FORRESTER®

New Technology: The Projected Total Economic Impact™ Of Microsoft Security Copilot

Cost Savings And Business Benefits Enabled By Security Copilot

A FORRESTER NEW TECHNOLOGY PROJECTED TOTAL ECONOMIC IMPACT STUDY
COMMISSIONED BY MICROSOFT, NOVEMBER 2024

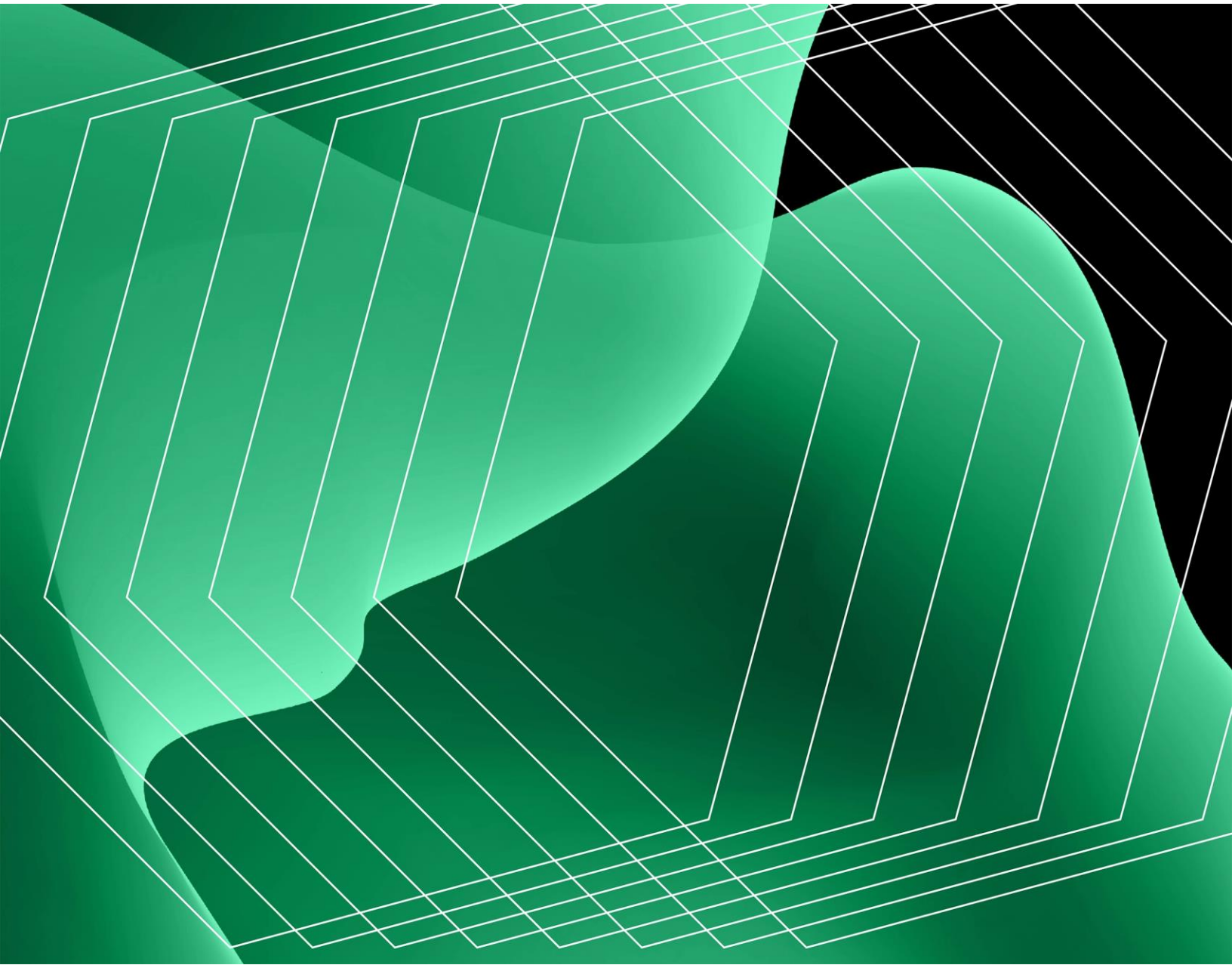


Table Of Contents

Consulting Team:

Kris Peterson

ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute their specific priorities using a unique engagement model that ensures lasting impact. For more information, visit forrester.com/consulting.

Executive Summary

In today's rapidly evolving digital landscape, organizations face an increasing number of more-sophisticated cyberthreats. The need for comprehensive security solutions that detect, respond to, and mitigate these threats is more critical than ever. At the same time, as the complexity of threats grows, there is significant demand for tools that not only enhance threat detection capabilities but also empower security teams through automation, actionable insights, and overall operational efficiency.

Microsoft Security Copilot is an advanced, AI-driven solution designed to augment and automate security operations. It helps organizations respond to threats in real time, reducing risk and improving efficiency. By seamlessly integrating with an organization's existing security tools, Security Copilot provides actionable insights, automates repetitive tasks, and enables security teams to focus on strategic initiatives.

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

Projected ROI

99% to 348%

Projected net present value

$500K to $1.8M

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four representatives with experience using Security Copilot at their organizations. Forrester also surveyed 307 security operations (SecOps) decision-makers about their use and the projected benefits of Security Copilot. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that is a global organization with $1 billion in annual revenue, 10,000 employees, and a 20-person SecOps team.

Before implementing Security Copilot, interviewees noted how their organizations managed a mix of security tools and third-party services that, while partially integrated, did not form a unified system or include extensive automation. This setup led to fragmented processes, slowed response times, and increased reliance on manual efforts, resulting in a reactive, rather than proactive, security program.

After deploying Security Copilot, the interviewees observed significant improvements in their security operations, including a reduction in breach risk due to faster detection and response capabilities, efficiency gains for SecOps personnel, and cost savings from reducing third-party services.

KEY FINDINGS

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

- **The reduced risk of security breaches.** The implementation of Security Copilot lowers the likelihood of security breaches for the composite, with a projected present value between $547,000 and $1.0 million. This benefit is driven by the solution's advanced threat detection and response capabilities, significantly improving the composite's overall security posture.
- **The amplified efficiency of the SecOps team.** Security Copilot streamlines workflows, automates routine tasks, and supports the upskilling of SecOps personnel, boosting the productivity and efficiency of the composite's security teams. The projected present value of this benefit is between $372,000 and $993,000.

Average productivity gains for SecOps tasks

23.0% to 46.7%

> “The most important, high-level benefit is that we have this tremendously dedicated, capable person in our team — [Security Copilot] has all of the answers to all of our important questions. … We get that knowledge into our processes and within the team in a matter of seconds rather than days or weeks or [longer].”
>
> **CHIEF TECHNOLOGY OFFICER, ENERGY**

- **Cost efficiencies from SecOps centralization.** The capabilities provided by Security Copilot empower SecOps teams to reduce their reliance on third-party services. Over three years, this benefit is worth between $86,000 and $257,000.

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

- **A more empowered SecOps employee experience.** Security Copilot contributes to an enhanced security employee experience, improving recruitment, onboarding, morale, and retention within SecOps teams.
- **Rapid time to value.** With its easy deployment and user-friendly design, Security Copilot enables the composite organization to achieve meaningful results quickly, with minimal setup and training time.
- **An enhanced general employee experience.** Improved security measures and faster incident resolution provide a better experience for general employees, with fewer disruptions and faster recovery times, especially in response to phishing incidents.

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

- **Security Copilot consumption fees.** The composite organization provisions five security compute units (SCUs) from Microsoft at an annual cost of $175,200. The present value of the projected cost over three years is $436,000.

- **Training and learning.** Security Copilot users spend some time receiving training and learning in the course of their work with the solution. The projected cost over three years is $69,000.

Forrester modeled a range of projected low-, medium-, and high-impact outcomes based on evaluated risk. This range reflects both the variance in impacts observed across interviewed organizations and survey respondents, as well as the potential impact on the composite organization driven by the level of adoption, integration, and breadth of use cases for Security Copilot. This financial analysis projects that the composite organization accrues the following three-year net present value (NPV) for each scenario by enabling Security Copilot:

- Projected high impact of a $1.76 million NPV and projected ROI of 348%.
- Projected medium impact of a $1.13 million NPV and projected ROI of 224%.
- Projected low impact of a $500,000 NPV and projected ROI of 99%.

“Security Copilot is leveling the playing field. The people who just started … are able to provide a level of expertise that normally would have taken a couple of years to actually build out.”

DIRECTOR OF CYBER DEFENSE, MANUFACTURING

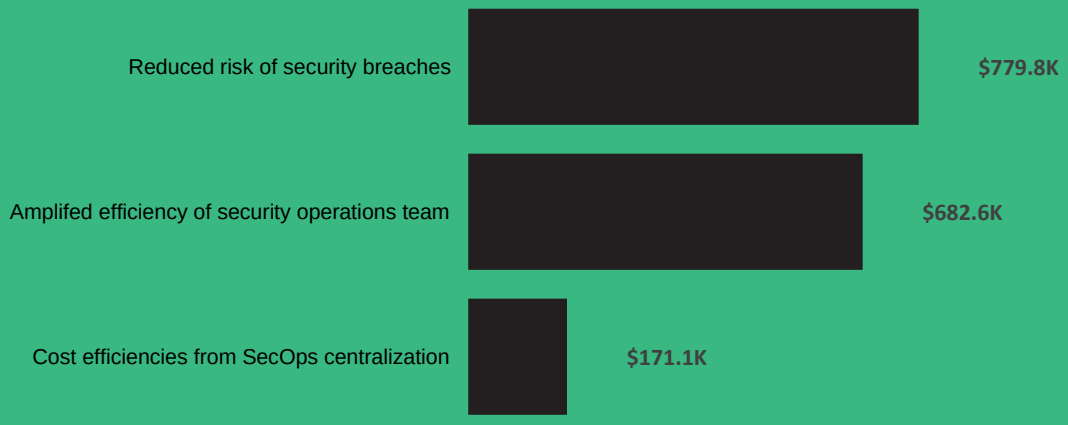
PROJECTED ROI
99% to 348%

PROJECTED BENEFITS PV
$1.00M to $2.26M

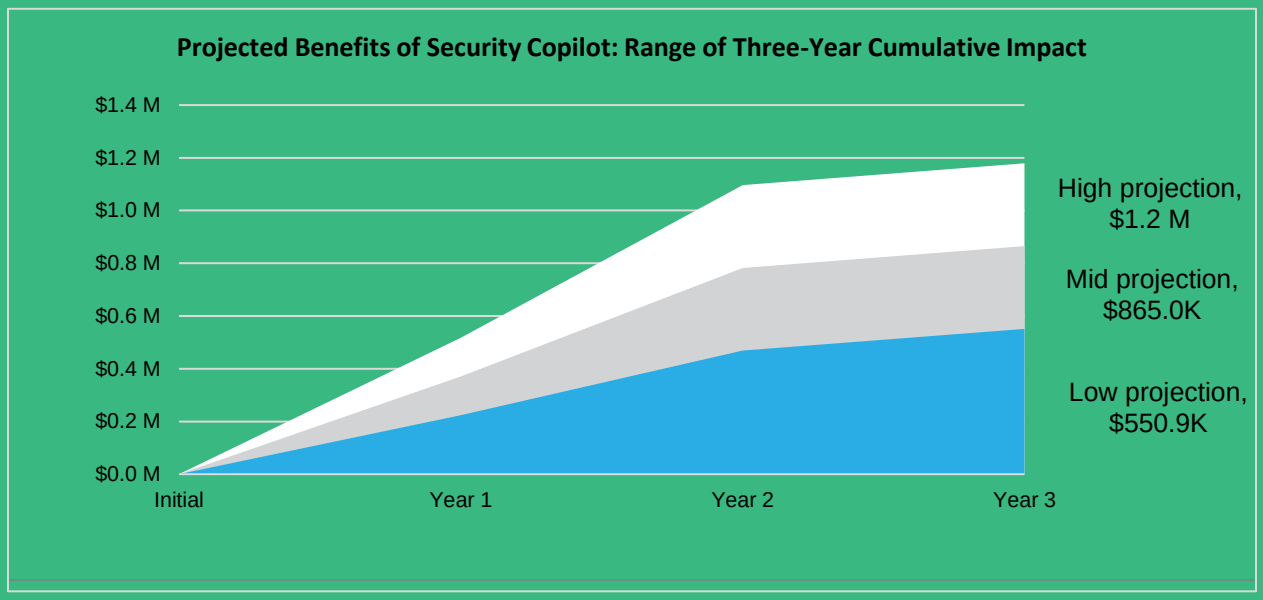
PROJECTED NET PRESENT VALUE
$500K to $1.76M

TOTAL COSTS
$504K

Projected Benefits (Three-Year)



Figures in chart are projections for mid-case scenario.



TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews and survey, Forrester constructed a New Technology: Projected Total Economic Impact™ (New Tech TEI) framework for those organizations considering adopting Security Copilot.

The objective of the framework is to identify the potential cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the projected impact that Security Copilot can have on an organization.

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 adopting Security Copilot.

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

Microsoft provided the customer names for the interviews but did not participate in the interviews. Forrester fielded the double-blind survey using a third-party survey partner.

1. **Due Diligence**
   Interviewed Microsoft stakeholders and Forrester analysts to gather data relative to Security Copilot.
2. **Early-Implementation Interviews And Survey**
   Interviewed four representatives at organizations using Security Copilot in a pilot or beta stage and surveyed 307 respondents from organizations with experience using Security Copilot to obtain data about projected costs, benefits, and risks.
3. **Composite Organization**
   Designed a composite organization based on characteristics of the interviewees' organizations.
4. **Projected Financial Model Framework**
   Constructed a projected financial model representative of the interviews and survey using the New Tech TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewees and survey respondents.
5. **Case Study**
   Employed four fundamental elements of New Tech TEI in modeling the investment's potential 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 Security Copilot Customer Journey

Drivers leading to adopting the Microsoft Security Copilot

Interviews					
Role	**Industry**	**Region**	**Annual revenue**	**Employees**	**Employees in SecOps team**
Director of cyber defense	Manufacturing	Global	$57B	38,000	20
Chief technology officer	Energy	Europe	$2B	1,400	10
Chief information security officer	Insurance	North America	$790M	3,000	4
Senior manager of cyber defense	Financial services	Asia Pacific	N/A	1,500	23

KEY CHALLENGES

Before adopting Microsoft Security Copilot, the interviewees' organizations managed their security operations using a mix of tools from Microsoft and other vendors, as well as other third-party managed services. While these tools provided a certain level of integration, they did not form a completely unified system or offer extensive automation, requiring substantial manual effort and coordination to operate efficiently. Interviewees noted that their organizations faced several common challenges, including:

- **Concerns about data security and usage.** Interviewees said they were hesitant to adopt generative AI (genAI) tools due to questions about data security, privacy, and control. The chief technology officer at an energy company explained that there were concerns in using genAI solutions, "[We wondered] what we would need to do to our information prior to onboarding to the service so that we could share as much as we'd like with the service without jeopardizing our business."
- **Uncoordinated security tools and processes.** Interviewees' organizations struggled to coordinate multiple security tools and platforms, leading to inefficiencies and potential gaps in security posture. Managing a blend of

systems often required substantial manual intervention, impacting response times and overall operational efficiency.

- **Inefficient threat detection and response.** With limited automation, security operations were often slowed by manual processes. Analysts spent time crafting queries and performing repetitive tasks, which reduced response times and increased the risk of extended dwell time for undetected threats.
- **Reliance on third-party managed services.** Due to limited in-house capabilities, some organizations depended on third-party security operations centers (SOCs) and other managed services to supplement their security operations. This reliance on external providers, while helpful, presented challenges in maintaining consistent threat visibility and optimizing response times.
- **Skill gaps and upskilling challenges among security personnel.** As cyberthreats grew more complex, interviewees' organizations found it challenging to train junior analysts to handle more advanced tasks like KQL querying. The learning curve posed a significant challenge for junior analysts, which placed additional strain on senior team members and impacted overall efficiency.
- **Challenges in attracting/retaining talent and having too much work.** Interviewees noted a very competitive landscape for attracting and retaining qualified talent to meet their organizational needs. The director of cyber defense at a manufacturing firm summarized, "We all face the same challenges of too much work, not enough people."

These challenges underscored the need for a more integrated, automated, and user-friendly security solution that could streamline operations, enhance threat detection and response capabilities, and bridge the skill gaps within security teams.

> "[With Security Copilot], we were able to provide even our most skeptical security employees with a tool where they could broaden their horizon in a very meaningful way."
>
> CHIEF TECHNOLOGY OFFICER, ENERGY

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 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 organization with annual revenue of $1 billion, 10,000 employees, and a 20-person SecOps team.

KEY ASSUMPTIONS

10,000 employees

$1 billion annual revenue

20-person SecOps team

> "Leadership [asked]: 'How long is it going to take to use [Security Copilot] and get a benefit from it?' … I'd say within 60 days, it pretty much paid for itself."
>
> CHIEF INFORMATION SECURITY OFFICER, INSURANCE

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits					
Benefit	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Total projected benefits (low)	$223,920	$468,439	$550,939	$1,243,298	$1,004,632
Total projected benefits (mid)	$370,656	$782,512	$865,012	$2,018,179	$1,633,560
Total projected benefits (high)	$517,392	$1,096,584	$1,179,084	$2,793,061	$2,262,488

THE REDUCED RISK OF SECURITY BREACHES

Evidence and data. Interviewees and survey respondents reported that Security Copilot substantially improved their organizations' ability to proactively detect and respond to security threats. By leveraging Security Copilot's automation and integration capabilities, teams could conduct significantly more threat-hunting activities, access and analyze a broader set of data, and respond to incidents more rapidly. These enhancements led to a noticeable reduction in security breaches and a marked improvement in their overall security posture, with organizations surpassing traditional limitations in their detection and response processes.

- Forrester's research shows that for organizations with annual revenue of $1 billion to $10 billion, the likelihood of experiencing one or more breaches per year is 69%.[2] The mean cumulative cost of breaches is $3.2 million.[3]
- The chief information security officer at an insurance firm shared: "We were already starting to transition into what I would consider proactive threat hunting and things like that. Before Copilot … we were doing a couple hundred [and] in a good month, probably 400 threat hunt campaigns internally. … [With] Copilot — 4,486 a month. That's actually now the norm, and the reason is because of how

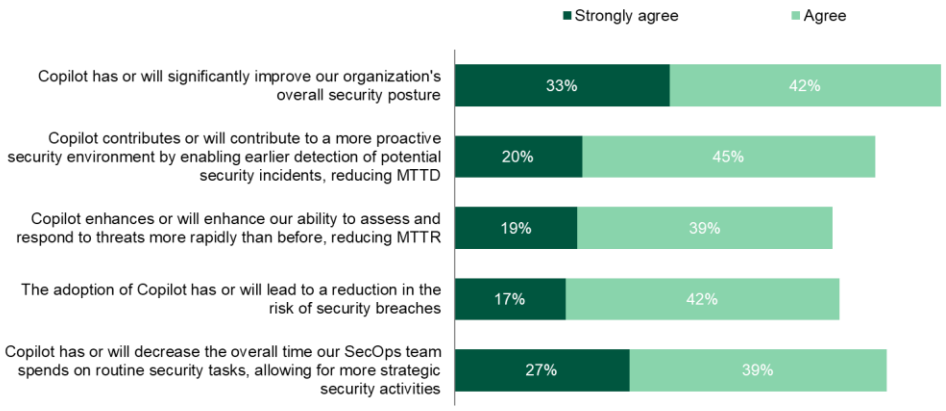
fast and integrated Copilot is to go and do these things. … So it's definitely, rapidly enhanced our posture on that in a major way."

- The chief information security officer added: "I have a really good team. We have experienced things without Copilot and with Copilot. Copilot has probably enhanced the response time by at least half the time. In certain scenarios, if you automate it, the response time is instantaneous. … Obviously, it's a game changer. Nothing can react faster than that."
- The senior manager of cyber defense in financial services explained that Security Copilot enabled their team to efficiently access and analyze data from their expanded log retention, which covers three months of hot storage and nine months of warm storage. Copilot's capabilities made it feasible to conduct comprehensive investigations spanning a full year, surpassing traditional security information and event management (SIEM) limitations and significantly enhancing their overall security posture.
- The director of cyber defense at a manufacturing firm said: "We did go through a fairly painful incident a couple weeks ago and we used the heck out of Security Copilot — everybody was hunting, pulling together queries trying to figure out what was going on, and getting data. Security Copilot was a huge benefit in that actual incident setting where we were working 24/7 trying to solve a problem."
- The chief technology officer at an energy company said, "We've dramatically changed our approach to how we do security operations, thereby dramatically increasing our security posture overall."

In the survey of SecOps decision-makers, respondents saw improvements in:

- **Threat detection and response.** Seventy-six percent of respondents saw an enhancement in or expected Security Copilot to enhance threat detection and response. KPI improvements included an average reduction in mean time to detect of 18.6% and an average reduction in mean time to respond of 12.3%.
- **The number of security breaches.** Seventy-seven percent of respondents reported that security breaches were reduced between 5% and 25%; 18% of respondents reported a reduction of between 26% to 50%. The overall average reduction after adopting Security Copilot was 17.4%.

“How much do you agree with the following statements?”



Base: 276 security operations (SecOps) decision-makers at organizations that use Microsoft Security Copilot
Source: New Technology: The Projected Total Economic Impact of Microsoft Security Copilot, a commissioned study conducted by Forrester Consulting

Modeling and assumptions. Based on the interviews and Forrester’s research, Forrester assumes the following about the composite organization:

- The likelihood of experiencing one or more breaches per year is 69%.
- The mean cumulative cost of breaches is $3.2 million per year.
- In the medium scenario, the composite organization achieves an 8.7% reduction in the risk of a security breach in Year 1 as it expands Security Copilot usage across its SecOps team and use cases; it achieves the 17.4% average breach risk reduction reported by survey respondents in Year 2.
- The high and low scenarios adjust the medium scenario’s breach risk reduction by plus and minus 30%, respectively, to capture central tendencies in the survey responses while excluding outliers. This approach provides a realistic representation of likely risk reduction outcomes, based on a range of results observed in the data.

Results. This yields a three-year projected PV ranging from $547,000 (low) to $1.0 million (high).

> "We spent a lot of time trying to address our email security posture over the last year, and we've seen a really significant decrease in the number of incidents. … That was such a big problem for us [and] now that we've got that solved, we're thinking what other measures do we need to focus on."
>
> DIRECTOR OF CYBER DEFENSE, MANUFACTURING

The Reduced Risk Of Security Breaches					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Likelihood of experiencing one or more breaches per year	Forrester research	69%	69%	69%
A2	Mean cumulative cost of breaches	Forrester research	$3,196,000	$3,196,000	$3,196,000
A3	**Subtotal: Annual risk exposure addressable with Security Copilot**	**A1*A2**	**$2,205,240**	**$2,205,240**	**$2,205,240**
$A4_{Low}$	Reduced risk of breaches attributed to Security Copilot	Survey	6.1%	12.2%	12.2%
$A4_{Mid}$			8.7%	17.4%	17.4%
$A4_{High}$			11.3%	22.6%	22.6%
At_{Low}	Savings from the reduced risk of security breaches	A3*A4	$134,520	$269,039	$269,039
At_{Mid}			$191,856	$383,712	$383,712
At_{High}			$249,192	$498,384	$498,384
Three-year projected total: $672,598 to $1,245,961			**Three-year projected present value: $546,770 to $1,012,870**		

THE AMPLIFIED EFFICIENCY OF THE SECOPS TEAM

Evidence and data. Interviewees and survey respondents reported that Security Copilot significantly enhanced the efficiency of their SecOps teams by streamlining workflows and offering automation; it also enabled them to rapidly upskill team members. By automating routine tasks and simplifying complex queries, Security Copilot allowed security analysts to focus on higher-value activities and handle complex tasks more efficiently. This increase in efficiency not only improved productivity but also reduced the need for additional staffing. The tool also empowered junior team members to perform tasks that previously required more-senior intervention, thereby enhancing the overall effectiveness of the team.

- Interviewees characterized the addition of Security Copilot as comparable to adding multiple personnel to the team. The chief technology officer at an energy company said: “We had plans [to hire] five more [to our team of 10] and we’ve decided to drop that and just continue our investment in Security Copilot.” They added: “On day-to-day [work], we save hours. What would take one person more than a day to achieve is done with one query today. It’s such a fundamental change that we really needed to work on changing our own mindset in approaching security pre- and post- Security Copilot because of the new capabilities.”
- The senior manager of cyber defense in financial services explained that, as a small team, one of the biggest benefits they gained from Security Copilot was in triage and alert contextualization. Analysts could engage in a dialogue with Copilot to unpack analytic rules they had never seen before, understand their purpose and use cases, and receive recommendations on the steps to take. This capability led to a significant shift in team dynamics; instead of constantly seeking assistance from more experienced colleagues, analysts began proactively determining and presenting appropriate actions. This interviewee said: “It was almost having like another senior analyst on the team to just get rid of that noise. … From that perspective, it’s been a massive game changer.”
- The chief information security officer at an insurance firm explained: “I hired a junior security analyst. I think he had four months of an internship in terms of security experience, and he is now functioning almost at the same level as a senior analyst. … Security Copilot really removed the barriers to learning and

applying that learning almost instantaneously for this person, and the same can be said for my senior analyst."

- The director of cyber defense at a manufacturing firm said: "For a lot of the work that the junior analysts were doing, they would ask Copilot as their first step when they were working on an incident. … The team really appreciated the fact that you could ask Copilot to craft KQL queries for you in Sentinel and Defender because that's one of the big challenges for the team. You have to know KQL to really use these tools, and it's a little bit of a pain to learn. … And now I've noticed … instead of just writing the KQL, Security Copilot can actually run the queries and get the data for you, which is great. … [Security Copilot] is allowing the junior analysts or newer people on the team to basically have the same type of analytic skills that the more advanced people would have because the Copilot can do the KQL work for them. … It's definitely taking the people who are junior and raising them up faster, and they're able to be more useful faster than before."

Some 71% of survey respondents reported an increase in the productivity of their SecOps team. Average time savings included:

- Suspicious script analysis: 47%.
- Building out workloads with natural language prompts: 42%.
- Summarizing alerts and incidents: 41%.
- Troubleshooting minor issues: 40%.
- Preparing reports: 39%.
- Incident prioritization, investigation, and response: 37%.
- Leveraging promptbooks: 37%.
- KQL querying: 35%.
- Threat hunting: 33%.
- Processing and resolving help desk calls/tickets: 28%.
- Vulnerability impact assessment: 25%.
- Threat intelligence assessment: 23%.

In addition, 62% of survey respondents noted that Security Copilot helped them upskill junior staff. Of these respondents:

- Seventy-nine percent agreed or strongly agreed that Security Copilot has allowed or will allow the organization to upskill Level 1 (L1) analysts to handle more complex security operations faster than traditional methods.
- Sixty-nine percent agreed or strongly agreed that Security Copilot has enabled or will enable L1 analysts to independently resolve issues that previously required escalation to more senior personnel.
- Sixty-eight percent agreed or strongly agreed that Security Copilot has enabled or will enable L1 analysts to efficiently complete tasks typically assigned to Level 2 analysts.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- In Year 1, 10 FTEs utilize Security Copilot; usage climbs to 15 FTEs in Years 2 and 3.
- In Year 1, streamlined workflows, automation, and upskilling results in net productivity and efficiency gains ranging from 5% to 15% as the organization ramps up usage of Security Copilot and integrates the solution into daily activities.
- In Year 2, net productivity and efficiency gains climb to 10% to 30% as the primary use cases are fully implemented for the full year.
- In Year 3, these gains increase an additional 5% as the organization extends Security Copilot to additional use cases and further integrates the solution into standard practices across the team.
- The average fully burdened annual salary for the FTEs using Security Copilot is $110,000.

Results. This yields a three-year projected PV ranging from $372,000 (low) to $993,000 (high).

> "A junior analyst just asked Copilot to explain it like I'm 5 years old and boom, I had something I could bring to our CEO and tell them what's going on … and they were able to understand fairly advanced security language and the context. That made them make some really good decisions that we wouldn't [have achieved otherwise] because we'd be stuck talking tech to a CEO and that doesn't work."
>
> CHIEF TECHNOLOGY OFFICER, ENERGY

The Amplified Efficiency Of The SecOps Team

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	SecOps FTEs using Security Copilot	Composite	10	15	15
$B2_{Low}$	Net productivity and efficiency gains from streamlined workflows, automation, and upskilling from Security Copilot	Interviews and survey	5%	10%	15%
$B2_{Mid}$			10%	20%	25%
$B2_{High}$			15%	30%	35%
B3	Average fully burdened annual salary for an FTE using Security Copilot	TEI standard	$110,000	$110,000	$110,000
Bt_{Low}	Amplified efficiency of SecOps team	B1*B2*B3	$55,000	$165,000	$247,500
Bt_{Mid}			$110,000	$330,000	$412,500
Bt_{High}			$165,000	$495,000	$577,500
Three-year projected total: $467,500 to $1,237,500			**Three-year projected present value: $372,314 to $992,975**		

COST EFFICIENCIES FROM SECOPS CENTRALIZATION

Evidence and data. Interviewees and survey respondents reported significant cost efficiencies from enhancing their internal capabilities with Security Copilot. By reducing their reliance on or eliminating some legacy third-party services, their organizations achieved measurable reductions in spending on outsourced services.

- The chief technology officer at an energy company said: “Because of the capabilities provided in [Security Copilot], we decided last year to home-source our SOC team. Last year, we discontinued our third-party SOC team and we cancelled the contract. We now have all of these capabilities on our own turf with our own people. ... We were able to achieve a much faster rate of incident management when we home-sourced it with this product than what the market was capable of delivering to us as a service.”
- The chief technology officer added that this action saves the organization over $200,000 annually and has improved key metrics: “We have reduced the time it takes from when an issue arises to it being solved by several hours. [With the] outsourced SOC, it could be 7 to 10 hours between there being an incident in the logs, us getting the message, being able to understand it, and fully resolve it, whereas today, it takes less than 10 minutes to resolve our cases. It’s such a dramatic change in our approach to everything.”

The survey data revealed how Security Copilot enabled SecOps decision-makers to reduce their reliance on managed services.

- A number of survey respondents said they have reduced or plan on reducing or eliminating the following managed services: managed detection and response (57%); security information and event management (53%); managed security operations center (49%); threat intelligence (41%); and incident response (39%).
- Survey respondents reported average savings of $206,000 from reducing or eliminating managed/professional services with Security Copilot; 59% reported savings greater than $100,000.
- Survey respondents also reported average savings of $59,000 from sunsetting tools and technologies no longer needed thanks to Security Copilot, with 49% reporting savings greater than $50,000.

> “The enhancement that came with the threat intelligence and analytics capabilities that are brought on with [Security Copilot] made us absolutely certain there we were capable of doing it all ourselves and not have a partner run the SOC for us.”
>
> CHIEF TECHNOLOGY OFFICER, ENERGY

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite organization reduces its reliance on or eliminates some third-party security services and saves $206,000 over three years.
- The high and low scenarios adjust the medium scenario savings by plus and minus 50%, respectively, to capture central tendencies in the survey responses while excluding outliers. This approach provides a realistic representation of likely cost efficiencies, based on a range of outcomes observed in the data.

Results. This yields a three-year projected PV ranging from $86,000 (low) to $257,000 (high).

Cost Efficiencies From SecOps Centralization					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
$C1_{Low}$	Cost reduction from reduced reliance on or elimination of third-party security services	Survey	$34,400	$34,400	$34,400
$C1_{Mid}$			$68,800	$68,800	$68,800
$C1_{High}$			$103,200	$103,200	$103,200
Ct_{Low}	Cost efficiencies from SecOps centralization	C1	$34,400	$34,400	$34,400
Ct_{Mid}			$68,800	$68,800	$68,800
Ct_{High}			$103,200	$103,200	$103,200
Three-year projected total: $103,200 to $309,600			**Three-year projected present value: $85,548 to $256,643**		

UNQUANTIFIED BENEFITS

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

- **A more empowered SecOps employee experience.** Interviewees highlighted that Security Copilot brought about a cultural shift within their SecOps teams, transforming the nature of their work and creating a more empowered employee experience. By reducing repetitive manual tasks and supporting upskilling, Security Copilot has enabled team members to focus on higher-impact responsibilities, leading to improved recruitment, onboarding, morale, and retention. The director of cyber defense at a manufacturing firm noted: “It’s an interesting transition. The team has been very used to grunt work, and we’re really working on upskilling, so there’s been a cultural change.”
    - Seventy-three percent of survey respondents indicated they are or expect to be more successful in attracting talent due to hands-on experience with Security Copilot. The chief technology officer at an energy company noted: “One other unforeseen benefit of [Security Copilot] is the attention [we get] once other organizations know that we’ve been playing with this [solution] — the attraction that we get as a company and [the number of] people that want to join our team has dramatically increased. … It’s really been

drawing attention to us as a modern company where we approach, in a meaningful way, the threat landscape and our security posture. We've been able to attract new talent because of this."

- Survey respondents said onboarding new hires has or will become, on average, 11.5% faster with Security Copilot. Interviewees noted that the ramp-up time dropped from months to weeks. The chief technology officer commented: "We very recently hired one person to the security team, and normally it would take us approximately six months to get the person operating. Now it was less than one week. … He's now on a senior level of our security operations team and he was very junior when he entered a couple of months back."
- Sixty-nine percent of survey respondents attributed or expect to attribute improved employee experience and retention to Security Copilot, with an average 20.4% reduction in the annual turnover/attrition rate for SecOps staff. The director of cyber defense at a manufacturing firm shared: "The team is really happy that they're playing with state-of-the-art technology. … We really do try and give the team access to the best technology and tools, [and that] is one of the reasons why they like being here. We've had very low turnover in the last two years … [Security Copilot] is one of many reasons right why they like to continue working in our SOC."

- **Rapid time to value.** Interviewees noted Security Copilot's easy deployment and user-friendly design, which allowed rapid adoption and time to value. The chief information security officer stated, "We started using [Security Copilot] in our live environment right away and immediately saw its impact on our security posture." The chief technology officer at an energy company said: "Implementation really was checking a couple of things in the portal, wait for 48 hours, and then … you're good. We had a week of workshops with the team, and then we were off running. That's really all the adoption we needed. … We were able to quickly gain some momentum in using the capabilities of the product to enhance our security posture and our journey."
- **An enhanced general employee experience.** Improved security measures and quicker resolution of incidents contributed to a better overall experience for general employees, with fewer disruptions and faster resolution times, especially

in handling phishing incidents. The director of cyber defense at a manufacturing firm explained that these improvements have reduced the downtime associated with this kind of security issue by half.

> "The guy that runs my security operations team was shocked at how seamless it was to get [Security Copilot] up and going. … It was not cumbersome at all to get it stood up. I think the longest part of it was just the paperwork."
>
> CHIEF INFORMATION SECURITY OFFICER, INSURANCE

FLEXIBILITY

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

- **Elevated agility and future-readiness.** Interviewees discussed how Security Copilot provides the agility and future-readiness that modern SecOps teams need to stay ahead of evolving threats and technological advances. The senior manager of cyber defense in financial services explained that adopting Security Copilot early has positioned their team to be "miles ahead" as the technology matures. They also noted that Copilot has become a tool to "amplify our capability," allowing the team to handle a broader range of security challenges with greater efficiency.
- **Increased risk tolerance and growth opportunities.** Security Copilot has also enabled organizations to take on new initiatives with higher confidence in their security posture. Sixty-seven percent of survey respondents reported that Security Copilot has helped or will help reduce security-related barriers to growth,

while 63% indicated increased customer or stakeholder confidence in their security measures.

The chief information security officer at an insurance firm shared an example, stating, “We moved three initiatives up at the end of last year that weren’t supposed to start until this year, thanks to the support from Security Copilot.”

The chief technology officer at an energy company described how Security Copilot unlocked new service offerings in a traditionally conservative organization considered part of the country’s critical infrastructure: “The trust that we’ve built in with [Security Copilot] enables us to really accelerate service development. We’ve even told the board of directors that we can accept a higher level of risk because of this security capability. … We’ve spun off a couple of new companies … [since we adopted Security Copilot], bringing new services and business in a secure and scalable manner. … We know that what we weren’t capable of last year, we are now capable of. It’s a game changer, both for the core IT team that’s now a business enablement team and for the board of directors to take us to the next level.”

- **Expanded opportunities for operational efficiency gains.** The chief technology officer also highlighted Security Copilot’s potential to optimize business operations on a large scale: “Because we’re able to use a modern, secure platform, we believe we can optimize our entire production chain by at least 30% within the next three years. This means we can produce and transport 30% more energy and build more infrastructure. … Security Copilot has given us the trust and assuredness needed to take these kinds of bold steps in a safe, secure manner.”

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A).

> “[Security Copilot] definitely transformed how the IT group is perceived as we move from this traditional IT team that’s always been lagging and always been ‘the guys who say no’ to the team that enables business growth and development. We even had to change the name from IT to the business enablement team.”
>
> CHIEF TECHNOLOGY OFFICER, ENERGY

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Dtr	Annual Security Copilot consumption fees	$0	$175,200	$175,200	$175,200	$525,600	$435,696
Etr	Training and learning	$22,260	$22,260	$16,695	$16,695	$77,910	$68,837
	Total costs (risk adjusted)	$22,260	$197,460	$191,895	$191,895	$603,510	$504,533

ANNUAL SECURITY COPILOT CONSUMPTION FEES

Evidence and data. Security Copilot operates within an organization's Azure environment, which enables a smooth deployment with minimal setup requirements. The pricing structure is currently set at $4 per hour for each security compute unit (SCU), allowing organizations to adjust compute power and capacity as needed. This intuitive model enables predicable cost management based on specific usage. Pricing may vary. Contact Microsoft for additional details.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- It provisions five SCUs.
- SCUs cost $4 per hour each.

Risks. No specific risks are noted, as the standard pricing model and deployment setup contribute to predicable costs across organizations.

Results. Forrester applied a 0% risk adjustment, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $436,000.

> "I was completely and utterly shocked at how common sense the cost structure of this was when it became public. I was so happy with Microsoft."
>
> CHIEF INFORMATION SECURITY OFFICER, INSURANCE

Annual Security Copilot Consumption Fees						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
D1	Security compute units provisioned	Composite		5	5	5
D2	Security compute unit cost per hour	Composite		$4	$4	$4
Dt	Annual Security Copilot consumption fees	D1*D2*24*365		$175,200	$175,200	$175,200
	Risk adjustment	0%				
Dtr	Annual Security Copilot consumption fees (risk-adjusted)			$175,200	$175,200	$175,200
	Three-year total: $525,600			**Three-year present value: $435,696**		

TRAINING AND LEARNING

Evidence and data. Interviewees stated that Security Copilot is intuitive and easy to learn, with users quickly becoming proficient due to its natural language interface. Some interviewees indicated that users participated in initial workshops, while others developed their skills through hands-on experience. The director of cyber defense at a manufacturing firm said: "In a couple of days to a week, you should be able to be fairly competent on it because it's natural language. You just ask it stuff."

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- Ten members of the SecOps team receive 40 hours of training and learning activities in the first six months; the remaining 10 members receive 40 hours of training by the end of Year 1.

- The 15 primary Security Copilot users receive 20 hours of training and learning activities in Years 2 and 3.
- The fully burdened hourly rate for a member of the SecOps team is $53.

Risks. This cost can vary across organizations due to differences in:

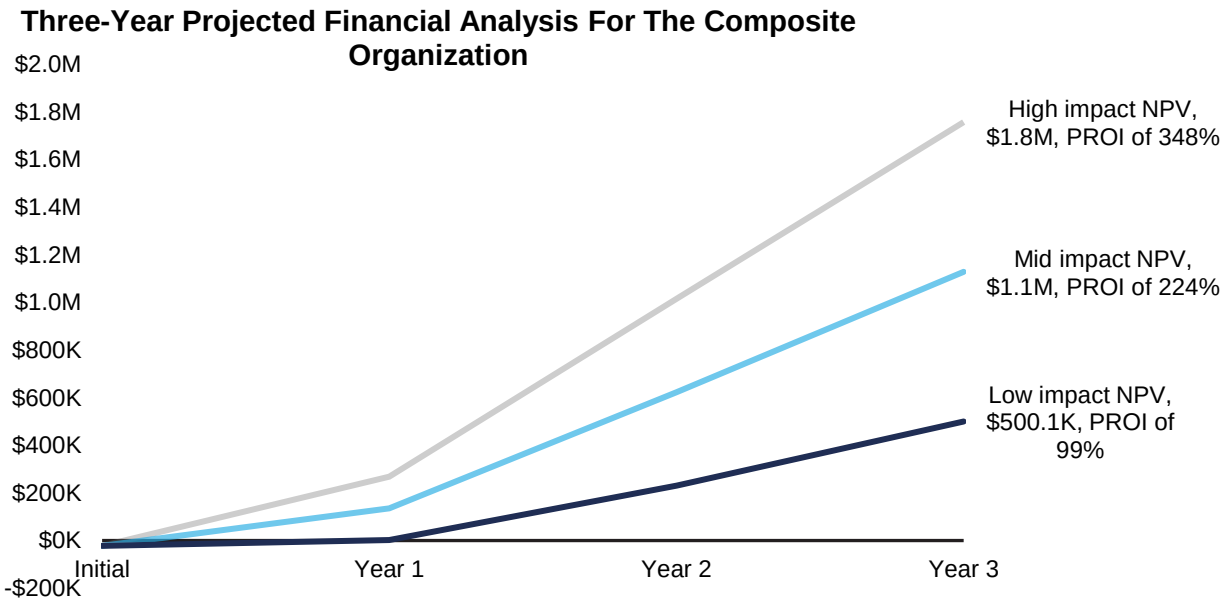
- A team's familiarity with genAI or natural language technology.
- Variability in initial user adoption rates

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $69,000.

Training And Learning						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Total security operations FTEs using Security Copilot	Composite	10	10	15	15
E2	Training and learning time per FTE (hours)	Interviews	40	40	20	20
E3	Fully burdened hourly rate for a SecOps FTE	Composite	$53	$53	$53	$53
Et	Training and learning	E1*E2*E3	$21,200	$21,200	$15,900	$15,900
	Risk adjustment	↑5%				
Etr	Training and learning (risk-adjusted)		$22,260	$22,260	$16,695	$16,695
	Three-year total: $77,910			**Three-year present value: $68,837**		

Financial Summary

Consolidated Three-Year, Risk-Adjusted Metrics



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

These risk-adjusted PROI and projected NPV values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Analysis (Risk-Adjusted)						
	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($22,260)	($197,460)	($191,895)	($191,895)	($603,510)	($504,533)
Total benefits (low)	$0	$223,920	$468,439	$550,939	$1,243,298	$1,004,632
Total benefits (mid)	$0	$370,656	$782,512	$865,012	$2,018,179	$1,633,560
Total benefits (high)	$0	$517,392	$1,096,584	$1,179,084	$2,793,061	$2,262,488
Net benefits (low)	($22,260)	$26,460	$276,544	$359,044	$639,788	$500,099
Net benefits (mid)	($22,260)	$173,196	$590,617	$673,117	$1,414,669	$1,129,027
Net benefits (high)	($22,260)	$319,932	$904,689	$987,189	$2,189,551	$1,757,955
PROI (low)						99%
PROI (mid)						224%
PROI (high)						348%

APPENDIX A: NEW TECHNOLOGY: PROJECTED TOTAL ECONOMIC IMPACT

New Technology: Projected Total Economic Impact (New Tech TEI) 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 New Tech TEI methodology helps companies demonstrate and justify the projected tangible value of IT initiatives to both senior management and other key business stakeholders.

Total Economic Impact Approach

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

Projected Costs consider all expenses necessary to deliver the proposed value, or benefits, of the product. The projected cost category within New Tech 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.

Projected Net Present Value (NPV)

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

Projected 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

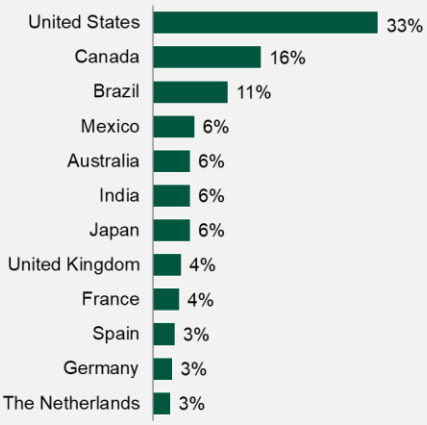
The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

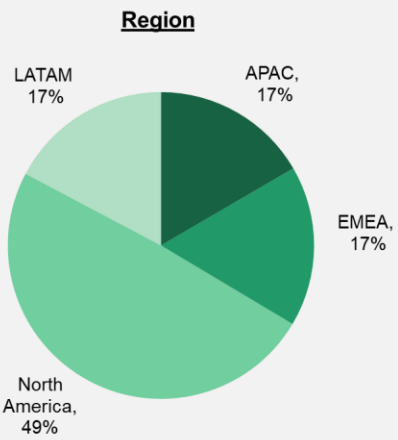
The initial investment column contains costs incurred at “time 0” or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations in the 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.

APPENDIX B: INTERVIEW AND SURVEY DEMOGRAPHICS

Interviews					
Role	**Industry**	**Region**	**Annual Revenue**	**Employees**	**Employees In SecOps Team**
Director of cyber defense	Manufacturing	Global	$57B	38,000	20
Chief technology officer	Energy	Europe	$2B	1,400	10
Chief information security officer	Insurance	North America	$790M	3,000	4
Senior manager of cyber defense	Financial services	APAC	n/a	1,500	23

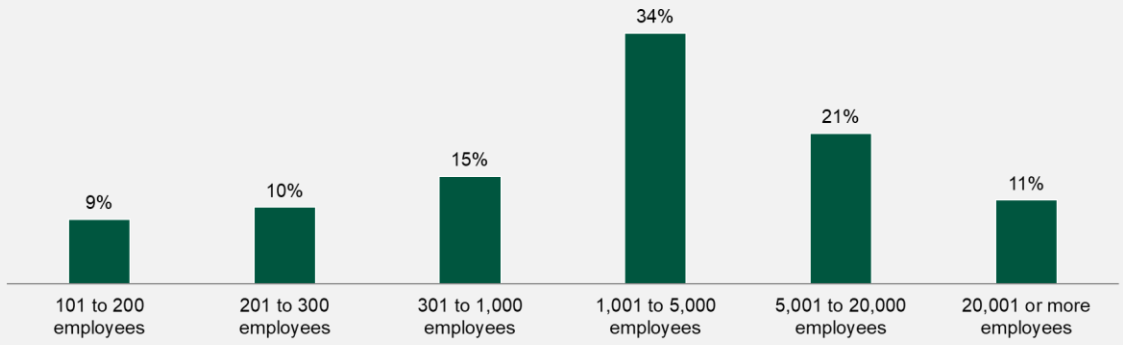
"In which country are you located?"





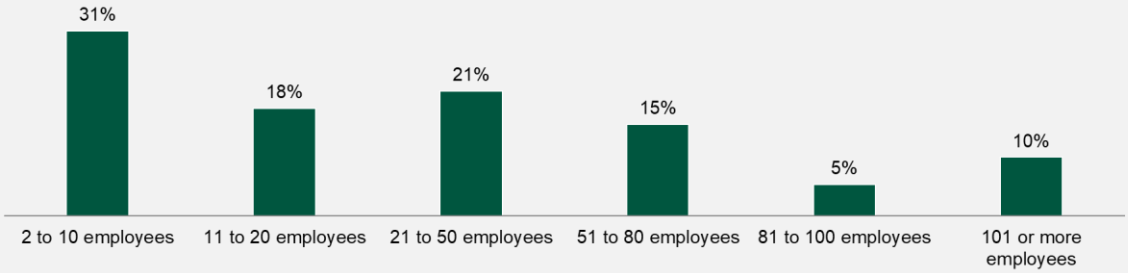
Base: 307 security operations (SecOps) decision-makers at organizations that use Microsoft Security Copilot
Note: Percentages do not total 100 because of rounding.
Source: New Technology: The Projected Total Economic Impact of Microsoft Security Copilot, a commissioned study conducted by Forrester Consulting

“How many employees work for your firm/organization worldwide?”



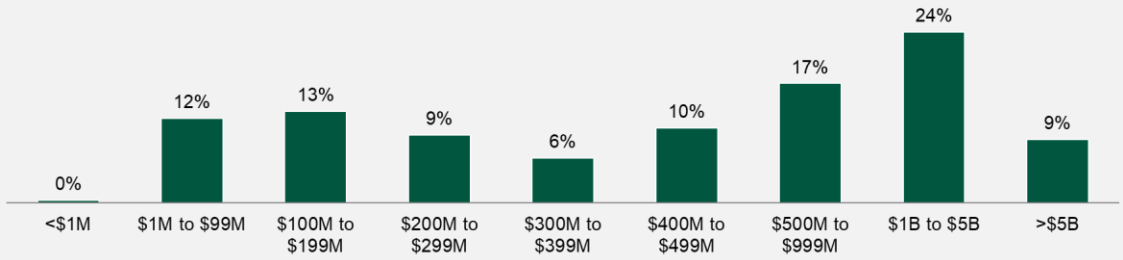
Base: 307 security operations (SecOps) decision-makers at organizations that use Microsoft Security Copilot
Source: New Technology: The Projected Total Economic Impact of Microsoft Security Copilot, a commissioned study conducted by Forrester Consulting

“How many employees are on your SecOps team?”



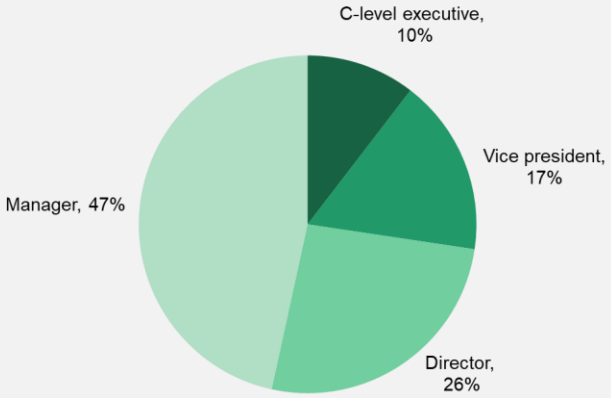
Base: 307 security operations (SecOps) decision-makers at organizations that use Microsoft Security Copilot
Source: New Technology: The Projected Total Economic Impact of Microsoft Security Copilot, a commissioned study conducted by Forrester Consulting

“What is your organization’s annual revenue (US$)?”



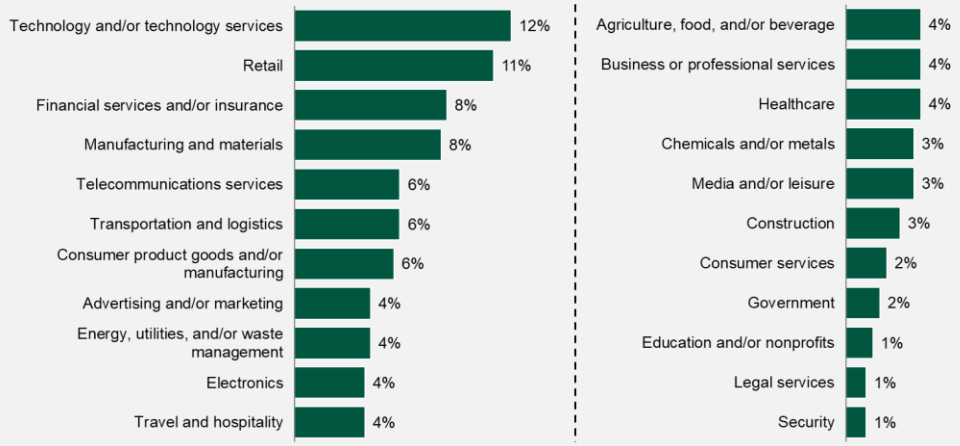
Base: 307 security operations (SecOps) decision-makers at organizations that use Microsoft Security Copilot
Source: New Technology: The Projected Total Economic Impact of Microsoft Security Copilot, a commissioned study conducted by Forrester Consulting

“Which title best describes your position at your organization?”



Base: 307 security operations (SecOps) decision-makers at organizations that use Microsoft Security Copilot
Source: New Technology: The Projected Total Economic Impact of Microsoft Security Copilot, a commissioned study conducted by Forrester Consulting

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



Base: 307 security operations (SecOps) decision-makers at organizations that use Microsoft Security Copilot
Note: Percentages do not total 100 because of rounding.
Source: New Technology: The Projected Total Economic Impact of Microsoft Security Copilot, a commissioned study conducted by Forrester Consulting

APPENDIX C: SUPPLEMENTAL MATERIAL

Related Forrester Research

Generative AI Use Cases For CISOs, Forrester Research, Inc., June 13, 2024.

Top Recommendations For Your Security Program, 2024, Forrester Research, Inc., March 4, 2024.

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.

[2] Base: 759 security decision-makers. Source: Forrester's Security Survey, 2024.

[3] Base: 511 security decision-makers. Source: Forrester's Security Survey, 2024.

FORRESTER®