FORRESTER®

BRILYANT

The Total Economic Impact™ Of Google SecOps

Cost Savings And Business Benefits Enabled By Google SecOps

A FORRESTER TOTAL ECONOMIC IMPACT STUDY
COMMISSIONED BY GOOGLE, JULY 2025

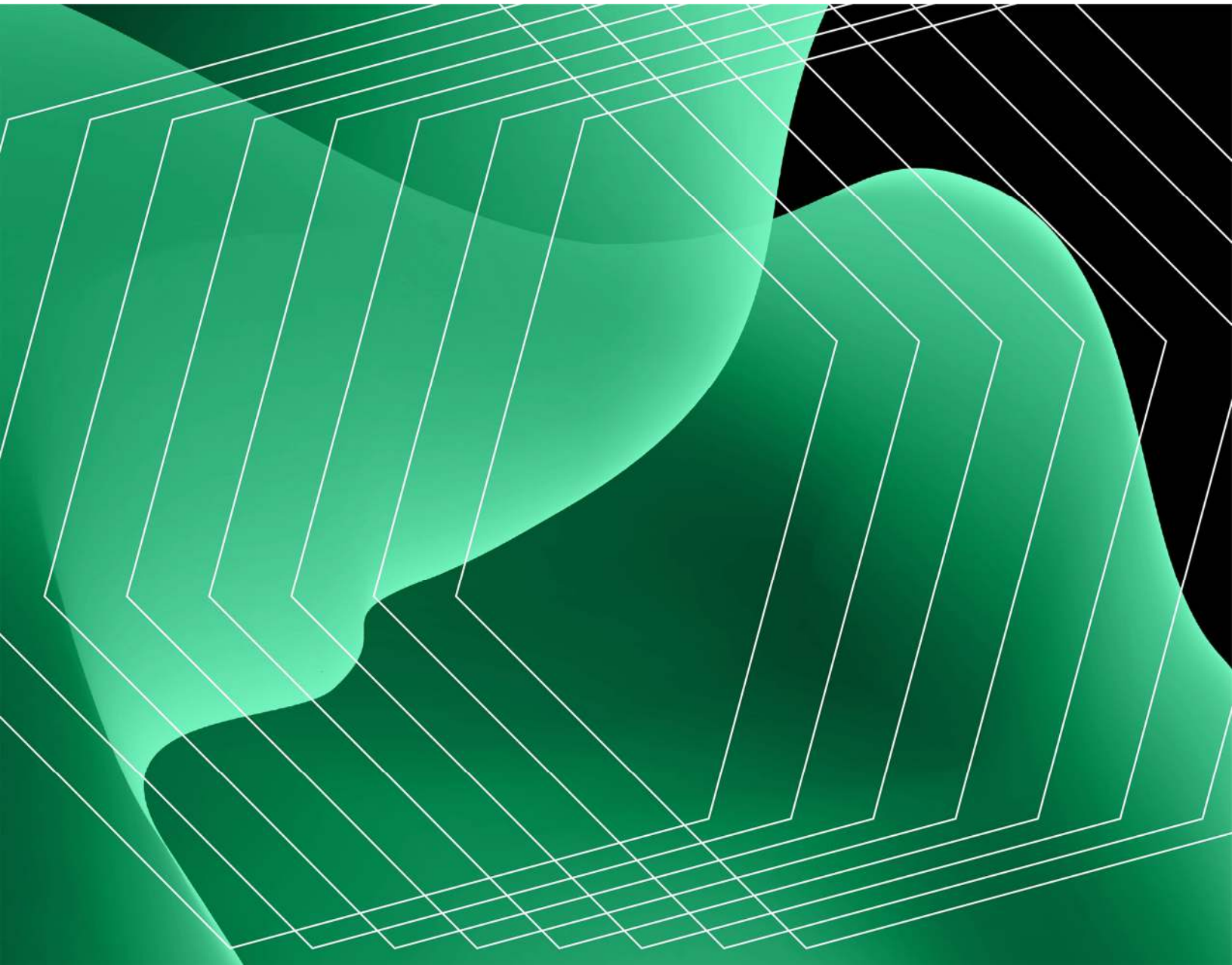


Table Of Contents

Consulting Team:

Matthew Carr

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

Security operations (SecOps) teams face an increasingly complex and fast-evolving threat landscape.[1] Organizations often struggle with fragmented tools, resource constraints, and operational inefficiencies that hinder their ability to detect, investigate, and respond to threats effectively. As a result, security leaders seek comprehensive solutions that provide agility, scalability, and automation to modernize security operations and reduce risk.

Google SecOps is a highly scalable, cloud-native platform that allows organizations to modernize their security operations and defend against evolving threats. It addresses operational inefficiencies by unifying security functions, automating manual processes, and enhancing visibility. The platform integrates advanced analytics, AI-driven insights, and frontline threat intelligence to help organizations achieve outcomes like faster and more accurate threat detection, accelerated investigation workflow to critical decision points, and rich, automated response operations.

Google commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Google SecOps.[2] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Google SecOps on their organizations.

Return on investment (ROI)
240%

Net present value
$4.3M

> "In simple terms, Google SecOps is a massive risk reducer. Threats that would have impacted our business no longer do because we have greater observability, better mean time to detect, and better mean time to respond."
>
> CISO, INSURANCE

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed five decision-makers across four organizations with experience using Google SecOps. For the purposes of this study, Forrester aggregated the experiences of the interviewees and combined the results into a single composite organization, which is a global enterprise with $8 billion in annual revenue and 25 employees on its SecOps team.

Interviewees said that prior to using Google SecOps, their organizations relied on legacy security tools that were fragmented, difficult to manage, and lacked the scalability needed to keep pace with a growing threat environment. These limitations led to operational inefficiency, insufficient visibility into threats, risk exposure, and vendor cost models that were difficult to sustain.

After the investment in Google SecOps, the interviewees reported a significant improvement to their security operations with a highly scalable solution that empowered their SecOps teams and resulted in more effective threat detection, investigation, and response. Key results from the investment include reduced risk, improved analyst productivity, and cost efficiency.

> "As a result of the move to Google SecOps, our security operations have matured exponentially. I wouldn't shift over from Google now if you paid me. It's very clinical in what it does, and we've saved so much time."
>
> SECURITY OPERATIONS LEAD, PROFESSIONAL SERVICES

KEY FINDINGS

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

- **Reduced risk and cost of a breach by 70%.** Google SecOps allows the composite organization to improve its security operations by increasing event ingestion, onboarding more log sources, increasing attack surface coverage through the scale of the platform, implementing more detection rules, enabling multistage detection modeling, and

prioritizing investigations. The breadth and depth of the platform's capabilities enable the SecOps team to evolve their day-to-day work and operate more proactively and efficiently. This translates into faster and more accurate threat detection, investigation, and response. The resulting reduced risk and cost of a breach is worth $2.8 million for the composite organization over three years.

- **Optimized security with faster investigation and response, reducing mean time to respond by 50% and mean time to investigate by 65%.** Google SecOps enables the composite organization to investigate and respond to threats more efficiently due to the platform's Unified Data Model; faster query and search capabilities; generative AI (genAI) assistance; access to 12 months of hot data by default with options for longer retention periods; integrated threat intelligence; automation with playbooks; and a reduction in false positives. These improvements reduce risk and save analyst time. The efficiency gains are worth $1.5 million for the composite organization over three years.
- **Empowered junior security analysts by shifting 35% of SecOps work and reducing time to productivity by 70%.** Google SecOps' ease of use and genAI capabilities empower junior SecOps analysts at the composite organization to take on more advanced responsibilities and quickly understand the platform's features. Work traditionally performed by more senior analysts is now handled by junior colleagues assisted by Gemini in SecOps, which can summarize alerts, provide recommendations, facilitate fast and comprehensive investigations, augment detection and playbook engineering with natural language, and analyze alert data with workflows for triage and assistive guidance. Google SecOps also shortens time to productivity for the composite's junior new hires, accelerating their ability to contribute to security operations. These benefits are worth $636,000 for the composite organization over three years.
- **Increased cost model predictability with Google and decommissioned legacy systems.** As a comprehensive and highly scalable solution that supports data from on-prem environments, Google Cloud, and other cloud providers, Google SecOps allows the composite organization to decommission its legacy on-prem security information and event management (SIEM), security orchestration, automation, and response (SOAR), user and entity behavior analytics (UEBA) platform, and custom data lake. This reduces operational complexity and saves costs. Additionally, the composite benefits from the simplified and more predictable pricing of Google SecOps, which offers tiered pricing packages based on organizational need. Decommissioning legacy systems saves $1.2 million for the composite organization over three years.

> "Google SecOps is a very scalable platform and very financially sustainable. It's also sustainable for our people because it does analyst legwork through its AI capabilities, which our analysts love."
>
> CISO, INSURANCE

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

- **Enhanced employee experience.** Google SecOps serves as a modern tool that engages the composite organization's SecOps team and reduces their time spent on mundane tasks.
- **Google partnership.** Google is an innovative partner for the composite organization and helps ensure smooth implementation and ongoing success.
- **Scalability.** Google SecOps is a highly scalable platform with the ability to meet the composite organization's needs as they grow and evolve over time.

> "Google SecOps allows us to do more with less — we're better at detecting and responding. But the other part of the equation is the innovation power of Google and all the puzzle pieces they put in place. And with Gemini and AI, we're working with a vendor that innovates fast."
>
> DEPUTY CISO, FINANCIAL SERVICES

"We really like Google SecOps. It's been a game changer in a very short period of time. … Migration was very easy; implementation was very easy."

CISO, INSURANCE

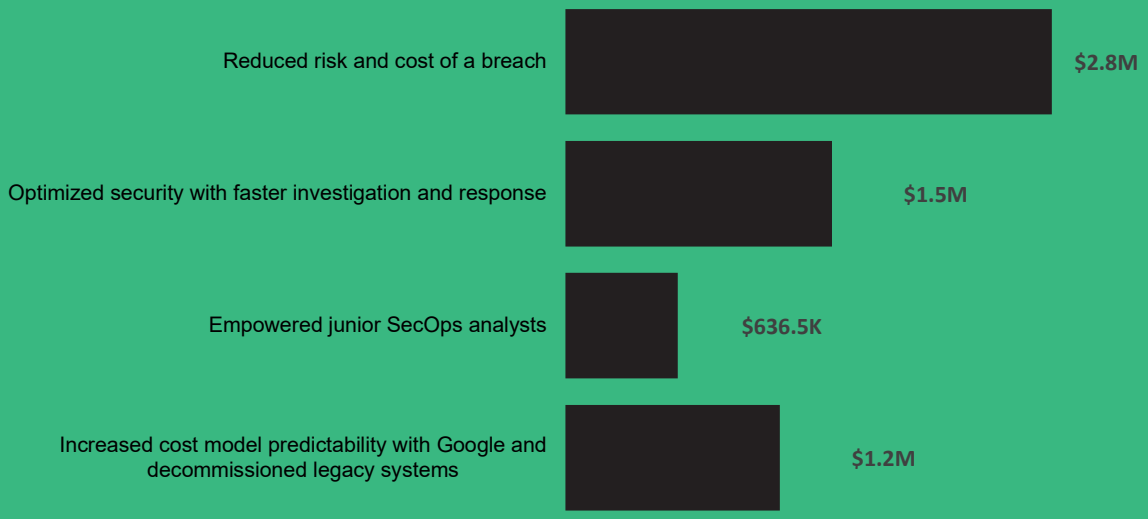
Costs. Three-year, risk-adjusted PV costs for the composite organization include:

- **Google SecOps licensing fees.** For the use of Google SecOps, the composite organization pays annual licensing fees to Google. These costs can vary by organization and depend on factors such as data volume and implementation scope. They total $1.4 million for the composite organization over three years.
- **Internal labor for implementation and ongoing maintenance.** A subset of the composite organization's SecOps team dedicates time to the implementation and ongoing maintenance of Google SecOps. Additionally, all team members participate in initial training on the platform. This employee time amounts to $371,000 for the composite organization over three years.

The financial analysis that is based on the interviews found that a composite organization experiences benefits of $6.1 million over three years versus costs of $1.8 million, adding up to a net present value (NPV) of $4.3 million and an ROI of 240%.

ROI	BENEFITS PV	NPV	PAYBACK
240%	**$6.1M**	**$4.3M**	**<6 months**

Benefits (Three-Year)



TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in Google SecOps.

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 Google SecOps can have on an organization.

DISCLOSURES

Readers should be aware of the following:

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

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

Google 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.

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

1. **Due Diligence**
   Interviewed Google stakeholders and Forrester analysts to gather data relative to Google SecOps.
2. **Interviews**
   Interviewed five representatives at organizations using Google SecOps to obtain data about costs, benefits, and risks.
3. **Composite Organization**
   Designed a composite organization based on characteristics of the interviewees' organizations.
4. **Financial Model Framework**
   Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewees.
5. **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 Google SecOps Customer Journey

Drivers leading to the SecOps investment

Interviews			
Role	**Industry**	**Region**	**Employees**
Global head of detection response	Financial services	$200 billion	150,000
Deputy CISO	Financial services	$200 billion	150,000
Director of cyber defense	Healthcare	$18 billion	75,000
CISO	Insurance	$5 billion	3,500
Security operations lead	Professional services	$400 million	1,500

KEY CHALLENGES

Before adopting Google SecOps, the interviewees' organization used legacy solutions, including on-prem SIEMs, and faced the following challenges:

- **Technical and operational complexity.** Interviewees described legacy environments as fragmented and difficult to manage, often involving multiple systems and high-maintenance configurations. The security operations lead in professional services said: "[Our legacy solution had] very intricate servers set up in a very complicated way. It was difficult to manage and required someone with significant engineering background. Google SecOps is a complete shift [from that complexity]."
- **Lack of scalability.** Interviewees emphasized that they needed a cloud-native solution capable of scaling in response to a rapidly evolving and intensifying threat landscape. The global head of detection response in financial services explained: "The biggest pain point [with our legacy environment] was we couldn't scale. We had 30% more attacks every single year. We needed a tool that could actually scale with the increase in attacks."

“We actually heard about Google SecOps through our clients, who were all waxing lyrical about what a great platform it is and how it changed their lives. Now that we have it for ourselves, we get it.”

CISO, INSURANCE

- **Manual processes.** Interviewees’ organizations struggled with overly manual workflows that hindered key performance metrics such as mean time to detect, investigate, and respond. They sought greater automation, analyst-focused genAI, and robust platform features to streamline security operations. The director of cyber defense in healthcare shared: “We knew cloud SIEM would definitely be better for our organization. Our on-prem SIEM was high effort for relatively limited returns.”
- **Limited threat visibility.** Legacy systems at the interviewees’ organizations often lacked fast, effective search capabilities and fully integrated threat intelligence. In discussing the value of threat intelligence, the director of cyber defense in healthcare noted, “Mandiant [as part of the Google SecOps implementation] greatly sweetened the deal.”
- **Financially unsustainable cost models.** Interviewees noted that their prior solutions’ ingestion models were expensive and difficult to sustain long term. The CISO in insurance explained: “[Our legacy solution] was not very financially sustainable. There were a lot of financial limitations that Google SecOps, as a hyperscaled model, doesn’t have.”

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of the interviewees' organizations, 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 enterprise with $8 billion in annual revenue, 20,000 total employees, and 100 security team employees. The SecOps team has 25 employees, and the average fully burdened annual salary for a SecOps analyst is $150,000.

Deployment characteristics. Prior to Google SecOps, the composite organization used a legacy on-prem SIEM and SOAR along with complementary solutions such as a UEBA platform and custom data lake. Google SecOps replaces this legacy environment and is implemented over a six-month period. All 25 employees on the SecOps team use Google SecOps.

KEY ASSUMPTIONS

$8 billion in annual revenue
20,000 employees
25 SecOps team employees

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits						
Ref.	**Benefit**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Atr	Reduced risk and cost of a breach	$1,027,603	$1,113,237	$1,198,870	$3,339,710	$2,754,944
Btr	Optimized security with faster investigation and response	$606,900	$606,900	$606,900	$1,820,700	$1,509,270
Ctr	Empowered junior SecOps analysts	$255,946	$255,946	$255,946	$767,837	$636,499
Dtr	Increased cost model predictability with Google and decommissioned legacy solutions	$488,750	$488,750	$488,750	$1,466,250	$1,215,449
	Total benefits (risk-adjusted)	$2,379,199	$2,464,832	$2,550,466	$7,394,497	$6,116,162

REDUCED RISK AND COST OF A BREACH

Evidence and data. All interviewees said that Google SecOps made their organizations more secure and reduced the likelihood of breach. Interviewees cited several improvements across key operational metrics, such as a three times increase in event ingestion, five times more log sources onboarded, eight times more detection rules implemented, and the ability to manage 10 times the number of cases. These gains, along with various Google SecOps capabilities that enabled their SecOps teams to operate more proactively and effectively, ultimately translated into faster and more accurate threat detection, investigation, and response.

- The CISO in insurance reported that Google SecOps increased event ingestion and, in turn, enhanced observability at their organization: “[With Google SecOps], there’s three-and-a-half times the number of events being ingested into the platform, which is enormous. That led to a 35 percentage point increase in observability. And it’s breadth as well as depth. The depth of the data [with Google SecOps] is far greater.”
- The same interviewee said their legacy solution’s architecture sometimes resulted in event data taking up to 72 hours to filter, but with Google SecOps, it was almost instant.

The interviewee added: “With Google SecOps, event data is near real time — every time, everywhere — which gives us the confidence that we are seeing everything as it’s happening. So, another real big win with Google SecOps.”

- The security operations lead noted their professional services organization was able to onboard five times the number of log sources with Google SecOps. The interviewee explained: “Google has a quick and easy approach to onboarding log sources into the platform. Managing the Google forwarder is a piece of cake. We reduce our cyber risk by ensuring that all tier-one critical applications are onboarded much quicker.”
- The same interviewee said their organization was able to deploy eight times more detection rules with Google SecOps, achieving greater coverage across its entire environment (e.g., on-prem, cloud, and multicloud). The security operations lead emphasized that this improved security: “The quicker we get logs in, the quicker we can create detection rules and alerts. The quicker [this is done], the lower our cyber risk. This greater visibility of our entire infrastructure reduces our cyber risk.”
- The global head of detection response said Google SecOps allowed their financial services organization to manage 10 times the number of cases. The interviewee said this enabled the SecOps team to stop even very sophisticated attacks.

> “With Google SecOps, we’re able to manage 10x the number of cases with half the number of people.”
>
> **GLOBAL HEAD OF DETECTION RESPONSE, FINANCIAL SERVICES**

- Interviewees explained that the efficiency gains with Google SecOps allowed their teams to engage in higher-value work like alert development, threat intelligence, and proactive threat hunting. The security operations lead added: “[Since adopting Google SecOps], we do threat hunting and proactively look at the threats we see in our environment and block any indicators of malware. We never had the time to do some of these things previously. It’s a game changer.”

- Interviewees said that these factors ultimately meant they could detect more, faster. The global head of detection response said: “Mean time to detect has gone down with Google SecOps. It’s faster running the rules. The time between log, ingest, and alert is shorter because Google has basically infinite capacity compute. They can run the queries every minute while traditional tooling did it every 15 minutes.”
- Interviewees explained that faster detection improved security by preventing the spread of malware. At the financial services organization, malware attacks impacted more than 1% of employees each year in their legacy environment, but this lowered to 0.07% upon the adoption of Google SecOps.
- The global head of detection response at the financial services organization accounted for this dramatic decrease in the number of employees malware impacted: “The scalability and speed of Google allows us to detect one [malware incident] and immunize the rest of our 300,000 endpoints just via Google SecOps. It basically takes minutes if not seconds. For that, we largely use the [Google SecOps] SOAR capability and the automation that’s built in. It’s been a huge game changer.”

Reduced risk of exposure to breach costs

70%

- Interviewees noted that Google SecOps is one of the few platforms that has threat intelligence fully integrated into its platform. They said Google Threat Intelligence is up to date, industry-specific, and includes frontline intelligence from Mandiant incident response engagements. Interviewees regarded the Mandiant threat intelligence layer as highly valuable.
- Some interviewees also used Mandiant Threat Defense, which enabled Mandiant experts to directly help their team. The director of cyber defense in healthcare said: “Mandiant Threat Defense will look at the entire corpus of our data, do threat hunting, and be another set of eyes. It’s a compelling differentiator ... [and a] force multiplier.”
- As a comprehensive platform, interviewees identified a multitude of additional factors that contributed to Google SecOps improving their security postures, such as its Unified

Data Model, fast query and search, genAI assistance, 12 months of hot data, and playbooks with automation.

> "The threat intel integration is a big deal and having Mandiant as part of the integrated Google SecOps package is a huge differentiator."
>
> DIRECTOR OF CYBER DEFENSE, HEALTHCARE

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

- The cumulative cost of breaches is $4,233,000 per year.[3]
- Prior to Google SecOps, there is a 68% likelihood of experiencing one or more breaches.[4]
- The percentage of the organization addressable with Google SecOps is 60% in Year 1, 65% in Year 2, and 70% in Year 3.
- Due to Google SecOps, there is a 70% reduced risk of exposure to breach costs.

> "Google SecOps allows us to detect and respond. It's a highly responsive platform with super-fast ingestion rates and analytics capability."
>
> CISO, INSURANCE

Risks. The benefit of reduced risk and cost of a breach will vary based on:

- The frequency and cost of breaches.
- The scale of the Google SecOps deployment and the percentage of the organization addressable with Google SecOps.
- The extent to which the organization leverages Google SecOps' capabilities and matured its security operations.
- The tools and solutions used prior to Google SecOps.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $2.8 million.

> "Google SecOps sits right at the cornerstone of our detection capability and defense-in-depth model. The good monitoring, good defensive capability, [and] good detection are ultimately what will be the difference between success and failure in breach scenarios."
>
> CISO, INSURANCE

Reduced Risk And Cost Of A Breach					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Cumulative cost of breaches	Forrester research	$4,233,000	$4,233,000	$4,233,000
A2	Likelihood of experiencing one or more breaches	Forrester research	68%	68%	68%
A3	Percentage of organization currently addressable with Google SecOps	Composite	60%	65%	70%
A4	Annual risk exposure addressable with Google SecOps	A1*A2*A3	$1,727,064	$1,870,986	$2,014,908
A5	Reduced risk of exposure to breach costs from addressable attacks with Google SecOps	Interviews	70%	70%	70%
At	Reduced risk and cost of a breach	A4*A5	$1,208,945	$1,309,690	$1,410,436
	Risk adjustment	↓15%			
Atr	Reduced risk and cost of a breach (risk-adjusted)		$1,027,603	$1,113,237	$1,198,870
	Three-year total: $3,339,710		**Three-year present value: $2,754,944**		

OPTIMIZED SECURITY WITH FASTER INVESTIGATION AND RESPONSE

Evidence and data. Google SecOps resulted in more efficient investigation and response at interviewees' organizations, which reduced risk and saved analyst time. With Google SecOps, on average, interviewees reported a 50% reduction in mean time to investigate and a 65% reduction in mean time to respond. Interviewees identified several Google SecOps features contributing to these improvements, including the Unified Data Model, faster query and search capabilities, genAI assistance, access to 12 months of hot data, integrated threat intelligence, automation with playbooks, and a reduction in false positives.

- Interviewees spoke highly of Google SecOps' Unified Data Model (UDM), noting that it streamlined the process of finding information and correlating patterns when investigating and responding to security threats. The security operations lead in professional services observed: "The UDM means correlation searches are probably the best they are in the industry. They are much, much easier and more powerful. It's a game changer."
- With Google SecOps, interviewees' organizations saw dramatic improvements in query speeds. The CISO in insurance explained: "[With Google SecOps], you're getting the

power of Google's infrastructure and big data capabilities. We have immensely improved response times for complex queries. It's guaranteed near real time. It's happening in seconds."

- The security operations lead in professional services said the genAI within Google SecOps was key to improving analyst efficiency: "Gemini in SecOps is very good at helping create search criteria. An analyst can ask in plain English, and Gemini will create the actual UDM search, which is the actual query, and they can run it and get their answer immediately. That's very, very useful."
- The global head of detection response in financial services said that automation streamlined investigations: "Mean time to investigate is absolutely faster with Google SecOps because of the automation. We halved our investigation time. And it's going to go down further once agentic AI is live."
- Automation in Google SecOps also improved response, as the CISO in insurance explained: "A maximum amount of observability and large degrees of automation help us respond and ultimately mitigate impact. Google SecOps allow us to ensure we're able to see what's going on quickly and then respond. Google SecOps is a response enabler."

> "Our employees really love that Google SecOps has a context-rich dataset along with Gemini, which can give a really slick summary really quickly. It's a huge accelerator when investigating. You get everything that you need, and it can write complex queries for you. They absolutely love it."
>
> **CISO, INSURANCE**

- The same interviewee noted the platform's user-friendly interface: "With Google [SecOps], everything is displayed there for our analysts. It's a really rich, really powerful investigative experience."
- Access to 12 months of hot data in Google SecOps made it an effective tool, as the director of cyber defense in healthcare stated: "Twelve months of hot data all in one

system [with Google SecOps] is definitely compelling. In our previous SIEM, cold data was so agonizingly slow to use it that it almost never got used."

- The integrated threat intelligence and SOAR capabilities provided analysts at interviewees' organizations with additional context, reducing the need for manual data gathering and providing a clearer understanding of who was attacking.
- Interviewees said playbooks in Google SecOps increased analyst speed while providing guardrails to prevent faulty decisions. Playbooks allowed their organizations to automate security tasks with a straightforward approach using prebuilt actions and decision logic, leading to end-to-end workflows that did not require deep coding skills.
- Interviewees reported that Google SecOps reduced false positives and increased their confidence that alerts were valid. The global head of detection response elaborated: "The false-positive rate for the analysts [investigating] went dramatically down because we can much more quickly tune stuff, especially with the playbooks and SOAR capabilities. If the analyst says they are false positives, that automatically triggers an automation, and the specific false positive will never come up again."

> "We're much quicker to react with all the automation [with Google SecOps]. We're much quicker at following up on alerts. And we're more confident the alerts are actually real alerts. Our business is more secure because we're way faster in responding."
>
> **DEPUTY CISO, FINANCIAL SERVICES**

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

- There are 20 SecOps analysts who work on investigation and response. These analysts represent 80% of the total SecOps team.
- On average, they spend 40% of their time on investigation and 15% of their time on response.

- Due to Google SecOps, there is a 50% reduction in the mean time to investigate.
- Due to Google SecOps, there is a 65% reduction in the mean time to respond.
- The average fully burdened annual salary for a SecOps analyst working on investigation and response is $150,000.
- The productivity recapture rate for employees is 80%. This means employees convert 80% of their saved time into productive time.

> "The investigative power of Google SecOps is a massive game changer, and our team absolutely loves it."
>
> CISO, INSURANCE

Risks. The benefit of optimized security with faster investigation and response will vary based on:

- The volume of security threats.
- The size of the SecOps team and how much time they spend on investigation and response.
- The prior state and maturity level for investigation and response.
- The average annual fully burdened salary of a SecOps analyst working on investigation and response.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.5 million.

Reduction in mean time to investigate

50%

Reduction in mean time to respond

65%

Optimized Security With Faster Investigation And Response					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	SecOps analysts who work on investigation and response	Composite	20	20	20
B2	Average percentage of their time spent on investigation	Composite	40%	40%	40%
B3	Reduction in mean time to investigate with Google SecOps	Interviews	50%	50%	50%
B4	FTEs no longer working on investigation due to Google SecOps	B1*B2*B3	4	4	4
B5	Average percentage of their time spent on response	Composite	15%	15%	15%
B6	Reduction in mean time to respond with Google SecOps	Interviews	65%	65%	65%
B7	FTEs no longer working on response due to Google SecOps	B1*B5*B6	1.95	1.95	1.95
B8	Fully burdened annual salary for a SecOps analyst	Composite	$150,000	$150,000	$150,000
B9	Productivity recapture	TEI standard	80%	80%	80%
Bt	Optimized security with faster investigation and response	(B4+B7)*B8*B9	$714,000	$714,000	$714,000
	Risk adjustment	↓15%			
Btr	Optimized security with faster investigation and response (risk-adjusted)		$606,900	$606,900	$606,900
	Three-year total: $1,820,700			**Three-year present value: $1,509,270**	

EMPOWERED JUNIOR SECOPS ANALYSTS

Evidence and data. Interviewees highlighted how Google SecOps' ease of use and genAI capabilities specifically empowered junior SecOps analysts to take on more advanced responsibilities and quickly understand the platform's features. For example, interviewees' organizations were able to shift approximately 35% of the work traditionally performed by more senior colleagues to junior analysts. Moreover, the average time to productivity for newly onboarded junior hires was reduced by about 70%, accelerating their ability to contribute to security operations. Interviewees explained that these improvements helped their organizations alleviate the challenge posed by an ongoing shortage of experienced SecOps talent.

- Interviewees explained that Google SecOps' ease of use allowed junior analysts to do work that traditionally required more senior staff. The security operations lead in professional services said: "[With Google SecOps], a junior analyst can do a very large amount of the work that a senior analyst would have done. There aren't the headaches and maintenance baggage that we had with [our legacy solution]. My senior analysts don't need to be staring at SecOps all day."
- The genAI embedded in Google SecOps helped junior analysts be more effective and efficient, according to interviewees. For example, Gemini in SecOps allowed their analysts to write queries in natural language. The director of cyber defense in healthcare said: "Gemini has helped less-skilled, less-trained junior analysts. It gets them started and makes the system more approachable."
- Interviewees also explained that Gemini in SecOps summarized alerts and provided recommendations on how to proceed. The director of cyber defense said: "An early career analyst can get an AI-based summarization with Gemini. It's an accelerator for them to do investigations."
- The CISO in insurance added, "The investigative power of Google SecOps really does support the human being and their innate curiosity, whereas other products just don't."

> "[Google SecOps] empowers [our team] to investigate quickly and deeply so that no stone is unturned. Gemini obviously plays a large part in that."
>
> **CISO, INSURANCE**

- The global head of detection response in financial services said that it was easy for new hires to get up to speed on Google SecOps and become fully productive. They added: "Onboarding time is much faster with Google SecOps — probably four or five times faster. Junior analysts don't have to know every step because the playbooks guide them along what to do next."
- Several interviewees predicted that their onboarding would reduce further as they continued to integrate Gemini into that process.
- Given the struggle to find highly qualified SecOps analysts, upleveling early career analysts to take on work traditionally performed by more seasoned analysts helped ease the skills shortage at some interviewees' organizations.

> "Google SecOps is designed with security operations in mind. The whole platform is very streamlined and intuitive. I have trained junior analysts on Google SecOps, and they are very quickly able to use it."
>
> SECURITY OPERATIONS LEAD, PROFESSIONAL SERVICES

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

- There are 12 senior and mid-level SecOps analysts. The average fully burdened annual salary for senior and mid-level SecOps analysts is $170,460.
- With Google SecOps, 35% of their work can be shifted to more junior analysts.
- The expected compensation savings for work performed by more junior analysts is 30%.
- There are four junior new hires each year. Prior to Google SecOps, time to productivity was two and a half months.
- With Google SecOps, time to productivity for junior new hires reduces by 70%.
- The average fully burdened monthly salary for a junior SecOps analyst is $9,943.50.

Risks. The benefit of empowered junior SecOps analysts will vary based on:

- The number of junior SecOps analysts and their skill set.
- The tools and processes they use prior to Google SecOps.
- The number of newly hired junior SecOps analysts onboarded each year.
- The average fully burdened salary of junior SecOps analysts and the extent to which this differs with the average fully burdened salary of more senior colleagues.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $636,000.

Percentage of work shifted to more junior analysts
35%

Reduction in time productivity for junior new hires
70%

Empowered Junior SecOps Analysts					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Senior and mid-level SecOps analysts	Composite	12	12	12
C2	Percentage of their work that can be shifted to more junior analysts with Google SecOps	Interviews	35%	35%	35%
C3	Expected compensation savings for work performed by more junior analysts	Composite	30%	30%	30%
C4	Fully burdened annual salary for a senior and mid-level SecOps analyst	Composite	$170,460	$170,460	$170,460
C5	**Subtotal: Cost savings of shifting work to more junior analysts with Google SecOps**	**C1*C2*C3*C4**	**$214,780**	**$214,780**	**$214,780**
C6	Onboarded junior SecOps analysts (e.g., new hires)	Composite	4	4	4
C7	Time to productivity before Google SecOps (months)	Composite	2.5	2.5	2.5
C8	Reduction in time to productivity with Google SecOps	Interviews	70%	70%	70%
C9	Fully burdened monthly salary for a junior SecOps analyst	Composite	$9,943.50	$9,943.50	$9,943.50
C10	**Subtotal: Cost savings from reduced time to productivity for new junior analyst hires**	**C6*C7*C8*C9**	**$69,604**	**$69,604**	**$69,604**
Ct	Empowered junior SecOps analysts	C5+C10	$284,384	$284,384	$284,384
	Risk adjustment	↓10%			
Ctr	Empowered junior SecOps analysts (risk-adjusted)		$255,946	$255,946	$255,946
	Three-year total: $767,837		**Three-year present value: $636,499**		

INCREASED COST MODEL PREDICTABILITY WITH GOOGLE AND DECOMMISSIONED LEGACY SOLUTIONS

Evidence and data. With the adoption of Google SecOps, interviewees' organizations were able to decommission tools like legacy SIEMs, SOARs, UEBA platforms, and custom data lakes. Interviewees described Google SecOps as affordable and cited its predictable cost model and high scalability as key advantages over their previous solutions. The consolidation to Google SecOps also helped simplify vendor and solution management.

- All interviewees said that Google SecOps delivered far greater benefits despite costing around the same or less than their legacy solutions.

- The CISO in insurance discussed Google SecOps' affordability and effectiveness: "The cost of Google SecOps is more sustainable and more predictable. … We are very early in our development curve with Google SecOps, and it has already far exceeded anything we had with [our legacy solution] the previous four years."
- The director of cyber defense in healthcare also appreciated the predictability of Google pricing: "The predictable cost model [of Google SecOps] is of great value to us. Some competitor solutions say, 'Only pay for what you use.' That inspires dread because one massive incident can run through a ton of budget. With Google, there's really no ongoing transactional costs outside of the licensing."
- Interviewees' organizations also saw value in moving from multiple, disparate tools (e.g., separate SIEM, SOAR, UEBA, and custom data lake) to a single platform with Google SecOps. This consolidation helped simplify vendor and solution management.
- Google SecOps supports data from on-prem, Google Cloud, and other cloud environments, enabling interviewees' organizations to ingest and analyze data from diverse environments.

> "Google SecOps provides a highly scalable platform that meets today's needs but can also scale to meet tomorrow's needs — and without creating an undue financial burden on the business."
>
> **CISO, INSURANCE**

Modeling and assumptions. Based on the interviews, Forrester assumes the composite organization saves $575,000 per year by decommissioning legacy solutions after the implementation of Google SecOps.

Risks. The benefit of increased cost model predictability with Google and decommissioned legacy solutions will vary based on:

- The number and cost of legacy solutions used by the organization.
- Adoption level of Google SecOps across the organization.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.2 million.

> "Google SecOps is the core of our fusion center. It's the driving platform behind how we do security operations within our business."
>
> CISO, INSURANCE

Increased Cost Model Predictability With Google And Decommissioned Legacy Solutions

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Cost of legacy security solutions decommissioned upon adoption of Google SecOps	Interviews	$575,000	$575,000	$575,000
Dt	Increased cost model predictability with Google and decommissioned legacy solutions	D1	$575,000	$575,000	$575,000
	Risk adjustment	↓15%			
Dtr	Increased cost model predictability with Google and decommissioned legacy solutions (risk-adjusted)		$488,750	$488,750	$488,750
	Three-year total: $1,466,250		**Three-year present value: $1,215,449**		

UNQUANTIFIED BENEFITS

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

- **Enhanced employee experience.** Interviewees said Google SecOps was a central component of their organizations' efforts toward a modern stack with leading-edge technology. The deputy CISO in financial services added: "Our people are definitely excited about [Google SecOps]. And automating the boring workloads allows them to do more of the interesting threat hunting work."
- **Google partnership.** Interviewees praised Google as an innovative partner who helped ensure a smooth implementation and ongoing success. The CISO in insurance said:

"Google didn't just drop a license deal on us. They help us through the journey and help us understand their technology and platform. The adoption and migration were super easy — far easier than we anticipated. We couldn't be happier with the process and outcomes."

The global head of detection response in financial services observed: "With Google, it's more like a partnership than a vendor-customer relationship. This is extremely valuable in terms of providing feedback and getting features implemented and set up the way we want." The CISO added, "Working with Google, we are able to drink from the fire hose in terms of cyber innovation."

- **Scalability.** Interviewees repeatedly emphasized the scalability of Google SecOps and their confidence in the platform's ability to meet their future needs. The CISO in insurance said: "We knew that it could scale and grow with our business. It has everything we need now, but also a whole load of benefits we can unlock for our roadmap moving forward.

> "We all noticed how easy Google is to do business with — how helpful and transparent they are. Investing in Google SecOps was a strategic decision for the tech capability but also for having the right partner in place."
>
> **CISO, INSURANCE**

FLEXIBILITY

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

- **Continued platform development and AI leadership.** Interviewees felt confident that Google would continually develop the SecOps platform and remain a dominant genAI player into the future. The global head of detection response in financial services said,

“Google has developed a very, very strong AI toolset. And from what I’ve seen, there’s an aggressive roadmap and I’m very comfortable that AI will only become more and more powerful on the Google SecOps platform.”

SECURITY OPERATIONS LEAD, PROFESSIONAL SERVICES

> “I’m super excited about the next evolution of Google SecOps, especially the agentic AI features just announced.

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	Google SecOps licensing fees	$0	$575,000	$575,000	$575,000	$1,725,000	$1,429,940
Ftr	Internal labor for implementation and ongoing maintenance	$156,170	$86,250	$86,250	$86,250	$414,920	$370,661
	Total costs (risk-adjusted)	$156,170	$661,250	$661,250	$661,250	$2,139,920	$1,800,601

GOOGLE SECOPS LICENSING FEES

Evidence and data. Interviewees' organizations paid annual licensing fees to Google for the use of Google SecOps. These costs varied across organizations and were largely driven by the volume of data and scope of implementation.

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

- The composite pays $500,000 annually for its Google SecOps licensing.
- Pricing may vary. Contact Google for additional details.

Risks. The licensing fees will vary based on:

- Customer-specific pricing.
- The pricing package the customer chooses.
- The volume of data.
- The scope of the implementation.

Results. To account for these risks, Forrester adjusted this cost upward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.4 million.

Google SecOps Licensing Fees						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Cost of Google SecOps licensing	Interviews		$500,000	$500,000	$500,000
Et	Google SecOps licensing fees	E1		$500,000	$500,000	$500,000
	Risk adjustment	↑15%				
Etr	Google SecOps licensing fees (risk-adjusted)		$0	$575,000	$575,000	$575,000
	Three-year total: $1,725,000			**Three-year present value: $1,429,940**		

INTERNAL LABOR FOR IMPLEMENTATION AND ONGOING MAINTENANCE

Evidence and data. At interviewees' organizations, a subset of their SecOps teams dedicated time to implementing and maintaining Google SecOps. Additionally, all members of the team spent time on initial training.

- The time to implement Google SecOps at interviewees' organizations varied but typically took six months or less.
- Interviewees described smooth adoptions with ample support from Google. The security operations lead in professional services said: "Google was very supportive. We were in full conversation on a regular basis. I could reach them anytime I wanted. There was a lot of support."
- Interviewees said that upon adoption of Google SecOps, their analysts typically spent a few days training on the platform.

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

- Five SecOps FTEs dedicate 20% of their time to implementing Google SecOps over the course of six months. After implementation, one SecOps FTE dedicates 50% of their time to ongoing maintenance of the platform.
- The fully burdened monthly salary for an FTE involved in implementation and ongoing maintenance is $12,500.

- There are 25 employees on the SecOps team. They spend an average of 32 hours training on Google SecOps. The fully burdened hourly rate for a SecOps FTE is $76.

Risks. The cost of internal labor for implementation and ongoing maintenance will vary based on:

- The scope of the implementation, including the number of employees on the SecOps team.
- The number of Google SecOps users.
- The skill set of the SecOps team.
- The fully burdened salary of employees.

Results. To account for these risks, Forrester adjusted this cost upward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $371,000.

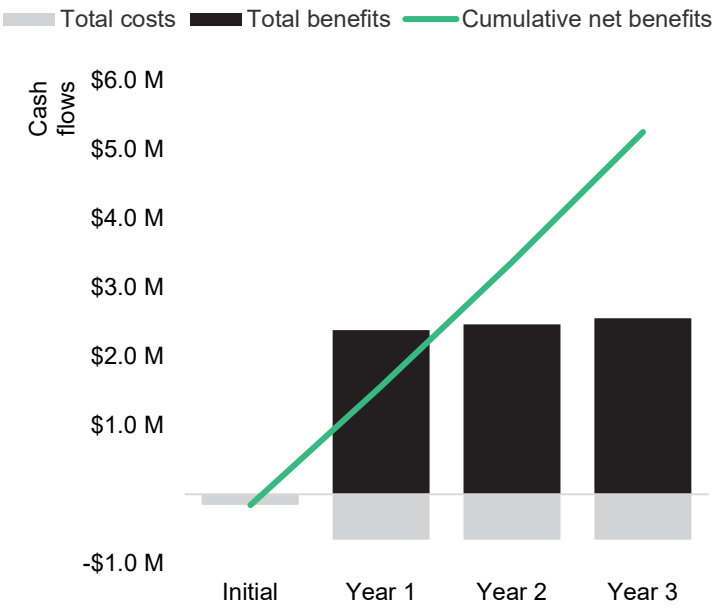
Internal Labor For Implementation And Ongoing Maintenance

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	FTEs involved in implementation and ongoing maintenance	Interviews	5	1	1	1
F2	Length of implementation (months)	Interviews	6			
F3	Percentage of FTE time dedicated to Google SecOps implementation or maintenance	Interviews	20%	50%	50%	50%
F4	Fully burdened monthly salary for an FTE involved in implementation	Composite	$12,500	$12,500	$12,500	$12,500
F5	SecOps team members trained	Composite	25			
F6	Hours spent on training	Interviews	32			
F7	Fully burdened hourly rate for a SecOps FTE	Composite	$76			
Ft	Internal labor for implementation and ongoing maintenance	Initial: (F1*F2*F3*F4) +(F5*F6*F7) Y1 to Y3: F1*F3*F4*12	$135,800	$75,000	$75,000	$75,000
	Risk adjustment	↑15%				
Ftr	Internal labor for implementation and ongoing maintenance (risk-adjusted)		$156,170	$86,250	$86,250	$86,250
	Three-year total: $414,920			**Three-year present value: $370,661**		

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)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($156,170)	($661,250)	($661,250)	($661,250)	($2,139,920)	($1,800,601)
Total benefits	$0	$2,379,199	$2,464,832	$2,550,466	$7,394,497	$6,116,162
Net benefits	($156,170)	$1,717,949	$1,803,582	$1,889,216	$5,254,577	$4,315,561
ROI						240%
Payback						<6 months

APPENDIX A: TOTAL ECONOMIC IMPACT

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

Total Economic Impact Approach

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

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

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

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

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.

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: SUPPLEMENTAL MATERIAL

Related Forrester Research

The Top Cybersecurity Threats In 2025, Forrester Research, Inc., April 14, 2025.

Lessons Learned From The World's Biggest Data Breaches And Privacy Abuses, 2024, Forrester Research, Inc., March 25, 2025.

APPENDIX C: ENDNOTES

[1] Source: The Top Cybersecurity Threats In 2025, Forrester Research, Inc., April 14, 2025; Lessons Learned From The World's Biggest Data Breaches And Privacy Abuses, 2024, Forrester Research, Inc., March 25, 2025.

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

[3] Regression analysis of the reported total cumulative costs of all breaches experienced by security decision-makers' organizations in the past 12 months. The composite organization's revenue is used as the input to the regression formula. Source: Forrester's Security Survey, 2024, "Using your best estimate, what was the total cumulative cost of all breaches experienced by your organization in the past 12 months?" Base: 1,660 global security decision-makers who have experienced a breach in the past 12 months

[4] Regression analysis of the likelihood of experiencing one or more breaches, using the frequency that organizations experienced breaches in the past 12 months as reported by security decision-makers. The composite organization's revenue is used as the input to the regression formula. Source: Forrester's Security Survey, 2024, "How many times do you estimate that your organization's sensitive data was potentially compromised or breached in the past 12 months?" Base: 2,769 global security decision-makers


BRILYANT


FORRESTER®