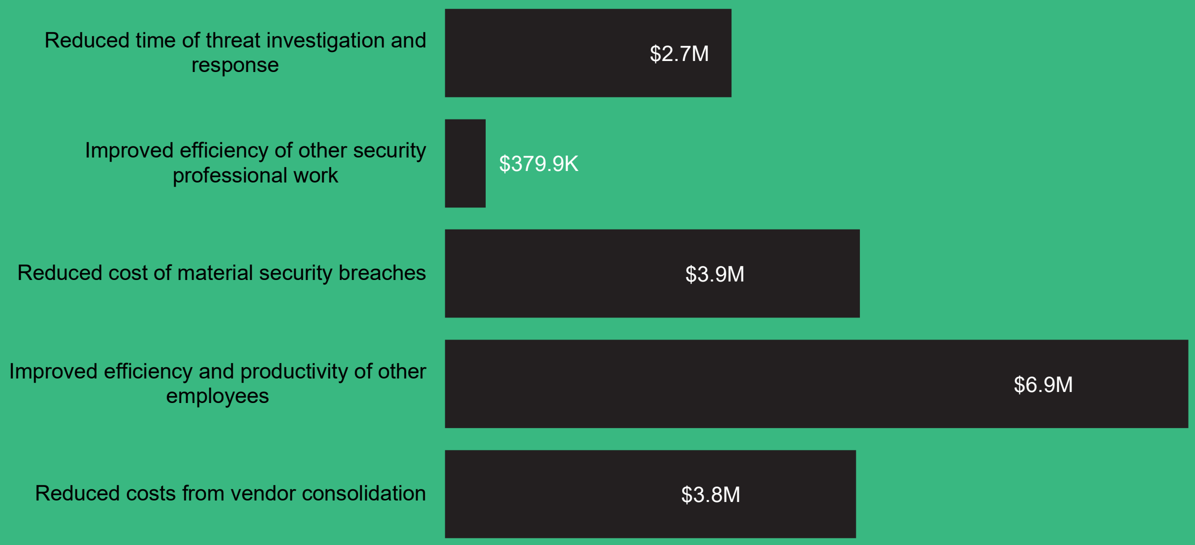
ROI
207%

BENEFITS PV
$17.68M

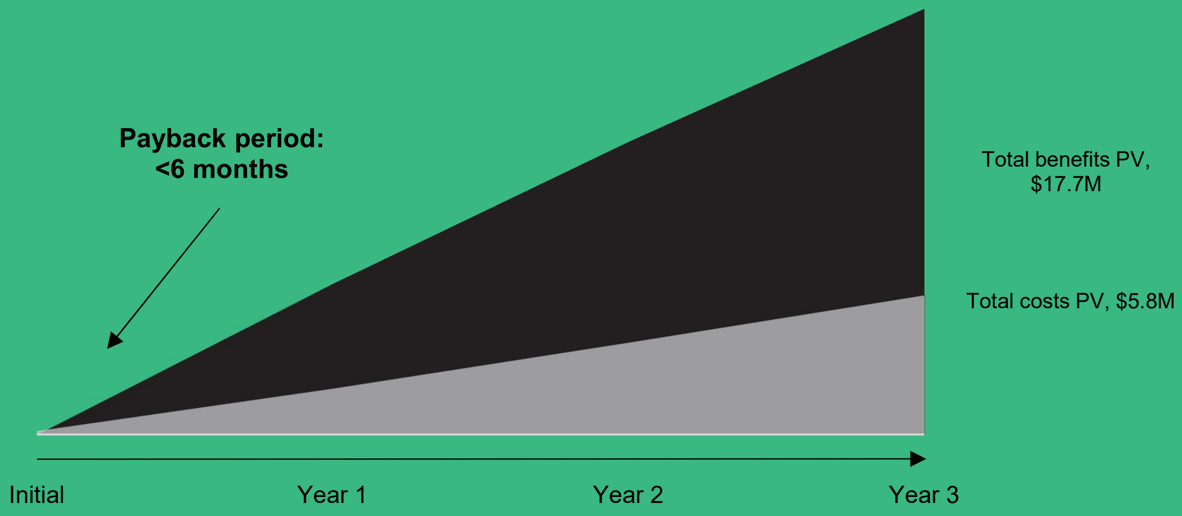
NPV
$11.92M

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 SIEM and XDR.

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 SIEM and XDR can have on an organization.

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

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 SIEM and XDR.

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.

DUE DILIGENCE

Interviewed Microsoft stakeholders and Forrester analysts to gather data relative to Microsoft SIEM and XDR.

INTERVIEWS

Interviewed four representatives at organizations using Microsoft SIEM and XDR to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

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

FINANCIAL MODEL FRAMEWORK

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

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 SIEM And XDR Customer Journey

🟩 Drivers leading to the Microsoft SIEM and XDR investment

Interviews

Role	Industry	Region	Total employees	Total SIEM and XDR users
CTO	Government	EMEA	300 employees	8 SIEM and XDR users
Manager of cloud security and compliance	Technology	Global	3,000 employees	4 SIEM and XDR users
Head of cyber and technology procurement	Logistics	EMEA	7,000 employees	15 SIEM and XDR users
Manager of cybersecurity and IT infrastructure	Professional services	North America	8,000 employees	6 SIEM and XDR users

KEY CHALLENGES

Before investing in Microsoft SIEM and XDR, the interviewees' organizations used a collection of point solutions to protect their organizations against security threats. Point-solution strategies left gaps in security coverage, which varied amongst interviewees, but were consistently exacerbated as organizations moved to the cloud. Point solutions also required more work from security professionals due to a lack of integration.

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

- **Disjointed, best-of-breed tooling.** The interviewees shared that their organizations' previous security environments relied on a series of best-of-breed point solutions. Although each solution was relatively effective in playing its part to protect the organizations, the interviewees found that chasing a best-of-breed strategy left certain assets, platforms, and workloads open to attack if they had not yet deployed a point solution for them. Importantly, point solutions lacked integration. This lack of integration generated additional serious problems in the organizations' security coverage, including a lack of visibility across their full environments and inefficiencies for security professionals.

> **"Before, I was a best-of-breed kind of person, but that just ended up introducing a lack of integration and visibility that created a lot of work for us."**
>
> *Manager of cybersecurity and IT infrastructure, professional services*

- **Lack of visibility.** The interviewees described prior security environments plagued with opacity. They consistently noted lacking protection and visibility for their cloud environments, but also missing important potential threats from lack of integration, such as getting no feed of threats from endpoints. Not only was protection lacking for several important assets, but organizations also flew blind without the ability to adequately quantify their levels of protection or any improvements in it. As the manager of cloud security and compliance from the technology industry stated: "We have lots of [virtual machines] (VMs) open to the internet which would get compromised frequently by, for example, someone dropping a cryptominer on the box. Before SIEM and XDR, we didn't have any way of detecting this, but we've since stopped 20 or so attempts."

- **Inefficient and ineffective threat remediation.** Lack of integration also increased the work burden on security professionals at the interviewees' organizations. For example, the manager of cybersecurity and IT infrastructure from the professional services industry noted that without integration and visibility, their security teams had to do all the manual work associated with correlating different data across different sources, sometimes lacking data that would be important in decision-making. The CTO from a government organization noted that relying on manual interventions created a "slow response" that also negatively impacted their "risk to network or other tools."

> **"With SIEM and XDR's technologies rolled into one platform, we get a level of visibility that we have never had before."**
>
> *Manager of cybersecurity and IT infrastructure, professional services*

SOLUTION REQUIREMENTS

The interviewees' organizations searched for a solution that could:

- Quickly deploy across the organizations' broad spectrum of assets, platforms, and workloads.
- Integrate policies and threats across the variety of assets, platforms, and workloads to improve organizationwide visibility and ease the burden on security professionals.
- Leverage the security experiences and needs of a broad set of other organizations across various industries and business sizes.

> **"We were looking through logs and hunting down spikes in traffic to understand what was happening, but I don't think we had much in the way of a proper investigation for security."**
>
> *Manager of cloud security and compliance, technology*

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 interviewees, 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 that generates $4 billion in revenue annually and employs 8,000 full-time workers. It currently employs 10 security and IT professionals that interact with its various security tools on a regular basis.

Deployment characteristics. The composite organization has traditionally followed a best-in-breed approach to its security tooling, purchasing specific point solutions generally regarded as the best in class for its specific security use case. However, the firm quickly notes that this point-solution strategy creates its own risks, namely a lack of visibility and increased burden on security professionals that opens additional gaps for potential threats to succeed.

Key Assumptions

- **$4 billion in revenue**
- **8,000 employees**
- **10 Microsoft SIEM and XDR users**

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 time of threat investigation and response	$1,025,470	$1,076,743	$1,130,581	$3,232,794	$2,671,538
Btr	Improved efficiency of other security professional work	$145,825	$153,116	$160,772	$459,713	$379,901
Ctr	Reduced cost of material security breaches	$1,521,931	$1,557,384	$1,594,610	$4,673,926	$3,868,722
Dtr	Improved efficiency and productivity of other employees	$2,659,392	$2,792,362	$2,931,980	$8,383,733	$6,928,206
Etr	Reduced costs from vendor consolidation	$1,518,733	$1,541,533	$1,565,473	$4,625,740	$3,830,824
	Total benefits (risk-adjusted)	$6,871,351	$7,121,139	$7,383,416	$21,375,906	$17,679,191

REDUCED TIME OF THREAT INVESTIGATION AND RESPONSE

Evidence and data. The interviewees shared experiencing improved security workflow metrics, including mean time-to-investigate and mean time-to-respond, after deploying Microsoft SIEM and XDR. Before the investment, mean time-to-investigate and time-to-respond were each measured in days. The interviewees described investigation processes that required:

- Several hours, but potentially days depending on time zones, just to get access to the appropriate resources.
- Potential additional hours to get access to the system if needing different credentials.
- A minimum of a day to a day and a half to drop tools onto the machine and sift through what is there.

The CTO from the governmental organization specifically discussed a prior investigation process that lacked any proactiveness on the part of security professionals, instead relying on employees to report potential threats like suspicious links and attachments. For response, this organization's security team depended on signature detection from antivirus tools, which were then flagged through a system management console that was imperfect and lacked consistency, often creating the need for additional investigations.

> **"Having multiple security tools from same vendor has helped us to save detection and response time. We no longer have to go into a bunch of different screens and tools to conduct investigations and respond to threat. The integration is seamless."**
>
> *Head of cyber and technology procurement, logistics*

With Microsoft SIEM and XDR, the interviewees reported shortening mean time-to-investigate and mean time-to-respond from days to minutes. Integration played a key role in this reduction. As everything was connected from the start, the interviewees could reliably leverage Sentinel to work on incidents with nearly all data accessible through this single pane of glass. They could then investigate the connections between different data points, drilling down into various XDR tools, such as Microsoft Defender for Endpoint or Azure Defender, for their cloud workloads.

The interviewees also noted that automation played a significant role in reducing meant time-to-investigate and mean time-to-respond. Because these firms could now deploy automated rules for addressing security threats, security professionals were granted conditional access only to those automations rather than full systems, granting them the flexibility to act when needed rather than waiting on access credentials or having default access to all systems.

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

- The composite experiences an average of 50,000 threat alerts annually, 26% of which require security professional attention with 70% of these (9,100 alerts annually) requiring investigation.
- A conservative 2 hours is needed to investigate each threat before Microsoft SIEM and XDR.
- Microsoft SIEM and XDR reduces this time by 65%.
- Two percent of investigated alerts require a response.
- Two working days or 16 hours are required to respond to each threat.
- Microsoft SIEM and XDR reduces this time by 88%.
- Security professionals incur a fully burdened hourly cost of $75, growing at 5% annually.

Risks. The reduced cost of threat investigation and response will vary with:

- The number of threat alerts experienced annually and the number of alerts needing investigation and response.
- The current time-to-investigate and time-to-respond to each threat alert.
- The fully burdened hourly rate of security professionals and how this grows over time.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of almost $2.7 million.

Reduced Time Of Threat Investigation And Response

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Number of alerts requiring investigation	Composite	9,100	9,100	9,100
A2	Prior hours to investigate threats	Interviews	2	2	2
A3	Reduction due to Microsoft SIEM and XDR	Interviews	65%	65%	65%
A4	Percentage of investigated alerts requiring response	Interviews	2%	2%	2%
A5	Prior hours to respond to threats	Interviews	16	16	16
A6	Reduction due to Microsoft SIEM and XDR	Interviews	88%	88%	88%
A7	Fully burdened hourly rate of security professionals	TEI standard	$75	$79	$83
At	Reduced time of threat investigation and response	A1*(A2*A3+A4*A5*A6)*A7	$1,079,442	$1,133,414	$1,190,085
	Risk adjustment	↓5%			
Atr	Reduced time of threat investigation and response (risk-adjusted)		$1,025,470	$1,076,743	$1,130,581
	Three-year total: $3,232,794		**Three-year present value: $2,671,538**		

IMPROVED EFFICIENCY OF OTHER SECURITY PROFESSIONAL WORK

Evidence and data. The interviewees noted that Microsoft SIEM and XDR not only benefited security professional workflows related to investigating and responding to threats, but also made other security professional work more efficient. For example, security workbook creation accelerated after investing in Microsoft SIEM and XDR. The manager of cloud security and compliance from the technology company noted that, when a new threat presented itself, they would have to do all the work to get their prior SIEM where they wanted it, spending a full week digging through sources, turning on logs, and remediating blind spots. With Microsoft SIEM and XDR's automation and integration, all the data needed to run a new workbook was already at hand, turning what was sometimes a multiweek effort beforehand into a workflow that took only a couple hours.

The interviewees also noted that the ease of using SIEM and XDR with its integration and automation features required much less time to onboard security professionals than prior tools. The manager of cybersecurity and IT infrastructure from the

> **"When [a well-known supply chain attack] happened, we had all the data that we needed in our SIEM to just run a workbook that says here are all the [indicators of compromise] (IOCs) that we're looking for. It took a couple hours versus the multiweek effort in our environment."**
>
> *Manager of cloud security and compliance, technology*

professional services firm described a scenario where they were onboarded but not given access to a specific security tool for four months. They said, “Now, I can get a security team member onboarded and into all the systems in a much shorter time just because it’s all right there, it’s all integrated, it’s all in the Microsoft tool set.”

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

- Before Microsoft SIEM and XDR, all 10 security professionals are needed for 40 hours to run a new workbook quarterly.
- Microsoft SIEM and XDR reduces this workflow by 90%.
- One new security professional is hired annually.
- Before Microsoft SIEM and XDR, it would take four months for a new hire to get onboarded onto the various security tools.
- Microsoft SIEM and XDR reduces this time by 91%.

Risks. The improved efficiency of workbook creation and security professional onboarding will vary with:

- The number of security professionals needed for new workbooks.
- The frequency with which new workbooks are created and the time it takes to create them.
- The number of new security professionals hired annually and the time to onboard them.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of almost $380,000.

Improved Efficiency Of Other Security Professional Work

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Security professionals needed to run a new workbook	Composite	10	10	10
B2	Annual frequency of building new workbooks	Composite	4	4	4
B3	Hours required to run a new workbook prior to Microsoft SIEM and XDR	Interviews	40	40	40
B4	Reduction in time to run a new workbook from Microsoft Sentinel	Interviews	90%	90%	90%
B5	Subtotal: Reduced time to run a new workbook	B1*B2*B3*B4*A7	$108,000	$113,400	$119,070
B6	Number of new hires annually	Composite	1	1	1
B7	Months to get to full productivity prior to Microsoft SIEM and XDR	Interviews	4	4	4
B8	Reduction from Microsoft SIEM and XDR	Interviews	91%	91%	91%
B9	Subtotal: Improved time-to-value of new hires	B6*B7/12*B8*A7*2,000	$45,500	$47,775	$50,164
Bt	Improved efficiency of other security professional work	B5+B9	$153,500	$161,175	$169,234
	Risk adjustment	↓5%			
Btr	Improved efficiency of other security professional work (risk-adjusted)		$145,825	$153,116	$160,772
	Three-year total: $459,713		**Three-year present value: $379,901**		

REDUCED COST OF MATERIAL SECURITY BREACHES

Evidence and data. Regardless of the specifics of their prior environments, the interviewees consistently noted that Microsoft SIEM and XDR reduced the risk of a potential security threat across the organizations. Before investing in SIEM and XDR, some interviewees did not have any protection applying to particular platforms, most often their cloud environments. As the manager of cloud security and compliance from the technology industry described: “Something like 97% of our resources are in various cloud platforms. Because of its multicloud protection, SIEM and XDR has definitely had a huge bump in terms of risk reduction for us. The impact has been greatest for cloud, where we went from ‘nothing’ to ‘something.’”

> **“We’ve seen about a 90% improvement in our risk of security breach after deploying SIEM and XDR. It’s been a game changer for us.”**
>
> *CTO, government*

Other interviewees noted that the improvement to their security risk improved thanks to the close integration of SIEM and XDR tools. For example, the head of cyber and technology procurement from the logistics industry noted that, with the disjointed nature of their prior point solutions, certain important data feeds from endpoints were not adequately captured. In their case, they had wide protection from antivirus software across their endpoints, but these endpoints were not feeding any data back to security teams for them to monitor or investigate suspicious activity.

> **“Detection is way better with SIEM and XDR. Prevention is never 100%, so I would rather have the best detection in the world than have the best protection without the visibility.”**
>
> *Manager of cybersecurity and IT infrastructure, professional services*

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

- Before Microsoft SIEM and XDR, the composite experiences an annual average of 3.1 material security breaches at an average per-breach cost of $484,240.[2]
- Microsoft SIEM and XDR protects 95% of the organization after full deployment and reduces the risk of a breach by 60%.
- Breaches negatively impacts 33% of the composite’s 8,000 total employees at a time cost of 4 hours.
- The average employees’ fully burdened hourly rate is $40, growing at 5% annually.

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

- The frequency and cost of material breaches.
- The current productivity cost of material breaches to the employee base.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $3.9 million.

Reduced Cost Of Material Security Breaches

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Average annual number of material breaches	Forrester research	3.1	3.1	3.1
C2	Average total internal and external costs of a material breach	Forrester research	$484,240	$484,240	$484,240
C3	Percentage of organization Microsoft SIEM and XDR covers	Interviews	95%	95%	95%
C4	Risk reduction from Microsoft SIEM and XDR	Interviews	60%	60%	60%
C5	Subtotal: Reduced risk of a security breach	C1*C2*C3*C4	$855,652	$855,652	$855,652
C6	Total employees	Composite	8,000	8,000	8,000
C7	Average percent of employees material breaches impact	Forrester research	33%	33%	33%
C8	Prior downtime hours per breach per employee annually	Forrester research	4	4	4
C9	Average fully burdened hourly rate per employee	TEI standard	$40	$42	$44
C10	Subtotal: Improved productivity from reduced downtime	C1*C3*C4*C6*C7*C8*C9	$746,381	$783,700	$822,885
Ct	Reduced cost of material security breaches	C5+C10	$1,602,033	$1,639,352	$1,678,537
	Risk adjustment	↓5%			
Ctr	Reduced cost of material security breaches (risk-adjusted)		$1,521,931	$1,557,384	$1,594,610
	Three-year total: $4,673,926		Three-year present value: $3,868,722		

IMPROVED EFFICIENCY AND PRODUCTIVITY OF OTHER EMPLOYEES

Evidence and data. As it better protected against security threats compared to prior environments, Microsoft SIEM and XDR had the added benefit of improving the productivity of interviewees' organizations' wider employee bases. Before Microsoft's integrated solution, the interviewees had security environments and processes that regularly impacted employee productivity negatively.

In one example, the CTO from the government organization noted that, in order for their IT teams to address new security vulnerabilities, they would have to wait for reports from security professionals and then would often have to work with them to develop and deploy the recommended remediations. With Microsoft SIEM and XDR, there is a continuous scan of the environment and all the needed data is presented to IT teams via a dashboard. This enabled the government firm to reduce the IT workload by approximately 2,000 hours.

In another example, the same interviewee described that their main response to a potential threat in their prior environment was to isolate impacted employee machines. Affected employees would have to go through the process of backing up their data while the supplier was brought onsite to reimage the machine. Only if replacement workstations were available could the employees' productivity be reasonably recaptured during this time. Similarly, the manager of cybersecurity and IT infrastructure from the professional services industry described prior tooling that would completely lock employees out of applications, particularly legacy ones, based on security concerns. This introduced hours to days of downtime for employees, depending on the application.

As Microsoft SIEM and XDR leveraged Microsoft 365 Defender, organizations improved the performance of end-user devices by removing point-solution agents and consolidating onto Microsoft SIEM and XDR. As Microsoft 365 Defender customer organizations have noted, these improvements showed up in small increments (e.g., faster boot-up, more responsive app performance, etc.). They were noticeable to end users and very much appreciated.[3]

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

- Improved security data access and visibility reduces related IT work by 4,000 hours.
- The fully burdened hourly rate of an IT professional is $60, growing at 5% annually.
- The organization spends 11,520 hours each year restaging machines before deploying Microsoft SIEM and XDR.
- Productivity drops by 75% for those end users whose devices are evaluated and restaged.
- After deploying Microsoft SIEM and XDR, the time spent restaging machines drops to 24 hours per year. Interviewees estimated that the new security stack was at least 60% responsible for that improvement.
- With fewer, simpler agents running on their devices, each of 15,000 employees also saves 21 hours per year due to improved device performance.
- A conservative 35% of that time savings is recaptured in productive labor.

Risks. The improved efficiency of IT professionals and general employees will vary with:

- The current state of IT professional visibility into new security vulnerabilities and updates.
- The number of hours spent isolating machines.
- The current time cost to employee productivity from point-solution security tool agents.
- The average fully burdened rate of IT professionals and general employees.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $6.9 million.

Improved Efficiency And Productivity Of Other Employees

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Hours saved to IT from self-service	Interviews	4,000	4,000	4,000
D2	Fully burdened hourly rate per IT professional	TEI standard	$60	$63	$66
D3	Subtotal: Improved efficiency of IT	D1*D2	$240,000	$252,000	$264,600
D4	Prior total hours spent isolating and restaging employee machines	Composite	11,520	11,520	11,520
D5	Reduction from Microsoft SIEM and XDR	Forrester research	60%	60%	60%
D6	Fully burdened hourly rate per general employee	C9	$40	$42	$44
D7	Productivity recapture rate	Forrester research	75%	75%	75%
D8	Subtotal: Improved productivity of general employees	D4*D5*D6*D7	$207,360	$217,728	$228,614
D9	Hours saved annually from faster reboot/app open times	Composite	21	21	21
D10	Percent recaptured	Forrester research	35%	35%	35%
D11	Number of knowledge workers	Composite	8,000	8,000	8,000
D12	Subtotal: Improved productivity of general employees	D9*D10*D11*D6	$2,352,000	$2,469,600	$2,593,080
Dt	Improved efficiency and productivity of other employees	D3+D8+D12	$2,799,360	$2,939,328	$3,086,294
	Risk adjustment	↓5%			
Dtr	Improved efficiency and productivity of other employees (risk-adjusted)		$2,659,392	$2,792,362	$2,931,980
	Three-year total: $8,383,733		Three-year present value: $6,928,206		

REDUCED COSTS FROM VENDOR CONSOLIDATION

Evidence and data. Some interviewees chose to decommission prior security tools after investing in Microsoft SIEM and XDR, while others chose to utilize Microsoft's integrated solution as additional protection while keeping prior tools. Prior solutions that interviewees decommissioned after their investment included:

- Legacy SIEMs.
- Two-factor authentication tools.
- Email security tools.
- Network security solutions.
- Cloud security solutions.

In addition to the direct costs related to paying for these various security tools, interviewees were able to save on internal costs related to the ongoing management of these tools after decommissioning. For the composite organization, these ongoing costs amount to about 30% of 1 FTE.

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

- An annual licensing cost of a prior SIEM tool of $560,000.[4]
- An on-premises infrastructure cost for this SIEM tool of $366,667 annually.[5]

- Three point solutions are decommissioned thanks to Microsoft 365 Defender at a total annual cost of $192,000.[6]
- The equivalent of four IT professionals were needed to manage all of these now-decommissioned tools.

Risks. The reduced costs from vendor consolidation will vary with:

- The variety and number of prior security tools decommissioned.
- The annual cost of these security tools.
- The annual internal time cost of managing these security tools.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $3.8 million.

Reduced Costs From Vendor Consolidation

Ref.	Metric	Source	Year 1	Year 2	Year 3
E1	Licensing cost of prior SIEM	Forrester research	$560,000	$560,000	$560,000
E2	On-premises infrastructure cost of prior SIEM	Forrester research	$366,667	$366,667	$366,667
E3	Cost of point solutions made redundant by Microsoft 365 Defender	Forrester research	$192,000	$192,000	$192,000
E4	Reallocated IT professionals	Composite	4	4	4
E5	Fully burdened annual rate of IT professional	D2*2,000	$120,000	$126,000	$132,300
Et	Reduced costs from vendor consolidation	E1+E2+E3+(E4*E5)	$1,598,667	$1,622,667	$1,647,867
	Risk adjustment	↓5%			
Etr	Reduced costs from vendor consolidation (risk-adjusted)		$1,518,733	$1,541,533	$1,565,473
	Three-year total: $4,625,740		Three-year present value: $3,830,824		

UNQUANTIFIED BENEFITS

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

- **Improved visibility.** The interviewees consistently noted that having the Microsoft SIEM and XDR suite of solutions improved their visibility into their organizations' security environments. For example, the manager of cybersecurity and IT infrastructure from the professional services firm noted: "We had an outside party run a penetration test before our investment in Microsoft SIEM and XDR. They said they 'knocked really loudly' on our door and we didn't see them. We did the same test a year later with Microsoft SIEM and XDR, and we caught them left and right, blocking them at every attempt. This was only possible because we had a holistic platform."

  The manager of cloud security and compliance from the technology industry also noted the benefits of having better visibility from better integration of all Microsoft products: "We no longer deploy multiple agents and don't have to understand why any two findings might differ. Everything is cohesive, flowing from Defender to Sentinel. The defaults work well, we don't have to massage settings or triage alerts."

> **"With all the different Microsoft solutions we have rolled into Microsoft SIEM and XDR, we get a level of visibility that we never had before."**
>
> *Manager of cybersecurity and IT infrastructure, professional services*

- **Improved compliance.** Improved visibility into the security environment and the expansion of visibility across the organizations also helped to improve compliance at the interviewees' organizations. The CTO from the government organization said: "Lots of teams are getting a benefit from our Microsoft SIEM and XDR investment. For example, our governance team can now run their compliance checks on a continual basis via self-service." The manager of cloud security and compliance from the technology company noted: "We've been able to track and make progress towards hardening our customer privacy compliance. We can now better monitor where customer data is flowing and how it is used, correcting any issues with boundaries."

- **Improved IT asset management.** Interviewees also noted, but were unable to quantify, a benefit to their IT asset management practices. The head of cyber and technology procurement from the logistics industry said: "Microsoft SIEM and XDR helped us close preexisting gaps in our IT inventory management. We didn't have any active asset discovery before, nor were we able to group assets together by function. We had a number of assets running constantly that should have been powered down or switched off, for example when we shut down operations in particular sectors."

- **Microsoft support.** Interviewees also shared that Microsoft genuinely cared about the future direction of their products, wanting to meet customer needs with future iterations. The CTO from the government organization explained: "We get calls from customer support asking for information on the most important features we'd like to see in future Microsoft products. This gives us the opportunity to influence the future direction of the technology to further close any gaps in our technology operations."

FLEXIBILITY

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

- **Flexibility for work-from-home and hybrid-work environments.** The interviewees shared that Microsoft SIEM and XDR made their security environments flexible enough to withstand the changing work environment instigated by the COVID-19 pandemic. For example, the manager of cybersecurity and IT infrastructure from the professional service firm noted that their prior solutions focused on protecting work being done in the office. The sudden shift to a broad work-from-home environment would have introduced severe complications and significantly increased the risk of successful security threats. The interviewee said: “With our old security tools, we would not have been able to deal with COVID-19 and work from home. Microsoft SIEM and XDR helped us continue to protect systems as employees’ work locations moved out of the office.”

- **Custom ruling.** Interviewees also noted that Microsoft SIEM and XDR provided them with further flexibility to personalize their protection to their particular security environment. For example, the manager of cloud security and compliance from the technology industry said, “We are planning to take even more advantage of custom ruling in the future. As we learn more about our security environment from Microsoft SIEM and XDR, we will program and set custom rules that further enable us to protect our business and its unique security posture, above and beyond the enhanced protection provided out of the box.”

> **“Fortunately, we had been using SIEM and XDR for six months before we made the switch to work from home. With our prior solutions, the business would never have been able to deal with the impact of COVID-19.”**
>
> *Manager of cybersecurity and IT infrastructure, professional services*

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
Ftr	Microsoft SIEM and XDR fees	$0	$1,876,660	$2,243,373	$2,557,675	$6,677,708	$5,481,701
Gtr	Cost of deployment and implementation	$131,250	$0	$0	$0	$131,250	$131,250
Htr	Time cost of training and ongoing management	$18,900	$49,770	$52,259	$54,871	$175,800	$148,560
	Total costs (risk-adjusted)	$150,150	$1,926,430	$2,295,632	$2,612,546	$6,984,758	$5,761,511

MICROSOFT SIEM AND XDR FEES

Evidence and data. Microsoft SIEM and XDR is an amalgamation of three Microsoft security products, each with different pricing models: Microsoft Sentinel, Microsoft 365 Defender, and Microsoft Defender For Cloud.

Microsoft Defender For Cloud offers complimentary policy, compliance, and asset management functionality to Azure customers. The ability to do threat detection and management with Microsoft Defender For Cloud comes at a variable added cost depending on the number of servers, Structured Query Language (SQL) instances, transactions, etc., that an organization might need to run Defender For Cloud on.

Microsoft 365 Defender comes free with certain Microsoft licenses. Organizations that already have Microsoft 365 E5 licenses incur no incremental cost to deploy Defender. In other cases, organizations will need to upgrade to an E5 security license and pay the associated marginal costs.

Microsoft Sentinel's pricing is flexible and is based on the amount of data ingested and stored on a monthly basis. Additionally, Sentinel does not require any on-premises hardware and has no contract lock-in, enabling organizations to shift this spend from capex to opex.

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

- The cost of Microsoft Defender For Cloud servers is $18,000 annually.
- The storage cost related to Microsoft Defender For Cloud is $9,000.
- The SQL cost of Microsoft Defender For Cloud is $3,000 annually.
- The composite is not currently a full E5 license holder, but purchases 8,000 E5 security licenses for its knowledge workers.
- The price of an E5 security license is $185 per year.
- The composite ingests 350 GB per day in Year 1, then scales to 700 GB per day in Year 2 and 1 TB per day in Year 3.
- All logs must be stored for 12 months.
- Ingestion for Office 365 audit logs, Azure activity logs, and alerts from Microsoft Threat Protection solutions (all of which typically represents about

5% of total log volume) are free with Microsoft Sentinel.

Risks. The total cost of Microsoft SIEM and XDR will vary with:

- The annual cost of Azure servers related to Azure Defender.
- The annual cost of storage related to Azure Defender.
- Annual Azure Defender SQL costs.
- If the organization has already purchased full E5 licenses for its employees. In this case, the cost of the security platforms is included in that fee.
- The amount of data ingested and the length of time that the data needs to be stored.
- The region where the logs are ingested and stored.

Results. As Forrester priced these solutions directly with Microsoft, Forrester did not adjust this cost for risk, yielding a three-year total PV (discounted at 10%) of under $5.5 million.

Microsoft SIEM And XDR Fees

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Cost of Microsoft Defender for servers	Composite		$18,000	$18,000	$18,000
F2	Cost of Microsoft Defender for storage	Composite		$9,000	$9,000	$9,000
F3	Cost of Microsoft Defender for SQL	Composite		$3,000	$3,000	$3,000
F4	Subtotal: Total cost of Microsoft Defender For Cloud	F1+F2+F3		$30,000	$30,000	$30,000
F5	E5 security licenses purchased	Composite		8,000	8,000	8,000
F6	Cost per license	Microsoft		$185	$185	$185
F7	Subtotal: Cost of Microsoft 365 Defender	F5*F6		$1,480,000	$1,480,000	$1,480,000
F8	Logs ingested (daily average GB)	Composite		350	700	1,000
F9	Microsoft Sentinel Costs	Composite		$366,660	$733,373	$1,047,675
F10	Cost to ingest Microsoft logs (Azure activities, Office 365, Microsoft security alerts, etc.)	Free with Azure Sentinel		$0	$0	$0
F11	Subtotal: Cost of Microsoft Sentinel	F9		$366,660	$733,373	$1,047,675
Ft	Microsoft SIEM and XDR fees	F4+F7+F11	$0	$1,876,660	$2,243,373	$2,557,675
	Risk adjustment	0%				
Ftr	Microsoft SIEM and XDR fees (risk-adjusted)		$0	$1,876,660	$2,243,373	$2,557,675
	Three-year total: $6,677,708			**Three-year present value: $5,481,701**		

COST OF DEPLOYMENT AND IMPLEMENTATION

Evidence and data. The interviewees' organizations either incurred internal time costs associated with the deployment and implementation of Microsoft SIEM and XDR, or they utilized a professional services provider.

Importantly, interviewees noted that the integrated nature of Microsoft's SIEM and XDR tools enabled them to achieve the value of their investment faster than they otherwise would have. For example, the CTO from the government organization similarly noted: "One of the key strategic decisions behind our investment in Microsoft SIEM and XDR was its speed to deploy and time-to-value. Overnight, we had the majority of our log data sources onboarded. We started seeing value from Day 1."

The CTO from the government organization shared: "There was only a little effort involving a few employees across different teams to implement and deploy Microsoft SIEM and XDR, and the onboarding process was quite quick as well. We started seeing and taking value from the investment on Day 1."

The manager of cybersecurity and IT infrastructure from the professional services firm said: "It took 30 days end-to-end to get Microsoft SIEM and XDR deployed. We opted to work with a partner who predominantly did the work for us."

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

- The use of a partner to implement and deploy Microsoft SIEM and XDR.
- Partner deployment fees are $25,000.
- Partner implementation fees are $100,000.

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

- The choice to use a partner or internal resources.
- The size of the organization, its current on-premises environment, and its presence in the cloud.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of over $131,000.

Cost Of Deployment And Implementation

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	Cost of partner deployment	Interviews	$25,000			
G2	Cost of partner implementation	Interviews	$100,000			
Gt	Cost of deployment and implementation	G1+G2	$125,000	$0	$0	$0
	Risk adjustment	↑5%				
Gtr	Cost of deployment and implementation (risk-adjusted)		$131,250	$0	$0	$0
	Three-year total: $131,250		Three-year present value: $131,250			

TIME COST OF TRAINING AND ONGOING MANAGEMENT

Evidence and data. The interviewees also noted incurring internal time costs associated with training employees on Microsoft SIEM and XDR and with ongoing management of the solution. Microsoft provided the training materials to the interviewees for free, so the only training costs were that of the employee time spent training.

In terms of ongoing management, the interviewees estimated their costs as such:

- Ten to 20 minutes daily.
- A small percentage of 1 FTE.
- One FTE for 25% to 50% of their time.

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

- All 10 security professionals require training, which takes three fully days or 24 working hours.
- One new security professional is hired annually and requires training.
- Ongoing management requires 0.38 IT FTE.

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

- The number of employees needing training.
- The size of the organization and the extent of coverage of Microsoft SIEM and XDR.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of under $149,000.

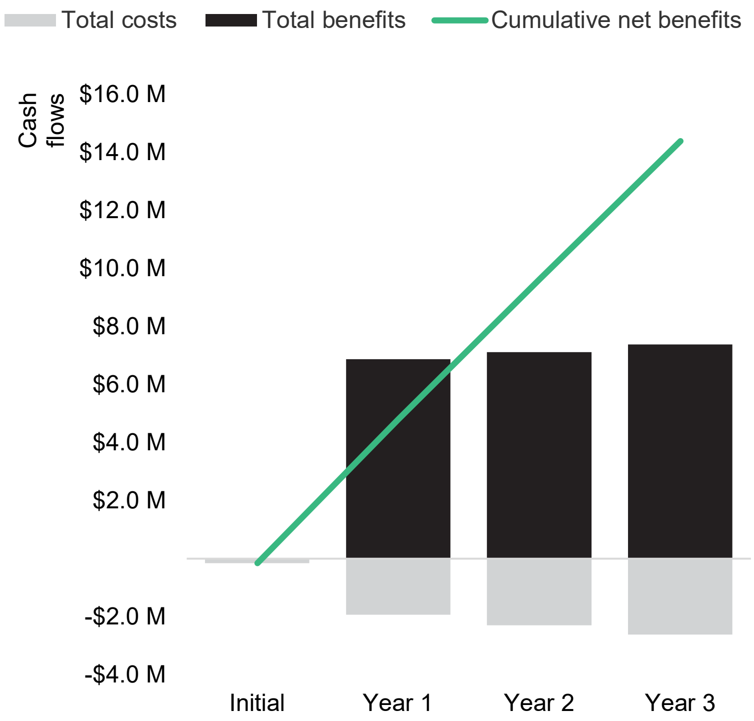
Time Cost Of Training And Ongoing Management

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
H1	Hours required for training	Interviews	24	24	24	24
H2	Security professionals trained	Composite	10	1	1	1
H3	Fully burdened hourly rate of security professionals	A7	$75	$75	$79	$83
H4	FTEs needed for ongoing management	Interviews	0	0.38	0.38	0.38
H5	Fully burdened annual rate of IT professional	E5	$0	$120,000	$126,000	$132,300
Ht	Time cost of training and ongoing management	H1*H2*H3*H4	$18,000	$47,400	$49,770	$52,259
	Risk adjustment	↑5%				
Htr	Time cost of training and ongoing management (risk-adjusted)		$18,900	$49,770	$52,259	$54,871
	Three-year total: $175,800		**Three-year present value: $148,560**			

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	($150,150)	($1,926,430)	($2,295,632)	($2,612,546)	($6,984,758)	($5,761,511)
Total benefits	$0	$6,871,351	$7,121,139	$7,383,416	$21,375,906	$17,679,191
Net benefits	($150,150)	$4,944,921	$4,825,507	$4,770,869	$14,391,148	$11,917,680
ROI						207%
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.

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

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

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

[5] Source: Ibid.

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

FORRESTER®