October 2026
Business Value White Paper
Sponsored by Google

The Business Value of Google Security Operations with Gemini



Michelle Abraham
Senior Research Director,
Security and Trust, IDC



Ladislav Kinda
Consultant,
Business Value Strategy Practice, IDC



Table of Contents

Click any title to navigate directly to that page.

Business Value Highlights 3

Executive Summary 4

Situation Overview 6

Google Security Operations with Gemini Overview 7

The Business Value of Google Security Operations with Gemini 8

- Study Firmographics 9
- The Environment That Google Security Operations with Gemini Protects 10
- Choice and Use of Google Security Operations 11
  - The Prior Security Environment 12
- Gemini in Routine Daily Use 13

Average Annual Benefits per Organization 14

How Google Security Operations with Gemini Creates Value 16

Security Team Efficiencies 17

- How the Investigation Process Changed 19
- Faster Security Reporting and Summarization 20

From Telemetry to Realized Loss Mitigation 21

- Mean Time to Detect and Remediate 22
- Detection Coverage and Incident Volume 23

Revenue Recovered Through Fewer Business Interruptions 24

Cost and Risk Avoidance 25

- Risk and Business Resilience 26

Business Impact and Agility 27

ROI Analysis 28

Challenges/Opportunities 29

Conclusion 31

Appendix: Methodology 32

About the IDC Analysts 34

Message from the Sponsor 35

Business Value Highlights

Click each to jump to related content. Use "Return to Highlights" in the page header to get back here.

319% three-year return on investment

7-month payback on investment

88% of analysts using Gemini regularly

98% reduction in mean time to identify threats

88% reduction in mean time to remediate threats

84% reduction in time spent creating security reports

50% fewer impactful security incidents per month

$5.4 million average annual benefits per organization

Executive Summary

This IDC Business Value white paper describes the experiences of organizations that have adopted Google Security Operations with Gemini. By consolidating fragmented security tooling onto a single platform and applying native Gemini AI directly to their unified data, these organizations detect and investigate threats dramatically faster, resolve incidents with substantially less manual effort, and allow a lean security team to cover far more of their environment. Analysts spend their time on deeper analysis of true positive alerts and improving automations rather than sifting through logs across multiple tools.

IDC conducted seven in-depth interviews with organizations running Google Security Operations (SecOps) with Gemini in production. The organizations span midmarket to global enterprises, three countries, and seven unrelated industries, and their security teams differ by an order of magnitude in size. Across that range, the interviewed organizations described the same shape of benefit. The value described in this document is not tied to one industry or one size of security team.

The results these organizations reported are not seven separate wins, but one mechanism observed seven times. Consolidating the security stack onto a single platform, enriching detections automatically with Google Threat Intelligence, and placing a native Gemini first pass in front of every human decision produce all of them. Interviewed organizations reported that consolidation retires overlapping tools, enriched data lets every investigation start with an AI first pass rather than a raw alert, and faster investigation means fewer incidents progress to the point of interrupting the business. One architectural decision produced four measurable consequences: staff efficiency, revenue recovery, cost avoidance, and risk reduction.

Gemini is in routine daily use rather than pilot use. Across the organizations IDC interviewed, Gemini assists in 55.5% of investigations and workflows, and 88.2% of security analysts use it regularly. Interviewed organizations attributed that level of adoption to native integration, as Gemini sits inside Google SecOps itself, so analysts do not actually choose to use an AI tool; they encounter it as part of how the work already happens.

A telecommunications organization described the practical effect on the skills required to interrogate security data:

Telecommunications:

"I consider myself very technical, but I can't write a fresh query on the spot. In SecOps, I can just say, 'Gemini, write me a prompt to find this,' and it produces a query in about three seconds. I don't need to learn a query language."

Those changes are visible across every measure this study captured. Interviewed organizations identify and remediate threats in a fraction of the time they previously required, detect a substantially greater share of the threats present in their environments, produce security reporting with a small portion of the effort it once demanded, and deliver materially greater output with the teams they already have. IDC's analysis translates those operational gains into substantial annual benefits per organization, a strong three-year return on investment, and a rapid payback period.

IDC identified key areas of value where Google SecOps with Gemini consistently delivered measurable impact by:

- **Enriching detections automatically with integrated threat intelligence** so that alerts arrive carrying the context analysts previously had to assemble by hand before any judgment could be applied
- **Shifting the role of analyst from investigator of first resort to reviewer and decision-maker** by placing a native AI first pass in front of every human decision, allowing analysts to start from an assessed and summarized case rather than a raw alert
- **Compressing detection and remediation timelines,** narrowing the window in which a threat can progress unnoticed and reducing the proportion of incidents that reach the point of business impact
- **Widening detection coverage across the monitored estate,** surfacing malicious activity in telemetry that was collected but previously went unexamined
- **Consolidating fragmented security operations tooling,** removing the condition in which analysts served as the integration layer between separate security information and event management (SIEM); security orchestration, automation, and response (SOAR); endpoints; networks; and cloud consoles
- **Releasing security capacity,** enabling the same team to absorb a growing estate and moving human attention up the escalation chain toward more consequential analysis
- **Removing reporting overhead from the analyst workload,** converting hours previously spent assembling case and incident summaries into analytical time and making continuous rather than periodic reporting practical
- **Protecting revenue and lowering expected breach loss,** as earlier containment keeps the business systems customers depend on available and reduces exposure to a serious breach

- **Delivering a strong return on investment and rapid payback,** with benefits that arrive together rather than in sequence because each of them derives from the integration of Gemini across the SecOps platform

Situation Overview

SIEM has moved well past its original function as a log aggregation and compliance tool. Real-time detection, alert correlation, behavioral analytics, and case management now sit inside the platform alongside increasingly automated response. Capabilities once sold as standalone products, user and entity behavior analytics (UEBA) and SOAR chief among them, have become baseline expectations rather than add-ons. That consolidation changed how much time analysts spend inside the tool: Organizations evaluating the SIEM market today are choosing a platform their teams will live in daily, not query occasionally.

The correlation and enrichment work is similar to what was once done with separate solutions, drawing on available threat intelligence to build incidents out of individual alerts, but the volume of alerts arriving each day has outpaced the head count available to triage them because of expanding attack surfaces. Assembling context consumes investigation time, which means pivoting between information and looking up indicators before any judgment is applied. Reporting is a manual exercise that competes directly with analysis for the same scarce hours.

Because security teams have not grown in proportion to the volume of alerts, the arrival of AI inside the security workflow has been a boon to security teams. Large language models can summarize a case, translate a plain-language question into a query, explain a detection rule, and propose a next action, all tasks that previously required either expertise or time, and often both. More recently, AI agents are handling alert triage and investigation in some organizations as well as threat hunting, detection rule development, parser generation, playbook construction, and reverse engineering malware. The agent makes the initial determination of what is benign and what warrants escalation, a judgment that previously required an analyst's direct attention on every alert.

The practical question for security leaders is whether AI changes measurable outcomes, and under what conditions. Two conditions matter in particular. AI agents are only as good as the data they can access and are trained on, which makes data retrieval a precondition rather than a separate initiative. And AI only affects outcomes if analysts actually use it, which depends less on model capability than on whether AI is truly helpful in reducing toil. IDC designed this study to test both propositions against the experience of organizations running such a platform in production.

Google Security Operations with Gemini Overview

Google Security Operations is a cloud-native security operations platform that combines SIEM with SOAR in a single solution. Architecturally, the platform is organized around three workload pillars (Detect, Investigate, and Respond) layered on a unified data lake. Ingestion draws from a large library of connectors covering network devices, endpoints, cloud services, identity management systems, business applications, and third-party security tools, with events normalized into the Unified Data Model so that data from different sources can be searched and correlated consistently. Google SecOps applies detection rules maintained by Google alongside rules written by the customer, running both against the same normalized data set. All data is enriched at ingest with threat intelligence from Google Threat Intelligence. Google Threat Intelligence offers a diverse set of intelligence sources across Mandiant frontline research, open and crowdsourced VirusTotal data, and telemetry from Workspace, Gmail, Chrome, and Android. UEBA and risk-based alerting combine lower-fidelity signals into higher-value detections, addressing the false-positive volume that drives much of the manual tuning burden in a SIEM. Curated detection content, authored by Google and Mandiant analysts and mapped to MITRE ATT&CK, is refreshed on a regular cadence.

On the SOAR side, the platform provides case management, playbook-driven automation, and a substantial catalog of integrations with third-party tools, allowing response actions to be executed from the same environment in which the investigation takes place. Gemini is integrated throughout the analyst workflow rather than offered as a separate assistant. Analysts can query platform data in natural language, with Gemini translating the question into SecOps' query syntax, a capability that may help newer staff reach proficiency faster. Gemini generates case and alert summaries, drafts reports, explains detection rules and assists in authoring them, builds playbooks, and can run an agentic investigation and triage workflow, surfacing the analyst's recommended next step.

The interviewed organizations consistently attributed their level of AI adoption to the fact that Gemini is encountered within the workflow they were already in rather than in a separate tool they would have to choose to open. Agentic capability built on Gemini extends beyond assistance into autonomous task execution. The Alert Triage and Investigation agent collects evidence, runs correlated searches, and produces a verdict, which reduces analyst workload by handling first-pass case analysis. The Detection Engineering agent translates new exploitation patterns into custom detections for a specific environment, analyzing a diverse array of input sources,

including Google Threat Intelligence and internal security telemetry. Google SecOps offers a remote Model Context Protocol server, giving customers a path to build their own agentic workflows on top of the platform.

Google SecOps includes one year of hot data retention, and Google administers the platform itself, a delivery choice several interviewed organizations cited as a selection criterion because security teams could focus on more security work versus managing infrastructure. The AI stack is vertically integrated, which supports the unit economics and gives it tighter control over the iteration cycle that improves agent accuracy on security-specific tasks. Google designs the silicon, runs the infrastructure, develops the Gemini foundation models, and encodes its internal security expertise into the agent evaluation loops.

The Business Value of Google Security Operations with Gemini

IDC conducted in-depth interviews with seven organizations that have deployed Google Security Operations with Gemini in production. The interviews followed a structured framework designed to capture both quantified operational data and qualitative testimony and were conducted with the people who run these security operations day to day rather than with a survey panel.

IDC asked for measured figures wherever they existed: time to identify a potential threat, time to address or remediate it, the share of potential threats being identified, the volume of impactful incidents, security staffing levels and the allocation of analyst time, tool and platform spend, deployment effort, and exposure to a serious breach. Where a hard measurement was not available, which is common in security operations because many teams are not instrumented to record these figures, the interviewee's direct experience was captured as evidence in its own right. The quantified findings in this document carry a respondent count; findings that rest on qualitative testimony are presented as such and are excluded from the financial model.

The quantified results reflect the platform as it is deployed, with Google SecOps and Gemini operating together, and Gemini's specific contribution is identified where interviewed organizations attributed it directly.

One participant summarized the combined effect of consolidated data and integrated intelligence:

Chemical:

"The threat intelligence capability within Google SecOps has been, I guess we could say, game-changing. There are very rich data sources in there, information that would be more difficult to find otherwise. Having it in one place has made life a lot easier, and we've managed to proactively stop some attacks by seeing things early."

Study Firmographics

The interviewed organizations span midmarket to global enterprises across a broad range of industries, so the findings reflect widely differing security-team scale. Employee counts, IT and security staffing, application estates, and revenue all vary by an order of magnitude across the sample **(Table 1, below).**

Table 1

Firmographics of Interviewed Organizations

Firmographics	Average	Median
Number of employees	35,100	10,000
Number of total IT staff	470	300
Number of security staff	110	30
Number of security engineers and specialists	30	7
Total number of business applications	1,050	475
Annual revenue	$25.5B	$4.1B

n = 7; Source: IDC Business Value In-Depth Interviews, August 2026

The spread across the sample is wide. Employee counts run from a median of 10,000 to an average of 35,100; security staffing from a median of 30 to an average of 110; and annual revenue from a median of $4.1 billion to an average of $25.5 billion. In each case, the average sits well above the median, reflecting the presence of several very large participants alongside a majority of midmarket and mid-enterprise organizations.

The interviewed organizations are based in the United States (four), the United Kingdom (two), and Portugal and represent seven unrelated industries: media and technology, fintech, telecommunications, education, chemicals, industrial automation, and retail.

The sample therefore covers organizations that differ considerably in scale, sector, and regulatory environment and that arrived at the same platform from those different starting points. The value described in this document is not a function of one industry, one regulatory environment, or one security team size.

The Environment That Google Security Operations with Gemini Protects

Google SecOps with Gemini protects hybrid and multicloud estates from a single platform because telemetry is ingested centrally rather than monitored tool by tool. The median interviewed organization protects 9,000 endpoints, with the average pulled up to 33,900 by the largest participants, and the same organizations run an average of 9,900 Google Cloud virtual machines alongside on-premises and other cloud infrastructure **(Table 2, below).**

Table 2

The Environment Protected with Google SecOps with Gemini

Environment Measure	Value
Endpoints protected per organization (average)	33,900
Endpoints protected per organization (median)	9,000
Google Cloud VMs per organization (average)	9,900
Months to initial deployment (average)	4.1

n = 7; Source: IDC Business Value In-Depth Interviews, August 2026

Two characteristics of these estates shape the results that follow. First, they are genuinely hybrid: Google Cloud, other clouds, and on-premises infrastructure appear in the same picture and are monitored from one platform rather than from a console per environment. That is the consolidation argument expressed in physical terms.

Second, the interviewed organizations reached initial deployment in an average of 4.1 months. For a platform that replaces several incumbent tools and sits at the center of security operations, that is a short implementation, and it is a substantial part of the reason the payback period lands where it does. No interviewed organization described an implementation approaching a year.

Choice and Use of Google Security Operations

Adoption did not follow from a single motivation. Across the interviewed organizations, four distinct entry points recur: platform consolidation, vendor simplification, operating-model preference, and a combination of price and included capability.

Most participants describe some combination of these entry points, weighted differently according to their circumstances. The accounts below illustrate each of the four.

Consolidation with attached, integrated intelligence was the requirement for one media and technology organization so that data could be contextualized and then acted on in the same place:

Media/Technology:

"We needed a solution that could consolidate various SIEMs and data-aggregation tools into a single platform, where we could contextualize the data and then act on it intelligently. Google SecOps had the scale we needed, built-in threat intelligence, and the SOAR platform for agentic workflows."

An industrial automation manufacturer evaluated the market with a specific consolidation test in mind and treated vendor and technology simplification as the return, with the commercial position roughly unchanged.

Industrial Automation:

"We had six to eight technologies we looked into and confirmed Google SecOps could consolidate them together. From a vendor perspective, it's easier: one vendor. From a technology standpoint, it's easier: one platform. And from a cost perspective, it was approximately neutral for us."

Across the interviewed organizations, consolidation consistently centered on the SIEM and SOAR core rather than the wider security stack. Participants displaced a mix of commercial SIEM platforms, an incumbent SOAR tool, legacy open source and cloud-based log platforms, and, in one case, a bundled productivity AI assistant that natively integrated Gemini replaced. Several gained SOAR as a net-new capability their previous SIEM lacked, and one deployed both SIEM and SOAR for the first time to close an acknowledged gap.

A retailer led with an operating-model requirement, expressed as a decision about what its security staff should not be doing:

Retail:

"The first requirement was: We don't want our security people doing IT. That pushed us toward a software-as-a-service platform, so someone else handles the platform itself, guaranteeing stability and performance. We just want to ingest everything."

A chemical manufacturer weighed price against included capability and counted capabilities that would have been separately licensed elsewhere as part of the value.

Chemical:

"It was a mix of cost and capability. It was a significantly better price than our previous tool, but Google also had a lot of capabilities out of the box that you'd pay extra for elsewhere. Gemini is a good example, and the Google Threat Intelligence platform was another."

The Prior Security Environment

The environments Google SecOps was brought in to replace differed in their specifics but shared a structural weakness. The accounts that follow are representative rather than exhaustive; organizations across the sample described comparable difficulties.

The volume of data its previous SIEM could usefully handle constrained one fintech organization:

Fintech:

"It's improved things through the efficiency SecOps has with large data sets; they're easier to deal with, query, and interact with. It was almost impossible to investigate with our last SIEM tool; SecOps deals with that large data much better and faster."

An industrial automation manufacturer identified a different gap, in which detections arrived without the context needed to act on them because the previous tools could not be connected to intelligence sources.

Industrial Automation:

"One challenge before was that our detections didn't have enough context because we couldn't connect the previous SOAR and SIEM to intelligence sources. With SecOps tightly integrated to Google Threat Intelligence, enrichment happens automatically."

For one media and technology organization, detection engineering had been an entirely manual discipline, but it is now a combination of curated and self-authored content.

Media/technology:
"Detection generation was manual before. Now we get a curated list from Google and also ones we make ourselves, so it's a hybrid approach. Historically, it was purely manual."

A chemical manufacturer describes the day-to-day consequences of a distributed toolset; an investigation conducted by moving between products.

Chemical:
"Having a platform like this is where you get the benefit: pulling it all into one. Without it, you'd have to go into several different places: into your EDR tool for EDR investigations, then jump into your network tool for those. It stops you jumping between tools."

The specific difficulties differ, but they share a common root cause across the sample: The data, intelligence, and response actions lived in separate places, so the analyst was the integration layer. Every benefit quantified in the remainder of this document is, at bottom, a consequence of removing that condition. It is also the baseline against which the operational figures are measured.

Participants consistently described Google SecOps as the central aggregation and orchestration layer their wider security stack feeds into, rather than a closed system. Out-of-the-box connectors, API-based integration, and a native integration marketplace materially reduced the effort of wiring in endpoint detection, network monitoring, cloud posture management, and identity and IT service management tools. Several emphasized that openness compounds the value of the platform's AI: The more telemetry fed in, the more context Gemini has to work with, and one participant highlighted that free and open source intelligence feeds integrate as readily as commercial ones, which was not true of alternatives they had used.

Gemini in Routine Daily Use

Google SecOps with Gemini reaches everyday adoption by embedding AI natively in the analyst workflow rather than bolting it on. Across the interviewed organizations, Gemini assists in 55.5% of investigations and workflows, and **88% of security analysts use it regularly.** That is not pilot activity confined to a group of enthusiasts; it is a routine part of how most analysts in these teams work.

Interviewed organizations attributed that adoption directly to where Gemini sits. Because it is part of the platform rather than a separate service, using it does not require a decision to leave the investigation and go elsewhere:

Telecommunications:
"It's native; it's actually within SecOps itself. That's a huge thing; you're not calling outside at all. When you log in, you have a whole section of Gemini right there."

The platform's agentic capabilities sit at an earlier stage of adoption than Gemini's assistive features. One of the interviewed organizations runs the Triage and Investigation agent in production and credits it with accelerating the determination of a true positive incident from a false positive. Another describes the same capability as experimental, using it to augment analysts rather than to make decisions. Several others describe agent-driven behavior without reference to the feature by name: autonomous first-pass analysis of incoming cases, a completed recommendation waiting on a ticket before an analyst opens it, and agentic logic built into their own response workflows. That distribution reflects a recently released capability rather than an established one, and it is distinct from the routine daily use of Gemini's assistive features reported above.

This adoption level is the precondition for everything that follows. The operational improvements quantified in the remainder of this document are not the benefits available in principle from AI assistance; they are the benefits realized by teams in which most analysts use that assistance most days.

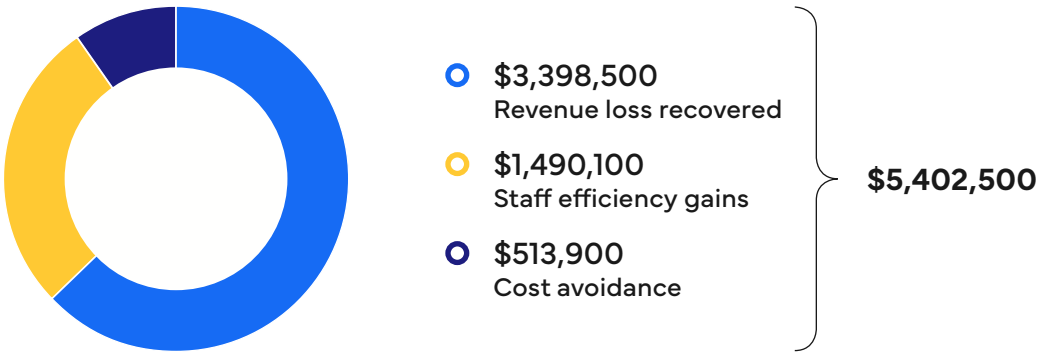
Average Annual Benefits per Organization

Across the seven interviewed organizations, Google SecOps with Gemini produces average annual benefits of $5.40 million per organization. These benefits fall into three categories: recovered revenue losses, security staff efficiencies, and cost avoidance **(Figure 1, next page).**

Figure 1

Average Annual Benefits

($ per interviewed organization)



Note: Factoring in deployment time of 4.1 months
n = 7; Source: IDC Business Value In-Depth Interviews, August 2026

These figures describe the average organization in the study rather than a uniform outcome. The composition of the benefit varies by participant: Most of the interviewed organizations retired platforms or licenses as part of the move to Google SecOps, but not all did, and for at least one, the platform change was commercially neutral, with the return arising from efficiency and simplification instead. The averages reported here reflect that mix.

What the three streams have in common is their origin. Bringing the security operations stack onto a single platform retires overlapping tools and their maintenance where duplication existed, which is the cost avoidance. That same single platform means investigations begin from enriched data with an AI first pass already performed, which is the staff efficiency. And because investigations resolve faster, fewer incidents progress to the point of interrupting the business, which is the recovered revenue. One architectural decision produces all three, which is also why the benefits arrive together rather than in sequence.

How Google Security Operations with Gemini Creates Value

Google SecOps with Gemini turns a consolidated data platform into separate value streams by putting an AI first pass in front of every human decision. The interviewed organizations describe a four-stage sequence, in which each stage depends on the one before it **(Table 3, below).**

Table 3

How Value Is Created with Google SecOps with Gemini

Stage	What Changes
Consolidate	Some organizations can consolidate tools.
Enrich	Threat intelligence context attaches to detections automatically.
Triage	An AI first pass analyzes and summarizes the case.
Respond	Analysts act on a summarized case in the same tool.

This produces four measurable value streams:

Value Stream	Mechanism
Staff efficiency	The same team can deliver a greater volume of work without adding head count.
Revenue recovery	Business interruptions are fewer and shorter.
Cost avoidance	Organizations can retire platforms, licenses, and maintenance.
Risk reduction	The expected loss from a serious breach is lower.

n = 7; Source: IDC Business Value In-Depth Interviews, August 2026

The sequence is presented as a chain rather than a list because that is how the benefits behave. The triage benefit is not available without automatic enrichment, and enrichment is not available without consolidated data. Interviewed organizations credit Gemini itself, principally at the triage and investigate stages, where the first-pass analysis is produced and the recommended action is presented; the earlier stages are properties of the consolidated platform on which that analysis depends. This interdependence is also part of why payback is so fast. The stages reinforce one another, so the value does not accumulate stage by stage over years; it arrives once the platform is live and ingesting.

Security Team Efficiencies

Google SecOps with Gemini allows the same security team to absorb more work because Gemini takes on the first-pass triage that used to consume analyst hours. The interviewed organizations quantified this as the staffing that the equivalent volume of work would require without the platform: an average of 28.6 full-time equivalents, against the 17.7 actually performing it with Google SecOps with Gemini. This is a 38.2% efficiency gain, equivalent to 10.9 FTEs of capacity released back to the team and worth $1,093,300 per organization annually **(Table 4, below).**

Table 4

Security Operations Team Efficiency Gains with Google SecOps with Gemini

Efficiencies	Before Google SecOps with Gemini	With Google SecOps with Gemini	Difference	Benefit
FTEs needed for equivalent work	28.6	17.7	10.9	**38.2%**
Value of staff time per year	$2,864,700	$1,771,400	$1,093,300	**38.2%**

n = 7; Source: IDC Business Value In-Depth Interviews, August 2026

Alongside this released capacity, the interviewed organizations quantified hiring they have been able to defer as their estates grew: 5.9 FTEs avoided, worth $587,500 annually.

Together, capacity released back to the team and hiring not required amount to $1,680,800 in savings per organization per year.

The nature of this benefit is specific, and the interviewed organizations were precise about it. Organizations did not reduce their teams. The gain is that the same people cover more ground and that roles that would otherwise have been needed to keep pace with a growing estate were not required.

One industrial automation manufacturer described redirecting people to other work within the security function rather than changing the team's size:

Industrial Automation:
"We were able to repurpose about four head counts because of Google SecOps and Gemini. Our detect-and-response team is about 20 people; we studied it and concluded we could repurpose 4 of the 20 to support other functions within the team, 100% of their time."

A chemical manufacturer draws the same distinction explicitly and locates the value in automation of work that was previously manual:

Chemical:
"We haven't reduced head count, but it allows us to do more with the team we have. We can automate work that would be manual; that's where we get the value, rather than reducing head count."

For a telecommunications operator, that additional capacity changed where human attention is applied, moving analysts up the escalation chain rather than out of the team:

Telecommunications:
"We can also not do as much tier 1 activity. We've allowed humans to focus on tier 2 and tier 3. From a business perspective, we don't really need tier 1 anymore."

Others expressed the same gains as throughput or as the staffing the work would demand without the platform:

Retail:
"The team is about 50% more efficient and productive compared to the pre-SecOps environment."

Fintech:
"Without it, it would be 10 to 12 people to do what 7 people do today."

These are the same mechanism expressed in different ways: an unchanged team covering an expanding estate, analysts redeployed to higher-value work within the security function, and hires not required as volumes grew. For security teams that are chronically short of people, that is the relevant currency. The value here is additional capacity and coverage, not a smaller security organization.

How the Investigation Process Changed

Google SecOps with Gemini reshapes the investigation process by handing the analyst a completed first pass instead of a raw alert. In the prior process, a raw alert arrived, the analyst pivoted between tools, built the context by hand, and only then decided and responded. In the current process, the alert arrives already enriched, Gemini performs a first pass, and the analyst reviews that completed analysis and responds in the same tool **(Table 5, below).**

Table 5
The Investigation Process Before and with Google SecOps with Gemini

Process	Step 1	Step 2	Step 3	Step 4
Before Google SecOps with Gemini	Arrival of raw alert	Pivoting between tools	Building context by hand	Deciding and responding
With Google SecOps with Gemini	Alert auto-enrichment	Gemini first pass	Analyst reviews	Responding in one tool

n = 7; Source: IDC Business Value In-Depth Interviews, August 2026

IDC also asked the interviewed organizations to assess the individual security analyst activities that the change affected. Averaged across those activities, interviewed organizations reported performing them 47.5% more efficiently with Google SecOps with Gemini. This is a discrete, activity-level measure of how analyst work itself has changed, expressed as an average across activities of differing frequency and duration. It is reported separately from the team-level efficiency figure above, and the two are not proportional to one another: No share of the 38.2% team efficiency gain is derived from this figure, and the two should not be read as the same finding measured at different scales.

The structural change is that the analyst is no longer the integration layer or the first pass. The analyst is the reviewer and the decision-maker and receives a case with an assessment and a proposed course of action already attached:

Telecommunications:

"An analyst picks up a ticket, and there's already an AI recommendation waiting. The human reads what the AI says: 'This is not a false positive, and here's why, and here are some actions I think you should perform.' SecOps is very good for that."

This change also alters which analysts can perform which work. Because the context an investigation requires is supplied rather than assembled, work that previously required senior involvement can be handled earlier in the escalation chain.

A point several interviewed organizations raised independently:

Retail:

"Gemini's first triage and case summarization enable junior analysts to handle initial investigations that previously required senior involvement. The automated preliminary analysis provides the context that junior analysts would otherwise lack."

Faster Security Reporting and Summarization

Google SecOps with Gemini shortens security reporting because Gemini writes the case and log summaries that analysts previously assembled by hand. Producing a security report or incident summary took an average of 5.2 hours before the platform; it now takes 0.8 hours, a reduction of 84% **(Table 6, below).**

Table 6

Time to Produce a Security Report or Incident Summary

Reporting Activity	Before Google SecOps with Gemini	With Google SecOps with Gemini
Hours to produce a security report or summary	5.2	0.8
Reduction in time required	N/A	84%

n = 7; Source: IDC Business Value In-Depth Interviews, August 2026

The industrial automation manufacturer described the change in concrete terms, attributing it to the speed at which the platform processes the underlying data:

Industrial Automation:

"It takes my team about eight hours to complete security reports and incident summaries. With Gemini, it's more than half, about an hour or a couple of hours to get the summaries, because it processes the data really fast."

This benefit is worth isolating because reporting is pure overhead. Every hour spent assembling a summary is an hour not spent on analysis, so the reduction converts almost directly into analytical capacity and reinforces the efficiency gain quantified above. It also changes what is feasible. Several interviewed organizations reported that once reporting became less labor intensive, they moved from periodic to continuous reporting, producing more reports in less time than the previous cadence required. One organization uses the platform's agentic capabilities to assemble reporting for board members and organizational leadership. Reporting at that frequency was not previously viable on either a time or cost basis.

From Telemetry to Realized Loss Mitigation

Google SecOps with Gemini narrows the path from monitored estate to realized loss because Gemini intervenes at the stages when a threat would otherwise progress unnoticed. The study measured that path at five points, from the estate under monitoring through to the expected annual financial loss from a serious breach **(Table 7, below).**

Table 7

From Telemetry to Realized Loss Mitigation

Stage	What the Study Measured
Monitored estate	33,900 endpoints and 9,900 Google Cloud VMs protected
Threats identified	34.9% to 74.4% of potential threats identified
Contained early	21.95 to 0.40 hours to detect; 14.8 to 1.85 hours to remediate

Table 7 continued next page

Table 7 continued from previous page

Stage	What the Study Measured
Impactful incidents	64.3 to 32.0 impactful incidents per month
Breach exposure	$555,000 to $346,900 expected annual loss

Note: The stages are illustrative of the narrowing from monitored estate to realized loss, not proportional to volume. The study attributes a measured share of the gain at the threat-identification and containment stages to Gemini itself; the later stages are outcomes of those interventions rather than separate Gemini findings. The financial impact at the final stage is an average across the interviewed organizations and reflects the scale of their estates and overall operations. It is modeled conservatively so that the analysis is not driven by a theoretical avoidance figure, while the underlying effect was consistently documented in the interviews.

n = 7; Source: IDC Business Value In-Depth Interviews, August 2026

The logic of the sequence is straightforward: A threat that is seen sooner and contained faster has less opportunity to become a loss. The two stages that follow quantify the interventions at the center of that sequence.

Mean Time to Detect and Remediate

Google SecOps with Gemini compresses detection and remediation because alerts arrive already enriched and pretriaged, and the response action sits in the same tool. **The average time to identify a potential threat fell from 21.95 hours to 0.40 hours, a reduction of 98%,** and the average time to address or remediate a threat fell from 14.8 hours to 1.85 hours, a reduction of 88% **(Table 8, below).**

Table 8

Mean Time to Detect and Remediate a Threat

Operational Metric (Hours)	Before Google SecOps with Gemini	With Google SecOps with Gemini	Percent Reduction
Average hours to identify a potential threat	21.95	0.40	98.2%
Average hours to address or remediate a threat	14.80	1.85	88%

n = 7; Source: IDC Business Value In-Depth Interviews, August 2026

These are averages across the interviewed organizations, with participants who began from the weakest position influencing them; at least one was measuring detection in days rather than hours. The mechanism behind the reduction is the one already established: The analyst is not spending hours assembling context because the context arrives with the alert, and there is no pivot to another product to execute the response.

Detection Coverage and Incident Volume

Google SecOps with Gemini widens detection coverage and thins incident volume because curated Google and Mandiant detections reach telemetry that previously went unexamined. The share of potential threats identified rose from 34.9% to 74.4%, an improvement of 53.1%, while impactful security incidents fell from 64.3 to 32.0 per month (32.3 fewer incidents), a reduction of 50% **(Table 9, below).**

Table 9

Detection Coverage and Impactful Incident Volume

Detection Measure	Before Google SecOps with Gemini	With Google SecOps with Gemini	Change
Share of potential threats identified	34.9%	74.4%	53.1% improvement
Impactful security incidents per month	64.3	32.0	50% reduction

n = 7; Source: IDC Business Value In-Depth Interviews, August 2026

These two findings belong together and are presented together deliberately. Wider coverage means the platform surfaces activity that previously passed unobserved, and several interviewed organizations noted that their raw detection counts rose after deployment for exactly that reason. What fell is the number of incidents that became impactful.

Catching more while fewer progress to the point of mattering is the expected result of better detection combined with faster containment, and the industrial automation manufacturer connects the two directly:

Industrial Automation:
"Because we're able to mitigate faster, incidents are a lot lower."

Revenue Recovered Through Fewer Business Interruptions

Google SecOps with Gemini protects revenue by containing incidents early, so attacks are stopped before they interrupt the operations customers depend on. The chain is a direct extension of the operational findings above: Threats are found earlier and contained before they spread, impactful incidents are halved and remediation time falls sharply, business systems remain available and customers stay served, and revenue that would have been lost is never lost.

IDC quantifies this at $3,833,300 in annual revenue losses recovered per organization, alongside $89,100 in annual third-party remediation costs avoided, as interviewed organizations required fewer hours from outside consultants to support incident response at the previous level **(Table 10, below).**

Table 10
Revenue Recovered and Third-Party Remediation Costs Avoided

Business Interruption Benefit	$ per Organization Annually
Annual revenue losses recovered	$3,833,300
Annual third-party remediation costs avoided	$89,100

n = 7; Source: IDC Business Value In-Depth Interviews, August 2026

This is revenue recovery, not revenue growth. The value arises from avoided interruptions rather than from new sales, and it is modeled conservatively against the scale of the interviewed organizations. For several of the participants in manufacturing, telecommunications, and retail, any interruption that reaches business operations translates immediately into material revenue exposure, which is why containment speed and incident volume carry a financial value at all.

Cost and Risk Avoidance

Google SecOps with Gemini removes duplicated platform spend and lowers expected breach loss by consolidating an overlapping stack of tools that reside on a single managed platform. Interviewed organizations avoid $282,500 annually in platform, maintenance, and operational costs and reduce risk-weighted breach exposure by $208,100 annually, a fall in expected annual loss from a serious breach from $555,000 to $346,900, or 37.5% **(Table 11, below).**

Table 11

Cost and Risk Avoidance with Google SecOps with Gemini

Cost and Risk Benefit	$ per Organization Annually
Platform, maintenance, and operational costs avoided	$282,500
Reduction in risk-weighted breach exposure	$208,100

n = 7; Source: IDC Business Value In-Depth Interviews, August 2026

The commercial position varies across the sample, and an honest characterization of it is comparable or lower platform spend combined with net-new capability.

The industrial automation manufacturer was explicit that the platform change was cost neutral and located the return in vendor simplification and operational efficiency rather than in the license line:

Industrial Automation:
"From a vendor-management perspective, it's easier to manage one vendor versus eight. There was no incremental cost in changing to SecOps; it was cost neutral; and the efficiency gains gave it that value for us."

On the risk side, the chemical manufacturer frames the value as loss that never materialized, which is the form risk reduction takes when it works.

Chemical:
"The main business value is cost avoidance; we've managed to prevent attacks in a proactive way in a lot of cases. It's cost avoidance from those attacks not being realized."

Risk and Business Resilience

The interviewed organizations described dimensions of risk that a financial model does not price.

For the chemical manufacturer, the exposure is not only commercial because the systems in question control physical processes with people working alongside them:

Chemical:
"For us, it's not just cost that's the risk; because we're a manufacturing company, we also have personnel safety. People work in our production plants, and if someone breached those systems, they could turn off safety systems and put lives at risk."

The industrial automation manufacturer describes a compounding effect on detection quality in which the consolidated telemetry allows lessons from an incident to be converted into new detections quickly.

Industrial Automation:
"This year with Google SecOps, it helped us create detections from a lessons-learned perspective; we could build detections for the gaps we identified during incidents rather quickly because we have all the telemetry within SecOps."

And the retailer locates the risk in a distributed physical estate rather than in a digital product:

Retail:

"We're a very physical business; we have stores where people go to do their groceries, so we're not a digitally native company. One part of it is securing all the systems deployed across all our stores."

Taken together, these accounts show that the consequences of a security failure are not confined to financial loss. For several interviewed organizations, the systems being protected underpin continuity of operations, and in industrial settings, they extend to the environments in which employees work, considerations that sit alongside the quantified benefit rather than within it.

Business Impact and Agility

Interviewed organizations described business-level effects that this study did not quantify. These are single-organization and self-assessed accounts, and they are excluded from the average annual benefits and from the return on investment presented in this document. They are included here because they indicate where the value of these deployments extends as they mature.

The telecommunications operator connects the platform to the speed at which new applications can be brought into service securely and therefore to time to market:

Telecommunications:

"When a new app comes up, we're able to bring it online and secure it much quicker; the reduction in time to market is probably 50%. In theory, that could mean more revenue; I don't know exactly how much, but it would be millions a year for sure."

The media and technology organization reported a direct, if small, revenue effect alongside uniformly improving security metrics.

Media/Technology:

"In security, all of our metrics are on a positive trend because of it: mean time to remediation, mean time to detection. On the business side, it's enabled us to generate more revenue; I'd say half of 1% at the moment and increasing."

The common theme is a change in the role security plays in the organization: from a constraint on shipping new applications and services to a capability that allows them to be shipped sooner.

ROI Analysis

Google SecOps with Gemini pays back its investment quickly because additional team capacity, retired platform spend, and avoided incident loss all accrue from the same platform change. Over three years and per interviewed organization, IDC calculates discounted benefits of $12,784,800 against a discounted investment of $3,054,600, producing a net present value (NPV) of $9,730,200, a 319% return on investment, and a seven-month payback on investment at a 12% discount rate **(Table 12, below).**

Table 12

Three-Year ROI Analysis

ROI Analysis	Per Organization	Per 1,000 Endpoints Protected
Discounted benefits	$12,784,800	$377,610
Discounted investment	$3,054,600	$90,220
NPV	$9,730,200	$287,390
ROI	**319%**	**319%**
Payback	**7 months**	**7 months**
Discount factor	12%	12%

n = 7; Source: IDC Business Value In-Depth Interviews, August 2026

The second column normalizes the same analysis per 1,000 endpoints protected, which is the more useful basis for comparison across organizations of different scale given the range of estate sizes in the sample. On that basis, the platform returns $377,610 in discounted benefits and $287,390 in net present value per 1,000 endpoints protected.

The speed of the payback follows from the structure of the benefit rather than from the size of any single component. Because a single change produces additional capacity, retired platform spend, and reduced incident loss at the same time, benefits begin accruing as soon as the platform is live and ingesting, which, at an average of 4.1 months to initial deployment, is early. The staff efficiency and operational time savings are the most heavily evidenced components of the model, drawn from the interviewed organizations' own accounts of security operations center staffing, analyst time allocation, and measured process durations.

Challenges/Opportunities

The results in this document describe organizations that have already crossed several adoption thresholds. For organizations earlier in that process, four conditions determine whether comparable outcomes are achievable.

AI analysis depends on the context provided, which is contained in the accessible data. The value the interviewed organizations attribute to Gemini is inseparable from the consolidation and automatic enrichment that precede it because a first-pass analysis is only as good as the telemetry and context available to it. Organizations that treat AI assistance as a capability to add to an existing fragmented estate should expect a materially smaller effect than the one this study describes.

The second is adoption at the point of work. Participants attributed the adoption levels in this study, and therefore the benefits, to native integration rather than to model capability in the abstract. AI assistance that requires the analyst to leave the investigation competes with the investigation and loses.

The third is the persistence of human review. The value this document describes comes from analysts reviewing a completed first pass rather than from unsupervised automation, and the interviewed organizations consistently described the analyst as the reviewer and decision-maker. Operating models that assume the AI first pass is a final answer rather than a starting position are not the models under which these results were produced.

The fourth is measurement. Security teams are not always instrumented to record the figures this study asked for: time to identify a threat, share of potential threats identified, and hours per report. Organizations that establish those baselines before deployment are in a substantially better position to demonstrate the value afterward and to govern the cost of AI-assisted operations as usage scales across more of the workflow.

Analyst observations:

- The determining variable in AI security operations is not model quality but data access and workflow placement; both are architectural decisions taken before any AI capability is evaluated.
- Buyers should consider their own operating model. The benefit this study quantifies arises from analysts moving from first-pass investigation to review and decision, and that shift is visible in how a security operations center is tiered and staffed.
- Wider detection coverage and lower impactful-incident volume should be assessed together. Coverage improvements can raise raw detection counts, and evaluating either measure in isolation gives a misleading picture of the change.
- As AI assistance moves from triage into more of the workflow, the economics of that assistance become an operational discipline in its own right, and organizations should expect to govern where they apply AI rather than applying it everywhere by default.

Conclusion

Security operations teams are being asked to monitor attack surfaces that grow faster than they do, often with tooling that was accumulated rather than architected to work together. The consequence is that the analyst becomes the integration layer, needing to swivel into various interfaces during an investigation. This caps how many of the alerts are reviewed, as each investigation is a labor-intensive exercise.

The experiences of the organizations in this study indicate that the effective response is architectural rather than incremental. Consolidating telemetry onto a single platform, attaching threat intelligence automatically, and placing a native AI first pass in front of every human decision changed the same set of measures in every organization IDC interviewed, across seven unrelated industries and security teams differing by an order of magnitude in size. Detection and remediation times fell by 98.2% and 87.5%, respectively; the share of potential threats identified rose from 34.9% to 74.4%, while impactful incidents halved; reporting time fell by 83.9%; and the security team absorbed 38.2% more work.

Within IDC's Business Value framework, those operational changes produce average annual benefits of $5.40 million per organization, a 319% three-year return on investment, and payback in seven months. The composition of that return matters as much as its size. It does not rest on a single benefit; released capacity, recovered revenue, retired platform spend, and reduced breach exposure each contribute, and each derives from the same consolidation. That is also why the payback is fast; the benefits do not arrive in sequence as the deployment matures but together, once the platform is ingesting.

For security leaders evaluating AI in the security operations center, the finding with the widest application is about sequencing. The interviewed organizations did not obtain these results by adding AI to their existing environment; they obtained them by consolidating the environment first, which is what made the AI assistance useful and, at 88.2% analyst adoption, actually used.

Appendix: Methodology

IDC utilized its standard Business Value methodology for this project, gathering data from organizations currently using Google SecOps with Gemini as the foundation for the model **(Table 13, below).**

IDC performed a three-step process to calculate the ROI and payback period:

1. **Measure the savings** from reduced operational expenses, increased user productivity, and revenue growth over the term of the deployment.
2. **Ascertain the investment** made in deploying and using the solution and the associated migration, training, and support costs.
3. **Project the costs and benefits over a three-year period** and calculate the ROI and payback period from the use of Google SecOps with Gemini.

Table 13

IDC Business Value Methodology Measures

Measure	Explanation
Present value of benefits (discounted benefits)	The current value of the total benefits over the time frame, reduced by the discount factor
Present value of investment (discounted investment costs)	The current value of the total investment over the time frame, reduced by the discount factor
Net present value	Present value of cash flows = discounted benefits – discounted investments
ROI	The ratio of the NPV and the discounted investment = NPV/ discounted investment
Payback period (months)	The point at which cumulative benefits equal the investment up until that time
Discount factor (average cost of capital)	The cost to discount the cash flow to allow for the missed opportunity cost, accounting for both the assumed cost of money and the assumed cost of risk

n = 7; Source: IDC Business Value In-Depth Interviews, August 2026

IDC bases the payback period and ROI calculations on several assumptions, which are summarized as follows:

Table 14

Assumptions Used in This Study

Assumption	Value
IT and security staff annual salary	$100,000
Other-user annual salary	$70,000
Hours worked per year	1,880
Operating-margin assumption	15%
Discount rate	12%

n = 7; Source: IDC Business Value In-Depth Interviews, August 2026

Further, because IT solutions require a deployment period, the full benefits of the solution are not available during deployment. To capture this reality, IDC prorates the benefits on a monthly basis and then subtracts the deployment time from the calculated benefits.

About the IDC Analysts



Michelle Abraham

Senior Research Director,
Security and Trust, IDC

Michelle Abraham is a senior research director in IDC's Security and Trust Group and is responsible for the Security Information and Event Management, Exposure Management, and Related Artificial Intelligence Technologies practice. Abraham's core research coverage includes SIEM platforms, exposure management platforms, attack surface management, breach-and-attack simulation, cybersecurity asset management, and device vulnerability management alongside AI-related security topics.

More about Michelle Abraham →



Ladislav Kinda

Consultant,
Business Value Strategy Practice, IDC

Ladislav Kinda is a consultant in the IDC Business Value Strategy practice team. Kinda conducts customized business value research and consulting projects for clients across various technology domains. His primary focus is assessing the return on investment from their adoption of enterprise technologies. Kinda's research delves into how organizations leverage digital technology solutions and initiatives to enhance efficiency and drive business growth.

More about Ladislav Kinda →

Message from the Sponsor

Google Cloud

A modern, AI-powered security operations platform. Google Security Operations is a cloud-native SecOps platform that empowers security teams to better defend against today's and tomorrow's threats.

By combining Google's hyper-scale infrastructure, unparalleled visibility and understanding of cyber-adversaries, Google Security Operations provides curated outcomes that proactively uncover the latest threats in near real time, and enable security teams to detect, investigate, and respond with speed and precision.

- Eliminate blind spots. Ingest and analyze your security telemetry at scale with 12 months of hot data retention.
- Get ahead of threat actors. Proactively uncover and defend against novel attacks in near real time without extensive custom engineering. Curated outcomes apply Google's vast threat and exposure visibility to your unique environment.
- Elevate talent and productivity. Duet AI in Security Operations simplifies complex data analysis and security engineering and provides insights so your team can detect and respond to more threats faster.

Learn more about Google Security Operations

IDC Custom Solutions

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies.

This IDC material is licensed for external use and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

IDC.com | IDC on LinkedIn | IDC Blog

International Data Corporation (IDC) is the technology intelligence layer of the AI economy. A global leader in research and data for more than 60 years, IDC's expert analysts, proprietary datasets, and rigorous methodologies are trusted by business and IT leaders to guide critical business strategies and IT investments. Today, that intelligence is built into the tools and workflows where work gets done with IDC Quanta, making work sharper, teams faster, and businesses harder to beat.

©2026 IDC. Reproduction is forbidden unless authorized. All rights reserved. CCPA