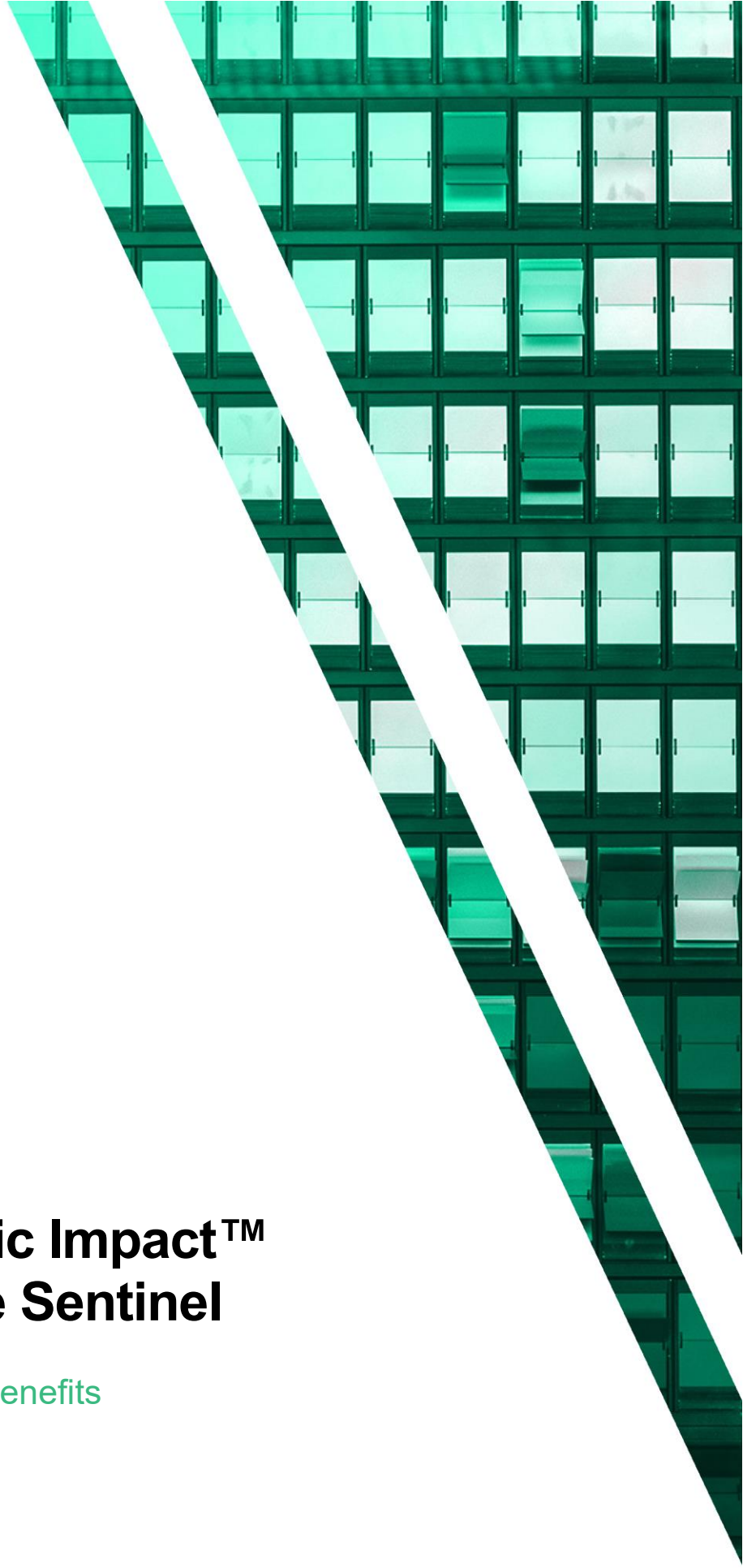
FORRESTER®



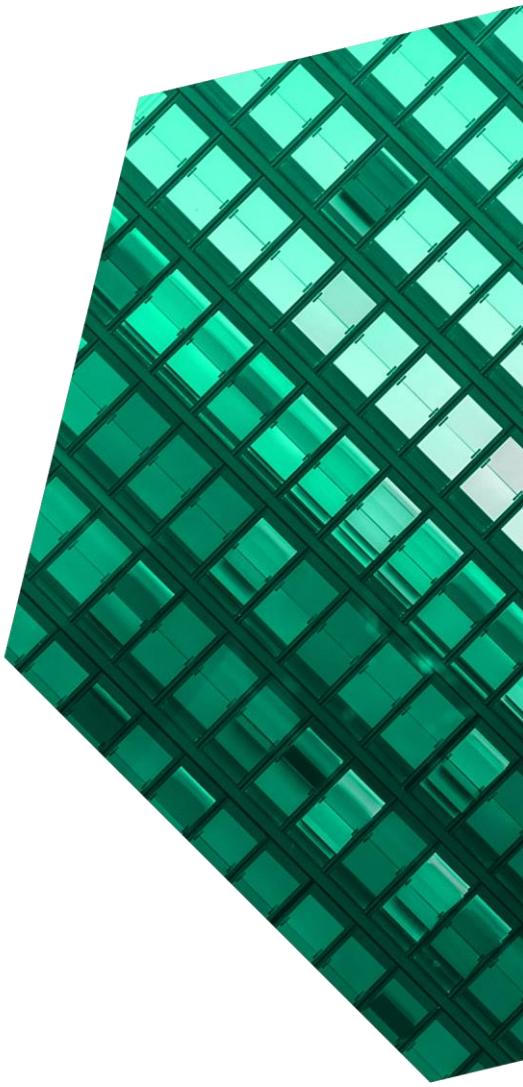
The Total Economic Impact™ Of Microsoft Azure Sentinel

Cost Savings And Business Benefits Enabled By Azure Sentinel

NOVEMBER 2020

Table Of Contents

Consulting Team: Nicholas Ferrif
Jasper Narvil



Executive Summary

Information security leaders are faced with a challenging task: provide consistent and reliable security in the face of growing complexity, increasingly diverse attack surfaces, growing alert volumes, and increasingly sophisticated and difficult-to-detect cyberattacks. Moving to a cloud-based security information and event management (SIEM) solution allows organizations to use automaton capabilities to assist their security operations teams and advanced AI/machine learning (ML) capabilities to detect advanced threats.

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 Azure Sentinel.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Azure Sentinel on their organizations. Azure Sentinel reduces SIEM costs at scale, simplifies SIEM management, and improves the efficiency and effectiveness of security operation center (SOC) teams.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four customers using Azure Sentinel. For the purposes of this study, Forrester aggregated the experiences of the interviewed customers and combined the results into a single composite organization.

Prior to using Azure Sentinel, interviewed customers used on-premises SIEM solutions utilizing and maintaining multiple sites and servers, or they used internal, custom-built solutions managed by a managed service provider (MSP) to replicate SIEM infrastructure. However, prior attempts yielded limited success, with customers unable to scale these labor-intensive solutions in cost-effective ways, and they invested significant resources in maintenance activities and investigating false positives.

After the investment in Azure Sentinel, the customers were able to benefit from the cloud-native SIEM infrastructure that Azure Sentinel provides, saving costs and enabling their SOC teams to detect and investigate threats more effectively. Key results from the investment include increased SOC team efficiency including reduced MTTR, avoided legacy SIEM costs, improved management efficiencies, and a reduced time to deploy and configure with Azure Sentinel.

KEY STATISTICS

Return on investment (ROI)
201%

Net present value (NPV)
$5.9M

> **"All of a sudden, all server logging is there in volume, every single patching event is there at scale. We don't have to pick-and-choose anymore. Now, we are only constrained by the amount that we're willing to spend on consuming the data and we're currently consuming 8.5 TB per day, so we have a very hungry appetite."**
>
> *Senior VP of global threat management, financial services industry*

> **Azure Sentinel addresses all the foundational SIEM use cases. It address data aggregation at scale horizontally forever, and the proof is in the pudding. How do you go from 50 gigabytes to 8.5 terabytes a day in a period of six months? The answer is with Azure Sentinel.**
>
> — Senior VP of global threat management, financial services industry

KEY FINDINGS

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

- **Azure Sentinel drove an increase in SOC efficiency by reducing the number of false positives and the effort required by analysts to investigate alerts, leading to $2.2 million in efficiency gains.** Azure Sentinel's AI-driven correlation engine and behavior-based analytics reduced the number of false positives for the SOC team by up to 79%, and it reduced the amount of labor associated with advanced investigations by 80% resulting in an improved MTTR. Additionally, Azure Sentinel's intuitive platform and prebuilt playbook enabled junior analysts to perform higher-value work and enabled senior analysts to focus on high-priority work, ultimately reducing the average salary for the SOC team.
- **Azure Sentinel was less expensive than the legacy SIEM solution, saving on licensing, storage, and infrastructure costs totaling $4.9 million.** Compared to the legacy, on-premises SIEM solution, Azure Sentinel was less expensive on per-GB data ingestion and licensing costs. Additionally, organizations were able to avoid the capital investments required for storing logs on-premises. Total costs for Azure Sentinel were 48% lower than the cost of the legacy solution including licensing, storage, and infrastructure costs.
- **Reduced management effort by 56% with Azure Sentinel's cloud-delivered platform, saving $1.2 million.** With Azure Sentinel's cloud-native platform, organizations were able to reallocate security professionals away from servicing on-premises infrastructures and onto other value-adding initiatives. Automatic updates, an intuitive and centralized platform, and reduced planning and maintenance associated with the legacy SIEM solution drove these gains.
- **Save 67% of time to deployment with pre-built SIEM content and out-of-the box functionality, saving $602,000.** Organizations could rapidly deploy Azure Sentinel and integrate it into their ecosystems faster due to Azure Sentinel's simple

connections to data sources and prebuilt SIEM content.

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

- **Enhanced automation capabilities.** Azure Sentinel makes it possible for organizations to automate many of the administrative tasks traditionally performed by SOC analyst, freeing up additional time for those analysts to do investigation, threat hunting, or work on enhancements.
- **Improved visibility and overall coverage.** Azure Sentinel provides prebuilt connections to many different applications and data sources, making the ingestion of new data as simple as a few clicks. Interviewees said their organizations noted that the reduced effort to develop and maintain those connections, along with the flexible and transparent pricing, allowed them to dramatically increase the amount of data that they ingested, improving visibility and overall coverage.

Cost savings compared to legacy SIEM solution

$4.9 million
48% less expensive

Costs. Risk-adjusted PV costs include:

- **With flexible, consumption-based pricing, Azure Sentinel costs $2.5 million over three years, 48% lower than the legacy SIEM deployment.** Organizations are able to scale up their data ingestion much faster with Azure Sentinel and have greater control over costs with transparent monthly billing, which eliminates lock-in and ingestion limits.
- **Deployment costs for Azure Sentinel include a deployment team and professional services, totaling $424,426 PV over three years.** These costs include an eight-person deployment team working four months to deploy and configure Azure Sentinel, along with professional services.

Reduction in false positives (over three years)

79%

The financial analysis based on the customer interviews and survey found that a composite organization experiences benefits of $8.9 million over three years versus costs of $2.9 million, adding up to a net present value (NPV) of $5.9 million and an ROI of 201%.

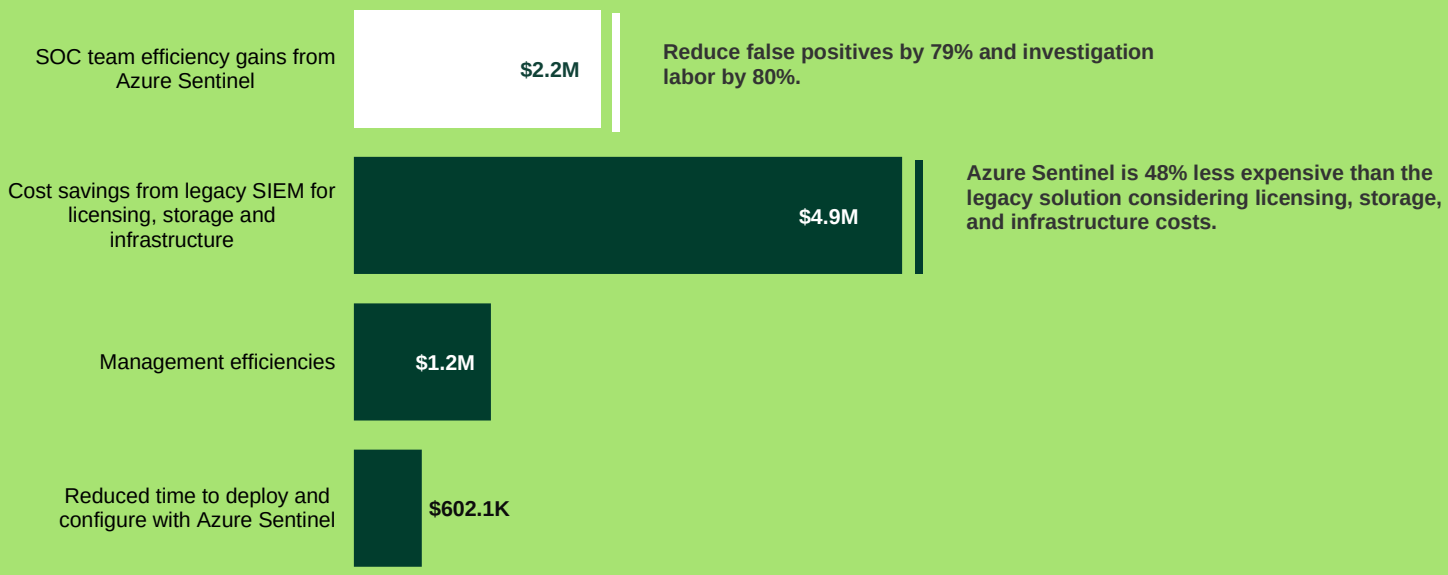
ROI (Three-Year)
201%

BENEFITS PV
$8.9M

NPV
$5.9M

PAYBACK
< 6 months

Benefits (Three-Year)



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 the Azure Sentinel.

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 Azure Sentinel can have on an organization.

DUE DILIGENCE

Interviewed Microsoft stakeholders and Forrester analysts to gather data relative to Azure Sentinel.

CUSTOMER INTERVIEWS

Interviewed four decision-makers at organizations using Azure Sentinel to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

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

FINANCIAL MODEL FRAMEWORK

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

CASE STUDY

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

The Microsoft Azure Sentinel Customer Journey

Drivers leading to the Azure Sentinel investment

Interviewed Organizations

Industry	Region	Interviewee	Revenue
IT services	Global	Senior director of global security technology and operations	$2 billion
Big data	Global	Director of information security	$500 million
Financial services	Global	Senior VP of global threat management	$6 billion
E-commerce/fashion	Global	Chief information security officer	$3.3 billion

KEY CHALLENGES

Forrester interviewed four representatives of organizations with experience using Azure Sentinel. For more details on the organizations that participated in this study, see Appendix B.

The composite organization previously utilized an on-premises SIEM solution that required redundant storage for all security logs for 12 months for disaster recovery (DR) considerations before deploying Azure Sentinel's cloud-native solution.

The interviewees' organizations faced common challenges, including:

- **Struggled to scale SIEM operations in a cost-effective way.** Limited by their on-premises SIEM infrastructures, interviewees said their organizations experienced high costs as they attempted to adapt their SIEM solutions to a growing rate of data ingestion. Expensive capital expenditures required for additional disk storage, indexers, and search heads hindered these organizations' abilities to expand their log ingestions in a scalable way.

  The senior VP of global threat management in the financial services industry spoke to the inefficiencies caused by this capital expenditures driven cost model: **"**When we wanted to scale our legacy solution, to ingest an additional GB of data, you're buying a one-TB disk. So, when you're planning out your capacity, you experience the sunk cost of the new disk when you go to 1.1 TB, plus the license cost for the legacy solution. There's lost value every single day until you hit next capacity, at which point, you have to buy a new disk and start again or limit ingestion."

- **High-value labor resources were dedicated to maintenance and administrative tasks.** Before the simplicity of Azure Sentinel, interviewees said their organizations had to manage heterogenous SIEM environments. That required collaboration from multiple employees and roles to maintain, enhance the platform, or add features. The organizations needed input from the SOC teams, security architects, engineers, and managed service providers whenever the SIEM platforms needed improvements.

  The director of information security in the big data industry illustrated this point further: "We were standing still and, obviously, we had smart people who could troubleshoot and figure out the problem. The downside is that we needed an army of those people, and we didn't have that in security. We probably had a handful of people, and they had day jobs. They are engineers and

other roles as well. Sometimes when these alerts would come and we needed to investigate, we literally had to drop everything to do so and it might even be a false positive. This process is not really something that we wanted to do, especially not on a daily basis."

> **"Whether they are Tier 1, 2, or 3, the key is that everyone is working out of a single console. They can look at, triage, and act upon alerts and incidents from their single pane of glass and do more advanced hunting work. There is definitely an efficiency there."**
>
> *Senior director of security technology and operations, IT services industry*

- **Long mean time to resolution (MTTR) and investing too many resources investigating false positives.** As organizations grew and ingested more data, SOC teams were tasked with investigating a growing number alerts, many of which were false positives. Sometimes, one event could trigger multiple false-positive alerts with no easy way to correlate the data. Additionally, organizations were experiencing very long MTTR, forcing analysts to skip some investigations or leaving them open for days before resolving.

  The director of information security in the big data industry explained how this dynamic negatively impacted their organization: "Our investigation timeline is very important. When we got an alert in the past, it would take us two or three days to investigate it, only to find out it was actually false positive because they just didn't know what they were looking at until they escalated. We didn't get any resolution to that problem with our legacy system."

WHY AZURE SENTINEL?

The organizations searched for a solution that offered:

- **Scalability with clear monthly operating costs.** The director of information security in the publishing industry delineated how Azure Sentinel's pricing model made it easier to predict costs and scale SIEM operations: "Reducing costs was really the first driver for us. Because, compared to our legacy solution, Azure Sentinel offered many of the same features. But at the end of the day, Azure Sentinel won out because we were able to scale and control our costs."
- **Simplified management with reduced labor.** The senior director of global security technology and operations in the IT services industry explained, "Every time a new subscription or a new feature was deployed, we'd call our security architect, members of the SOC team, and maybe somebody from what we call 'core infrastructure' so that we could feed all of the necessary information to the collectors and get the collector to do the optimization before the handoff to the MSP [managed service provider]. This step, which had to be part of any new platform or feature change, took around eight days."
- **Improved effectiveness versus the legacy SIEM solution.** The senior VP of global threat management in the financial services industry spoke to the performance advantages that Azure Sentinel offers over their legacy SIEM solution: "The goal we set for Azure Sentinel was that it had to be as good or better than our legacy solution across the 30 use cases that we were running. We wanted to really dig deep and question it during that RFP process. Azure Sentinel met that goal, and we were able to increase the number of use cases, further enhancing our security posture."

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

Description of composite. The organization is a conglomerate based in the US with operations across the globe. Its annual revenue is $3.5 billion, and it employs 12,000 people. The organization's SOC team is comprised of 15 full-time employees, while eight people make up its infrastructure and SIEM maintenance team. As a large organization, it ingests around 500 GB of data each day in Year 1, scaling to 1 TB per day in Year 2 and 1.5 TB per day in Year 3.

Deployment characteristics. The composite organization starts with a proof of concept (POC) to test Azure Sentinel against their legacy solution. After a successful trial, the organization begins deployment with a team of eight FTEs who spend four months of their time working with the help of contracted professional services to get Azure Sentinel up and running. This team makes more than 200 data connections, including 140 subscriptions and 60 data sources.

Key assumptions

- **$3.5 billion annual revenue**
- **12,000 employees**
- **Global operations**
- **Ingests 500 GB/day in Year 1**

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	SOC team efficiency gains from Azure Sentinel	$817,594	$880,116	$957,066	$2,654,775	$2,189,693
Btr	Cost savings from legacy SIEM for licensing, storage and infrastructure	$1,250,550	$2,006,100	$2,761,650	$6,018,300	$4,869,666
Ctr	Management efficiencies	$489,888	$489,888	$489,888	$1,469,664	$1,218,279
Dtr	Reduced time to deploy and configure with Azure Sentinel	$615,600	$26,933	$26,933	$669,465	$602,129
	Total benefits (risk-adjusted)	$3,173,632	$3,403,036	$4,235,536	$10,812,204	$8,879,767

SOC TEAM EFFICIENCY GAINS FROM AZURE SENTINEL

SOC teams have a single pane of glass for all security logs, alerts, and incidents, which reduces false positives, simplifies investigations and reduces MTTR. Azure Sentinel's AI-powered correlation engine and user behavior analytics give SOC analysts a prioritized view of the organization, elevating high-priority threats and reducing false positives. Automation then enables the SOC team to respond to these alerts rapidly with built-in orchestration of common tasks. As a result, interviews noted a significant reduction in MTTR with average resolution times reduced from hours to minutes after deploying Azure Sentinel.

- Interviewees noted that with their organization's legacy SIEM solution, alerts were not well correlated, so a single event could trigger multiple actionable alerts with no simple way for the SOC analyst to recognize and clear the false positives. This also led to more escalations as analysts were required to search across multiple indexers and search heads to triage an alert. This required a more specialized skill set and increased the amount of labor involved in investigations.
- With Azure Sentinel, organizations were able to significantly reduce false positives, gain a better understanding of real threats by correlating multiple alerts in a single event, and subsequently reduce MTTR for security alerts. Azure Sentinel's intuitive user interface, built-in knowledge base, and ML give SOC analysts the information they need to quickly investigate and remediate any alerts without relying on complicated search queries or searching through disparate systems. Additionally, Microsoft's prebuilt playbook and queries enabled organizations to leverage more junior analysts for their Tier 1 alerts, reducing the overall salary burden of the SOC team.

The director of information security in the publishing industry said: "Before, things would often get escalated to me or someone on my team because the SOC analyst didn't really know what they were looking at. Azure Sentinel is different because the analysts have all the data in front of them. It's easier to use than our legacy solution, and they feel comfortable doing threat hunting. That's one of the biggest advantages that I see with Azure Sentinel."

- A CISO in the e-commerce/fashion industry explained: “The playbooks give you a prerecorded way of dealing with an incident, and the benefit to us is that I get consistency in response from any security analyst. The other thing that we’ve learned is that we can actually bring in far more junior security analysts, train them on the platform, and let them loose on a certain number of playbooks with certain amounts of responsibility. Our Tier 1 [analysts] are a lot cheaper than they used to be.”

“With Azure Sentinel, the false positive rate has dramatically improved, and we’re now down to responding within minutes whereas with our legacy solution, our average response time was eight hours.”

CISO, eCommerce / fashion industry

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

- The SOC team has 15 full-time employees covering Tiers 1 to 3 with an average fully burdened annual salary of $135,000.
- SOC analysts previously spent 25% of their time triaging false positives with the legacy solution. Azure Sentinel’s ML enabled correlation engine and automation capabilities significantly reduces this time.
- SOC analysts previously spent 25% of their time doing advanced, multitouch investigations (including escalations) with the legacy solution. With Azure Sentinel’s intuitive user interface and prebuilt playbooks and queries, SOC analysts can perform more advanced investigations on their own and faster.
- The average salary for the SOC team is reduced by 10% due to the ability to hire more junior Tier 1 analysts.

Risks. Organizations may realize results that differ from those presented in the financial model due to:

- The size and average salary of the SOC team.
- The average time SOC analysts spend on false positives and advanced investigations.
- The maturity and capabilities of the legacy SIEM solution.

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $2.2 million.

SOC Team Efficiency Gains From Azure Sentinel					
Ref.	**Metric**	**Calculation**	**Year 1**	**Year 2**	**Year 3**
A1	SOC team (FTEs)	Composite	15	15	15
A2	Time spent investigating false positives with legacy solution	Composite	25%	25%	25%
A3	Reduced false positives with Azure Sentinel	Composite	50%	63%	79%
A4	SOC analyst average fully burdened salary	$100,000*1.35	$135,000	$135,000	$135,000
A5	Subtotal: Analyst time saved from fewer false positives	A1*A2*A3*A4	$253,125	$318,938	$399,938
A6	SCO analyst time dedicated to advanced/multitouch investigations with legacy solution	Composite	25%	25%	25%
A7	Reduced labor effort for advanced/multitouch investigations (e.g., better correlations, searchability, dashboard info, etc.)	Composite	80%	80%	80%
A8	Subtotal: Analyst efficiency related to faster and easier investigations	A1*A4*A6*A7	$405,000	$405,000	$405,000
A9	Reduced average salary for SOC analysts with Azure Sentinel	Composite	10%	10%	10%
A10	Subtotal: SOC analyst salary savings	A1*A4*A9	$202,500	$202,500	$202,500
At	SOC team efficiency gains from Azure Sentinel	A5+A8+A10	$860,625	$926,438	$1,007,438
	Risk adjustment	↓5%			
Atr	SOC team efficiency gains from Azure Sentinel (risk-adjusted)		$817,594	$880,116	$957,066
	Three-year total: $2,654,775		**Three-year present value: $2,189,693**		

COST SAVINGS FROM LEGACY SIEM FOR LICENSING, STORAGE AND INFRASTRUCTURE

Organizations eliminated their legacy SIEM vendors, which reduced licensing costs for log ingestion and storage and removed the costly associated on-premises infrastructures. By moving to Azure Sentinel's cloud-based SIEM, the organizations no longer needed to store their log data on-premises. And with Azure Sentinel's flexible, consumption-based pricing, they were no longer locked into long-term contracts or capacity limits.

- Legacy vendors offered annual or multiyear contracts with capped ingestion and storage limits, leaving the organizations with an uncomfortable choice: pay more for capacity that may go unused or cap the amount of data ingested, limiting visibility into network activity. Additionally, due to disaster recovery considerations, interviewees reported needing to store redundant copies of all security logs, doubling the amount of on-premises storage needed compared to data ingested.
- With Azure Sentinel, the organizations pay for consumption and can scale their ingestion up and down as needed, creating predictable monthly operational expenditures and giving cost control back to the business. The senior VP of global threat management in the financial services industry said: "With Azure Sentinel, I have tremendous cost transparency and control. The transparency and dialogue we have with

Microsoft is phenomenal because it's not opaque. All the rates are understood."

- With Azure Sentinel's cloud-based SIEM, the organizations were able to reduce their on-premises footprints by moving storage to the cloud, saving on infrastructure costs. The senior VP of global threat management in the financial services industry said, "We avoided about $2.1 million of additional life cycle investments this year, and we also improved our environmental impact by reducing our footprint."

  The CISO in the e-commerce/fashion industry said: "Even with our legacy MSP, we had to run our own collectors. So, switching those off has saved quite a bit of compute costs. And we were able to save about $1 million on just security licensing from consolidation."

"With Azure Sentinel, we save $1.7 million over three years. And that's not a like-for-like comparison, we save $1.7 million to move away from our MSP, recruit an internal security operations team, run Azure Sentinel and bring in a response team that didn't exist before."

CISO, eCommerce / fashion industry

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

- It ingests security logs at a rate of 500 GB per day in Year 1, scaling to 1 TB per day in Year 2 and 1.5 TB per day in Year 3.
- The composite organization removes all SIEM-related infrastructure from its on-premises environment. This includes servers, storage, forwarders, indexers and search heads, and costs associated with DR and licensing.
- For DR purposes, it must retain redundant security logs for 12 months. This doubles the amount of storage needed compared to ingestion.
- Operating expenses cost 10% of capitalized infrastructure costs.

Risks. Organizations may realize results that differ from those presented in the financial model due to.

- The volume of logs ingested.
- The cost of legacy SIEM licensing and on-premises storage requirements.
- The cost and size of the on-premises infrastructure related to legacy SIEM.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $4.9 million.

Avoided Costs Associated With Legacy SIEM					
Ref.	**Metric**	**Calculation**	**Year 1**	**Year 2**	**Year 3**
B1	Logs ingested (daily GB)	Composite	500	1,000	1,500
B2	Log ingestion costs with legacy solution	Composite	$401,500	$803,000	$1,204,500
B3	Storage costs with legacy solution	Composite	$438,000	$876,000	$1,314,000
B4	Subtotal: Avoid legacy SIEM vendor costs	B2+B3	$839,500	$1,679,000	$2,518,500
B5	Avoided hardware costs for on-premises infrastructure and storage related to legacy SIEM	Composite	$500,000	$500,000	$500,000
B6	Avoided operating expenses for on-premises infrastructure (e.g., HVAC, power, etc.)	10% of deployment	$50,000	$50,000	$50,000
B7	Subtotal: Avoided hardware and operating costs for on-premises infrastructure	B5+B6	$550,000	$550,000	$550,000
Bt	Cost savings from legacy SIEM for licensing, storage and infrastructure	B4+B7	$1,389,500	$2,229,000	$3,068,500
	Risk adjustment	↓10%			
Btr	Avoided costs associated with legacy SIEM (risk-adjusted)		$1,250,550	$2,006,100	$2,761,650
	Three-year total: $6,018,300		**Three-year present value: $4,869,666**		

MANAGEMENT EFFICIENCIES

By reducing on-premises infrastructure and storage, infrastructure and SIEM management teams perform less maintenance and spend more time adding value to the business. Azure Sentinel's cloud-based SIEM reduces the size and complexity of the on-premises infrastructure, eliminating both planning and maintenance efforts associated with the legacy SIEM deployment.

- Before deploying Azure Sentinel, interviewees said their organizations had to meticulously plan their current and projected future capacity and storage needs to ensure their on-premises infrastructures could accommodate the log ingestion needs of the security operations team. Successfully managing the on-premises SIEM deployment required multiple skill sets and involved maintaining the connections between the SIEM and the various data sources, as well as the forwarders, indexers, and search heads. Additionally, maintenance teams had to implement regular updates and patches to keep the environments secure.
- Moving to Azure Sentinel eliminated these components from the on-premises environments, subsequently eliminating the maintenance effort involved and allowing IT resources to focus on value-adding tasks and projects. The senior VP of global threat management in the financial services industry said, "It's saved hundreds of person-hours and has alleviated a significant burden from the infrastructure management organization."
- With Azure Sentinel, organizations are no longer required to manage updates, upgrades, and patches to their SIEM environments because Microsoft does that work for them. The senior director of security technology and operations in

the IT services industry said: “Ease of the connections is a big [benefit]. The other one is that we get updates for free. Microsoft is constantly making changes, updates, and improvements to its products. [Microsoft] onboards new capabilities and improves how we can do queries and correlations in automations and investigations. And we get all of that for free. We never have to update Sentinel to the latest version. We just get it.”

With less on-premises infrastructure, organizations no longer need to leverage valuable resources for maintenance activities. The senior director of security technology and operations in the IT services industry said: “With Azure Sentinel, we don’t need the storage expert. We don’t need the computer expert. We don’t need the legacy platform integration expert when we are doing maintenance. Now, we’ve got one engineer and some other folks who are shadowing and learning to manage the environment. That’s it.”

The security engineer in the publishing industry said: “Azure Sentinel’s playbooks and logic apps have removed the need for a lot of custom coding and application development on our side. It allows us to focus on automation and improving the overall functionality, and we don’t need to hire a professional services person or pull a resource from the development team.”

“There is no more downtime with Azure Sentinel. It’s never blinked. It’s never gone down, and when we hit a certain capacity, Microsoft actually gave us our own dedicated cluster and the performance improved.”

Senior VP of global threat management, financial services industry

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

- A team of eight employees was previously responsible for managing and maintaining the on-premises SIEM infrastructure.
- There were 3.5 FTEs previously responsible for activities including the management of data connections, search heads, indexers, forwarders, capacity planning, updates and patching, and any system troubleshooting.
- An additional FTE who specializes in the legacy solution is reallocated and can move off maintenance and help fine-tune and improve the Azure Sentinel SIEM performance.

Reduced infrastructure and SIEM management effort

56%

Risks. Organizations may realize results that differ from those presented in the financial model due to:

- The size of the infrastructure and SIEM management team.
- The speed at which the organization deploys Azure Sentinel and can remove legacy infrastructure.
- The average salary for the IT management team.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $1.2 million.

Management Efficiencies					
Ref.	**Metric**	**Calculation**	**Year 1**	**Year 2**	**Year 3**
C1	Infrastructure and SIEM management team (FTEs)	Composite	8	8	8
C2	Reallocate infrastructure services professionals no longer doing on-premises maintenance	Composite	3.5	3.5	3.5
C3	Reallocate legacy solution specialist	Composite	1.0	1.0	1.0
C4	Total reduction in maintenance effort (showing rounded value)	(C2+C3)/C1	56%	56%	56%
C5	Average salary of management team	$90,000*1.35	$121,500	$121,500	$121,500
Ct	Management efficiencies	C1*C4*C5	$544,320	$544,320	$544,320
	Risk adjustment	↓10%			
Ctr	Management efficiencies (risk-adjusted)		$489,888	$489,888	$489,888
	Three-year total: $1,469,664		**Three-year present value: $1,218,279**		

REDUCED TIME TO DEPLOY AND CONFIGURE WITH AZURE SENTINEL

Cloud-native SIEM means organizations can start ingesting logs on Day 1, simplifying the RFP process and giving them more time and flexibility to develop automation, fine-tune, and connect more parts of their ecosystems. Azure Sentinel's prebuilt playbooks, queries, automation, and other SIEM tools gives organizations a head start in deployment and fine-tuning. Simplified data connections and integrations with many non-Microsoft systems reduce the time and effort involved with ingesting new data sources and allow organizations to cover more of their networks faster and with predictable monthly costs.

- For the interviewees' organizations, legacy solutions required a significant investment in on-premises infrastructure and orchestration to properly function. Issues and downtime were common as resource-strapped IT organizations were tasked with expanding the SIEM log ingestion sources and storage capacity while maintaining the searching and indexing capabilities that SOC analysts use. Additionally, the organizations struggled to find the resources to tackle improvements like additional automations, developing and updating playbooks, and other activities that could help reduce false positives and improve the performance of the SIEM and SOC teams.
- With Azure Sentinel's cloud-native SIEM, the interviewees' organizations could immediately start ingesting Microsoft with a couple of clicks. Prebuilt connections to other applications and sources reduced the overall effort required to deploy the SIEM, and flexible and predictable pricing let the organizations (rather than a vendor contract) dictate the volume of data ingested. The CISO in the e-commerce/fashion industry said: "Our number one criterion was to improve the security of our organization. Sentinel gave us a faster route to be a more effective and efficient organization. It's far more dynamic than our legacy solution. And we are a growing business, so we needed a security solution that could adapt and not get in the way. We feel like we have found that in Azure Sentinel."

The same interviewee also said: “Deployment was a lot quicker on Sentinel because there was a lot less plumbing to have to deal with, and we could get straight into the details on any issues. With Azure Sentinel, we deployed 75% to 80% faster.”

- The senior VP of global threat management in the financial services industry said: “It took us about five years to scale up from 500 GB to 6 TB per day of collection on our legacy solution. Azure Sentinel was practically zero to 8.5 TB in six months.”

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

- A team of eight employees is responsible for deploying and configuring the SIEM solution.
- With the legacy SIEM, it would have taken this team 12 months to fully deploy and ramp up data collection to an acceptable level.
- Work in Years 2 and 3 is to configure the solution, add new data sources, and update to the latest version.
- The average fully burdened salary for the deployment team is $121,500.

Risks. Organizations may realize results that differ from those presented in the financial model due to.

- The size, complexity, and specific requirements of the SIEM deployment.
- The number of data sources connections needed to reach steady state.
- The size and cost of the deployment team.

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $602,129.

Reduced deployment time

67%

Reduced Time To Deploy And Configure With Azure Sentinel

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
D1	Average salary of the deployment team	C5	$121,500	$121,500	$121,500
D2	SIEM deployment and configuration team (FTEs)	Composite	8	2	2
D3	Deployment and annual configuration time including adding additional connections/integrations with the legacy solution (months)	Composite	12	2	2
D4	Deployment and annual configuration time including adding additional connections/integrations with Azure Sentinel (months)	Composite	4	0.60	0.60
D5	Improved time to steady state	1-(D4/D3)	67%	70%	70%
Dt	Reduced time to deploy and configure with Azure Sentinel	(D1/12*D2*D3)-(D1/12*D2*D4)	$648,000	$28,350	$28,350
	Risk adjustment	↓5%			
Dtr	Reduced time to deploy and configure with Azure Sentinel (risk-adjusted)		$615,600	$26,933	$26,933
	Three-year total: $669,465		**Three-year present value: $602,129**		

UNQUANTIFIED BENEFITS

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

- **Enhanced automation enabled by Azure Sentinel frees up time for SOC analysts to advance other projects.** The senior VP of global threat management in the financial services industry said: "Thanks to the management efficiencies with Sentinel, I was able to reprogram the work effort of around four FTEs. They no longer had to be firefighters. They could focus on data factors and pipelines in Azure and they could focus on implementing other security capabilities or work on other projects or enhancements that have been on our roadmap. And we got to cancel a managed operations and maintenance contract with one of our providers simply because we now have the resources to do it ourselves."
- **Improve network coverage and visibility.** Through easy connections to more data sources, free ingestion for some Microsoft logs, and flexible and predictable monthly pricing, organizations ingest more data with Azure Sentinel. The CISO in the e-commerce/fashion industry said, "Azure Sentinel today covers far more — 400% more — of our network than our legacy solution ever did."

FLEXIBILITY

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

- **Microsoft ecosystem.** Interviewees noted that Azure Sentinel integrates tightly with other parts of the Microsoft ecosystem and offers free ingestion for certain Microsoft products. Their organizations benefited more when they had additional Microsoft products and services deployed in their ecosystems, and they found they were now leveraging products and services they didn't use or underutilized in the past.

  The CISO in the e-commerce/fashion industry said: "Having Azure Sentinel brings additional value to other Microsoft investments we had already made. We consider our E5 licenses a sunk cost, and there were some products that we did not leverage in the past like MCAS [Microsoft Cloud App Security]. Now we are massive MCAS consumers because of the integration with Azure Sentinel. Intune is another application that we are looking into. All of a sudden, the value of other security investments goes up because we've got this core product to build around."

  The SIEM platform services owner in the IT services industry said: "We are really getting best of breed from Microsoft. We're heavily invested in its ecosystem. Any work [Microsoft] puts in, we're getting the value out of that. And it set us up for the future. It really let us focus on value-add projects and lets us protect our company in new and better ways moving forward."
- **Data science opportunities with "Bring Your Own ML."** With Azure Sentinel, interviewees said their organizations have set ambitious goals for ways to enhance their capabilities. The senior director of security in the IT services industry said: "We are starting to investigate some features in Azure Sentinel around the "Bring Your Own ML" capabilities, and we are looking into how we can leverage data science for security. We have an internal data science team and our SIEM has the most data out of any single service at our company, so it is a great place for us to leverage data science. Azure Sentinel really allows us to do this work and has now got our company to look at data scientists as first-class citizens. That's a big [benefit]."
- **Additional flexibility for businesses during uncertain times.** Interviewees noted that Azure Sentinel helped their organizations control costs

during unexpected events when they previously would have been locked into their same annual contacts with legacy providers.

The senior director of security technology and operations in the IT services industry said: “One of the really nice things about Azure Sentinel is that you pay for what you use and can actually create the capacity reservations. That’s part of our realized savings: We are no longer committing to overpaying for something that we may not be using. Even with the COVID-19 pandemic, we’ve got fewer people in our offices, so we have actually been able to see a drop in traffic and respond accordingly. This saves on monthly ingestion costs.”

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**
Etr	Azure Sentinel costs	$0	$523,800	$1,047,675	$1,571,513	$3,142,988	$2,522,730
Ftr	Deployment costs	$392,700	$12,758	$12,758	$12,758	$430,973	$424,426
	Total costs (risk-adjusted)	$392,700	$536,558	$1,060,433	$1,584,271	$3,573,961	$2,947,156

AZURE SENTINEL COSTS

With Azure Sentinel, organizations have predictable monthly costs, and flexible pricing options and they no longer need to deal with capacity restrictions and scaling challenges. Organizations can leverage Microsoft's flexible pricing to minimize monthly costs. And with no on-premises hardware or locked-in contracts, they can shift SIEM costs from capex to opex.

- Interviewees noted that both ingestion and storage costs are cheaper with Azure Sentinel. The senior director of security technology and operations in the IT services industry said, "If you take costs for Azure Sentinel and compare them to the costs that we had to simply run our legacy solution — for hosting, licensing, etc. — we are seeing 15% savings with Azure Sentinel and we are getting more"
- The SIEM platform services owner in the IT services industry said, "We can manage our capacity reservations much more tightly, so we are not overpaying. If we need more tomorrow, we can up our capacity and licensing. And if we don't need it the month after that, we can drop it back down again."

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

- It ingests 500 GB per day in Year 1, then scales to 1 TB per day in Year 2 and 1.5 TB per day in Year 3.
- All logs must be stored for 12 months.
- Forrester calculated pricing by using Microsoft Azure Sentinel's price calculator for the US East region.
- 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 Azure Sentinel.

Risks. Organizations may realize results that differ from those presented in the financial model due to.

- 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.

To account for these risks, Forrester adjusted this cost upward by 0%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $2.5 million.

Azure Sentinel Costs						
Ref.	**Metric**	**Calculation**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Logs ingested (daily GB)	B1		500	1,000	1,500
E2	Azure Sentinel costs	Azure Sentinel cost calculator		$523,800	$1,047,675	$1,571,513
E3	Cost to ingest Microsoft logs (Office 365 audit logs, Azure activity logs, and alerts from Microsoft Threat Protection solutions)	Free with Azure Sentinel		$0	$0	$0
Et	Azure Sentinel costs	E2	$0	$523,800	$1,047,675	$1,571,513
	Risk adjustment	0%				
Etr	Azure Sentinel costs (risk-adjusted)		$0	$523,800	$1,047,675	$1,571,513
	Three-year total: $3,142,988			**Three-year present value: $2,522,730**		

DEPLOYMENT COSTS

Deploying Azure Sentinel was faster and easier for the interviewees' organizations than deploying the legacy SIEM solutions. With Azure Sentinel's prebuilt playbook, queries and data connections and free ingestion for some Microsoft logs (Office 365 audit logs, Azure activity logs, and alerts from Microsoft Threat Protection solutions), organizations can start using sentinel with minimal effort for free and scale up from there.

- Interviewees said their organizations typically started with an RFP or proof of concept to ensure that Azure Sentinel met their needs. After the RFP, the organizations could simply continue using Azure Sentinel and add more data connections and sources to cover more of their network.
- The organizations were able to ingest more data faster with Azure Sentinel, covering a larger percentage of their overall networks compared to legacy solutions.

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

- A team of eight FTEs spends four months deploying and configuring Azure Sentinel. That includes establishing connections to all applications and hardware, automating some false positives, and deploying playbooks and other SIEM content to assist SOC analysts.
- The organization allocates $50,000 in professional services to ensure a smooth transition to Azure Sentinel from the on-premises legacy solution.
- Once deployed, two FTEs spend several weeks per year ensuring managing and maintaining the platform.

Risks. Organizations may realize results that differ from those presented in the financial model due to.

- The size and complexity of the legacy SIEM deployment.
- The types of data connections needed to fully deploy Azure Sentinel.

- The amount of professional services needed to successfully transfer from the legacy SIEM to Azure Sentinel.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $424,000.

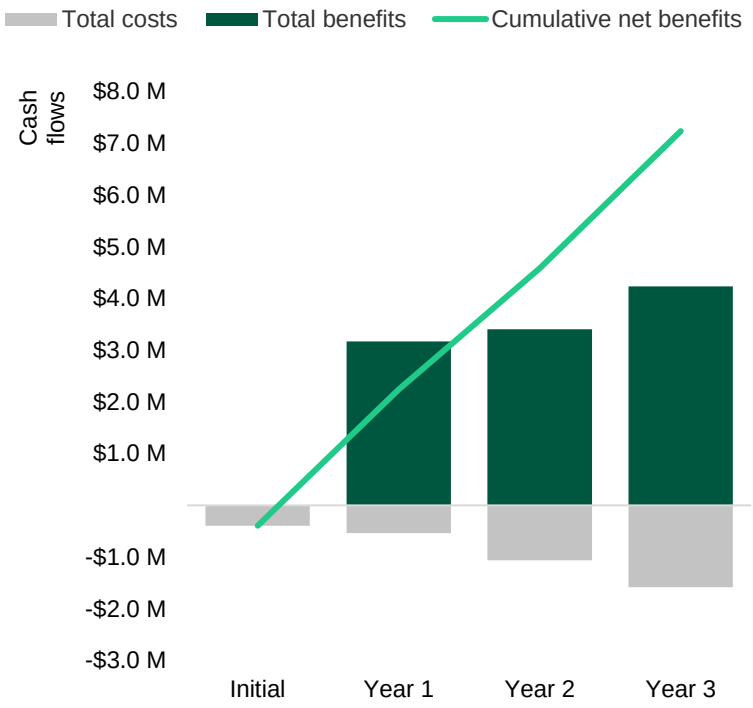
Deployment Costs

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
F1	Professional services	Composite	$50,000			
F2	Deployment team (FTEs)	Composite	8			
F3	Time to deploy (months)	Composite	4			
F4	Enhancement team (FTEs)	Composite		2	2	2
F5	Time spent on new data connections and enhancements	Composite		5%	5%	5%
F6	Average salary of management team	C5	$121,500	$121,500	$121,500	$121,500
Ft	Deployment costs	F1+(F2*F6/12*F3)+(F4*F5*F6)	$374,000	$12,150	$12,150	$12,150
	Risk adjustment	↑5%				
Ftr	Deployment costs (risk-adjusted)		$392,700	$12,758	$12,758	$12,758
	Three-year total: $430,973			**Three-year present value: $424,426**		

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	($392,700)	($536,558)	($1,060,433)	($1,584,271)	($3,573,961)	($2,947,156)
Total benefits	$0	$3,173,632	$3,403,036	$4,235,536	$10,812,204	$8,879,767
Net benefits	($392,700)	$2,637,074	$2,342,604	$2,651,266	$7,238,244	$5,932,611
ROI						201%
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."

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 D: Endnotes

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


FORRESTER®