The Business Value of Google Security Operations

Michelle Abraham
Research Director,
Security and Trust, IDC

Matthew Marden
Research Vice President,
Business Value Strategy Practice, IDC

Table of Contents

CLICK ANY HEADING TO NAVIGATE DIRECTLY TO THAT PAGE.

Executive Summary

The security information and event management (SIEM) platform is the central analytics tool for the security operations center. Telemetry and log data from other security tools are brought into the SIEM so that it can be correlated, and new understanding can be gained when it is analyzed together rather than in separate silos. Bringing the data together makes investigations easier, helping identify more adversary activity and increasing the efficiency of the security team. This in turn lowers the probability of large-scale attacks because teams detect adversary activity earlier and can stop threat actors before they take down an entire system.

SIEMs are complex security platforms with many data connectors and numerous options for detection rules. The rules must be tuned to the organization's specific environment to reduce false positive alerts so security teams can focus on detecting and investigating critical incidents. In addition to tuning, developing and running automated playbooks can greatly improve the efficiency of security teams by offloading mundane tasks in order to have time to focus on those that call for their expertise. Security teams need to make sure they are receiving the full value from their SIEM, taking advantage of all the capabilities.

IDC interviewed organizations using Google Security Operations (formerly known as Google Chronicle) to understand its impact on their security capabilities and operations. According to study participants, Google Security Operations enables them to analyze and correlate far more data, which leads to improved security outcomes and efficiencies for the staff responsible for analyzing and engineering security data.

IDC calculates that interviewed Google customers will realize average annual benefits worth $4.29 million per organization ($104,500 per 1,000 endpoints covered) by:

- Significantly improving threat identification and resolution capabilities, thereby limiting the likelihood of suffering serious security incidents
- Helping security operations teams work more efficiently by providing high-quality insights about threats and correlation and allowing them to spend less time on monitoring activities
- Capturing higher revenue by moving with greater speed and confidence to address business opportunities and customer needs
- Enabling ingestion of significantly more data and data logs by separating data volumes from incremental costs

Business Value Highlights

Click highlights below to navigate to content within this document.

$13.50 million
higher revenue per organization per year

7 months
to payback

407%
three-year ROI

283%
higher data ingestion volumes

87%
more potential threats identified

85%
more capacity for data logs

60%
reduced likelihood of a major security incident

42%
more efficient security operations teams

While this IDC study demonstrates the tangible benefits for study participants of using Google Security Operations, the more intangible value of peace of mind can be just as important. As an interviewed CISO at an EMEA automotive-related company with an annual revenue of $5 billion to $10 billion explained:

"Our cybersecurity teams deal with issues faster with Google Security Operations, but they also identify more issues. The real question is, 'How much safer do I feel as a CISO with Google Security Operations versus my old platform?' and I would say 100 times safer."

Situation Overview

SIEM was originally a storage platform for log data that may need to be retained for compliance reasons. Log storage is still a requirement in the SIEM today, but it also evolved into a security analytics platform that detects issues in an organization's IT environment and sends out alerts around questionable activity. Because it ingested telemetry from multiple tools, it brought together alerts from many sources. Therefore, security analysts did not have to work in each security tool dashboard, and they could perform much of their work in the SIEM.

Over time, security teams wanted to bring more and more data into the SIEM to help understand security incidents. Their IT environments grew more complex when they moved processes to the cloud while keeping others on premises. The data ingestion needs often grew faster than the infrastructure that supported it. Managing the SIEM infrastructure is the full-time job of a team of people in large enterprises. Cloud SIEMs change that requirement, freeing those people to other tasks to help detect, investigate, and respond to threats.

Typically, SIEM pricing is based on the amount of data ingested into the SIEM platform. Since there is consistently more data to evaluate, security teams have to make choices around what data to ingest and what to leave or store elsewhere. When data is stored outside the SIEM, it may not be queried as quickly as that stored in the SIEM.

As environments grow more complicated, the unknowns and lack of visibility can create problems for defenders. SIEM vendors have added user and entity behavior analytics (UEBA) functionality, which uses machine learning (ML) algorithms to identify anomalous behavior of humans and machines in the IT environment. UEBA helps find unknown threats and novel methods that do not yet have signatures or detection rules.

Our cybersecurity teams deal with issues faster with Google Security Operations, but they also identify more issues. The real question is, 'How much safer do I feel as a CISO with Google Security Operations versus my old platform?' and I would say 100 times safer."

CISO
EMEA automotive-related company, annual revenue of $5 billion to $10 billion

When it comes to detection rules, many organizations have a difficult time writing and maintaining detection rules for their environments because they lack the time or knowledge. Organizations may have detection engineering teams to do the work due to the complexity of the task.

The speed of attacks and the complexity of the environment also require automation and continuous monitoring of all relevant security data. SIEMs alert on issues, but there may be false positives where investigation time could be avoided if there is context for each alert. Multiple alerts may relate to the same incident, so it is better to correlate the alerts to present the security analyst with all the context available to help them determine the risks and the best response, making them more efficient and effective.

Google Security Operations

Google Security Operations is a unified, fully featured security operations platform. It offers the following benefits to customers:

- **AI integration:** Google has developed several cybersecurity Duet AI applications powered by its specialized large language models, fine-tuned for security use cases. Use cases today for Duet AI in Security Operations include natural language queries that are translated to machine query language, detection generation, case summaries, recommended next steps, and malicious scripts analyses.
- **Threat intelligence:** Google Security Operations customers receive intelligence from Mandiant, VirusTotal, and Google's own network and services, which is automatically correlated to threats seen in the customer environment. Google Security Operations stitches together the relevant information to offer context around the threat, which is one less task the security analyst has to perform.
- **Integrated case management:** Google Security Operations correlates alerts into threat-centric cases that can then be assigned in their entirety to an analyst. A built-in chat feature makes collaboration between analysts simpler. Playbooks enable automated response capabilities to reduce both proactive and reactive analyst tasks.
- **Response automation:** Google Security Operations offers integrated security orchestration, automation, and response, allowing customers to build playbooks that automate common response scenarios and speed up remediation.

- **Scalability and speed:** Google Security Operations runs on the same hyper-scalable infrastructure that powers popular Google services such as search, so customers do not have to be concerned about having the infrastructure needed to analyze their security data. Querying is a quick process and can be run against data where it resides.

To expedite time to value and decrease reliance on "DIY" detection engineering, Google is providing curated detections for customers based on emerging threats. In addition, customers can build their own detections using the YARA-L language. Ingestion of data from Google Cloud allows cloud monitoring to be automated. Customers can easily build playbooks that can be integrated with over 300 external security tools for faster, automated response.

Google Security Operations is also rapidly integrating Mandiant's capabilities and expertise. Customers can receive early warning signals about the latest breach data from Mandiant investigations in the console. Customers can also opt for integrated Mandiant threat hunting and incident response services. On the proactive side, Google Security Operations integrates with Mandiant attack surface management and will likely add security validation integration in the future.

> We researched competing solutions and determined that Google Security Operations is the best out there at identifying suspicious activity and threats … We needed something that was highly reliable and helps identify threats."
>
> CIO
> North America software company, annual revenue of $500 million to $1 billion

The Business Value of Google Security Operations

Study Demographics

IDC interviewed security managers and executives at eight organizations about their experiences using Google Security Operations. Interviews were designed to understand the impact of using Google Security Operations from both quantitative and qualitative perspectives.

Table 1 (next page) provides information about the organizations participating in the study. On average, they had 29,025 employees and an annual revenue of $8.34 billion at the time of interviews (medians of 14,500 employees, $5.30 billion in revenue), indicating the average profile of a large enterprise. They spoke about how they have used Google Security Operations to address security challenges from the perspective of various industry verticals: banking (2), automotive, healthcare, insurance, IT manufacturing, manufacturing, and software.

TABLE 1

Demographics of Interviewed Organizations

	Average	Median
Number of employees	29,025	14,500
Number of IT staff	1,478	925
Number of business applications	1,147	625
Annual revenue	$8.34B	$5.30B
Countries	United States (7), United Kingdom	
Industries	Banking (2), automotive, healthcare, insurance, IT manufacturing, manufacturing, software	

n = 8; Source: IDC's Business Value In-Depth Interviews, October 2023

Choice and Use of Google Security Operations

Study participants primarily deployed Google Security Operations as a one-to-one replacement for security solutions that they concluded no longer met their needs. They realized that rapid growth to data had made solutions for which price scaled alongside data volumes untenable and that they required a solution with the strongest possible capabilities in terms of analyzing and correlating data to enhance security capabilities. For these organizations, Google Security Operations met these foundational requirements that allow them to not only improve their security postures but also establish security capabilities that align with market and technological changes.

Organizations described important selection criteria in their own words:

Strong threat detection capabilities:

"We researched competing solutions and determined that Google Security Operations is the best out there at identifying suspicious activity and threats … We needed something that was highly reliable and helps identify threats."

— CIO, North America, software, annual revenue of $500 million to $1 billion.

Right platform for maintaining control over data security:

"We wanted to establish a data lake, and Google Security Operations allows for more granular control over how we process security data, given that we have a very technically capable security group."

— Information and product security officer, North America, IT manufacturing, annual revenue of $5 billion to $10 billion.

Right pricing model, improved capabilities:

"Google Security Operations' pricing model is fundamentally different … and drives a much more defined way of charging for growing a security monitoring and instant response capability."

— CISO, EMEA, insurance, annual revenue of $1 billion to $5 billion.

Table 2 provides an overview of how study participants use Google Security Operations. Most importantly, they use Google Security Operations to secure large numbers of endpoints and employee devices that access their networks, reflecting the extent to which they rely on Google Security Operations to secure the devices and productivity tools that their employees use on a day-to-day basis (41,048 endpoints on average, which includes 22,786 employee devices on average). **Table 2** also reflects interviewed customers' use of Google Security Operations to secure diverse IT infrastructures, ranging from on premises with minimal virtualization to largely cloud-based environments.

TABLE 2

Use of Google Security Operations by Interviewed Organizations

	Average	Median
Number of endpoints accessing internal networks	41,048	12,000
Number of total employee devices	22,786	12,000
Number of Google Cloud VMs	81	13
Number of other cloud VMs	1,008	25
Number of on-premises servers	1,141	420
Number of on-premises VMs	629	8

n = 8; Source: IDC's Business Value In-Depth Interviews, October 2023

Business Value Results

Interviewed customers linked their use of Google Security Operations to tangible improvements in security outcomes for their organizations. They consistently reported covering greater volumes of data and data logs without incurring parallel cost increases, with increased data coverage translating directly into a more actionable and robust understanding of security threats. They reported leveraging this understanding to better

track, identify, and address security threats, which yields significant efficiencies for their security operations teams while reducing business costs associated with security events.

Study participants detailed these main benefits of using Google Security Operations:

Data-centric and intelligence-led security posture:

"The investment in being data centric and intelligence led is very important for us, with Google Security Operations being core to moving us into almost a pre-attack-based defensive posture so we can anticipate much better what the attackers are going to do, and we can modify our defenses based on that."

— CISO, EMEA, insurance, annual revenue of $1 billion to $5 billion.

Speed, scale, and cost:

"Speed, scale, and cost are the most significant benefits of Google Security Operations … We're doing 10 times the amount of work that we could with our previous solution … At a minimum, we're avoiding doubling our costs with Google Security Operations."

— Information and product security officer, North America, IT manufacturing, annual revenue of $5 billion to $10 billion.

Unlimited data ingest capacity:

"The most significant benefit of using Google Security Operations is the ability to ingest unlimited data. Also, its dashboard is good, so you can look at activities for hourly or weekly, or however you want to see it."

— VP, Security Operations Center, North America, banking, annual revenue of $1 billion to $2 billion.

As shown in **Figure 1** (next page), IDC calculates that study participants will realize benefits worth an average of $4.29 million per organization per year through their use of Google Security Operations ($104,500 per 1,000 endpoints) in the following areas:

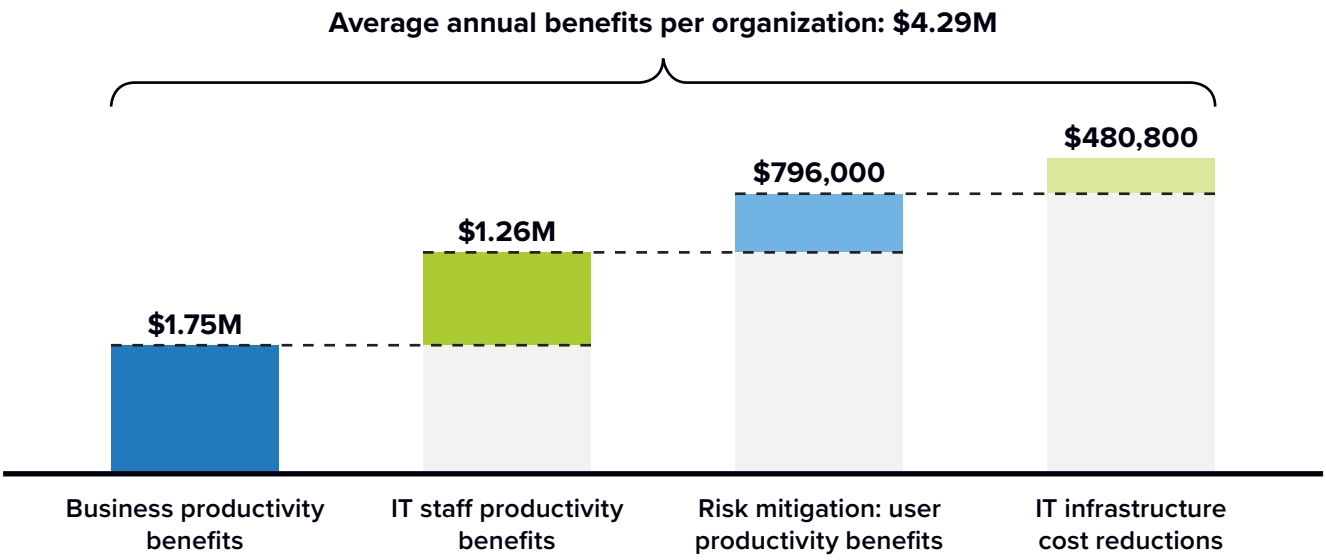
- **Business productivity benefits:** Study participants leverage increased confidence and stronger security foundations to move more readily and confidently to address business opportunities and serve their existing customers. As a result, IDC estimates that study participants will realize $1.75 million per organization in higher net revenue per year ($42,600 per 1,000 endpoints).
- **IT staff productivity gains:** Security operations teams responsible for analysis and engineering benefit from enhanced data and threat correlation, improved understanding of security threats, and the ease of use of Google Security Operations. IDC assesses the value of resultant security operations teams' efficiencies and productivity gains at an annual average of $1.26 million per organization ($30,700 per 1,000 endpoints).

- **Risk mitigation — user productivity benefits:** Interviewed Google Security Operations customers head off more security threats and resolve potential security incidents more quickly, bringing down the risk that security events pose to their organizations. IDC puts the value of reduced business losses and fines associated with security events and compliance at an annual average of $796,000 per organization ($19,400 per 1,000 endpoints).
- **IT infrastructure cost reductions:** Study participants generally replaced one or more other security solutions, allowing them to optimize spend even as they realize significant additional value in other areas with Google Security Operations. IDC calculates that study participants will no longer spend an annual average of $480,800 per organization on these other solutions ($11,700 per 1,000 endpoints).

FIGURE 1

Average Annual Benefits per Organization

($ per year per organization)



n = 8; Source: IDC's Business Value In-Depth Interviews, October 2023

For an accessible version of the data in this figure, see Figure 1 Supplemental Data in Appendix 2.

Improved Security Capabilities and Outcomes

Study participants connected their use of Google Security Operations to improved security capabilities and ultimately security outcomes. This reflects their ability with Google Security Operations to identify, address, and resolve potential security threats more efficiently and readily, which reduces their security exposure.

As explained, customers' ability to cost-effectively put more data and data sources into the Google Security Operations platform than they could with their previous security solution(s) is a fundamental benefit. However, they also spoke about numerous other features and capabilities of Google Security Operations that further enable them to improve their security position.

For example, study participants noted the ease with which Google Security Operations takes in and integrates disparate data sources, thereby not only reducing the burden of doing this but also allowing for security coverage for a broader spectrum of data inputs. Interviewed customers provided examples of beneficial features and functionalities of Google Security Operations:

- Ease of search for analysts because it is based on a Google search
- Ability to run precise reports to get metrics that identify anomalies
- Ability to collate and rationalize complicated data from multiple sources
- Importance of strong back-end compute platform to searches and timely resolution

Several interviewed organizations provided more detailed assessments of how Google Security Operations has improved their security capabilities:

Value of direct intelligence integration and dynamic rule application:

"The direct integration of intelligence into the Google Security Operations platform and being able to do that both with Google providers and through our own intelligence capability providers is absolute gold … It allowed us to pivot quickly away from being rules based to dynamic rules and using ML and AI."

— CISO, EMEA, insurance, annual revenue of $1 billion to $5 billion.

Ability to assess and ability to respond going forward based on strong historical understanding:

"Having good information and data in real time with Google Security Operations saves us a heck of a lot of effort. It's about using both the humans and the machines to do the job that they're good at to assess the threat, make sure we've got the intelligence around it, and make sure that we've not been hit by it previously and we can respond going forward."

— CISO, EMEA, insurance, annual revenue of $1 billion to $5 billion.

The direct integration of intelligence into the Google Security Operations platform and being able to do that both with Google providers and through our own intelligence capability providers is absolute gold … It allowed us to pivot quickly away from being rules based to dynamic rules and using ML and AI."

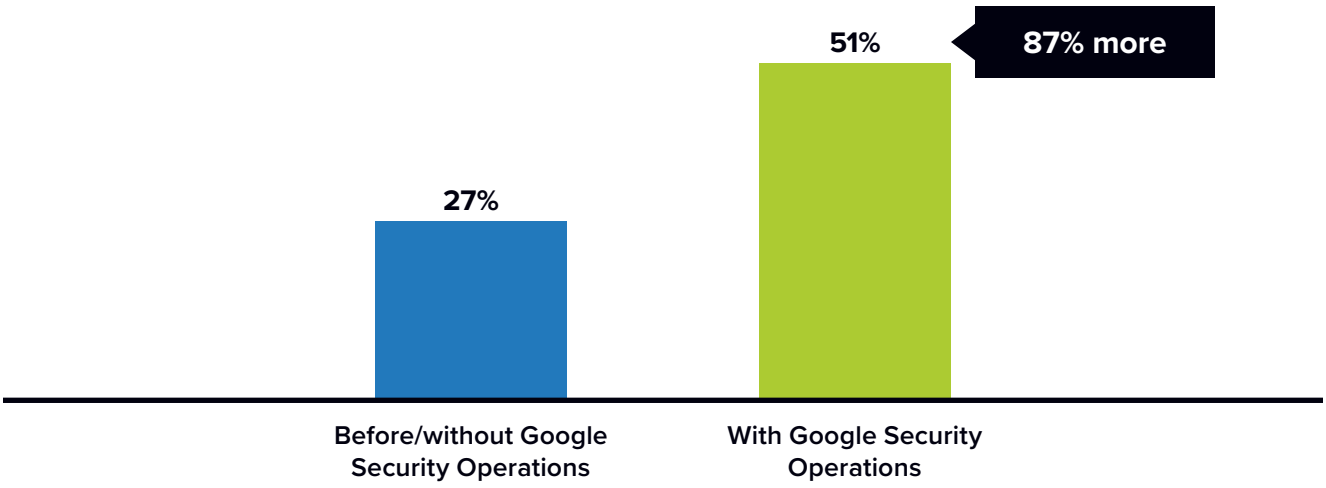
CISO
EMEA insurance company, annual revenue of $1 billion to $5 billion

For security operations teams, the first order of business is often identifying potential threats. Without the right tools to identify threats, it becomes more challenging to respond correctly and head off possible negative consequences. Study participants reported that they identify almost two times (87%) more security threats proactively with Google Security Operations (see **Figure 2**). A security analyst at the interviewed North American manufacturing customer with $10 billion to $20 billion annual revenue explained the value of improved data visibility: *"Google Security Operations allows us to identify more security threats, or at least we now know of more of them, before they become impactful … We now have better visibility into our data, so we can do more sophisticated searches with Google Security Operations."*

FIGURE 2

Impact on Threat Identification Capabilities

(Percentage of threats identified)



n = 8; Source: IDC's Business Value In-Depth Interviews, October 2023

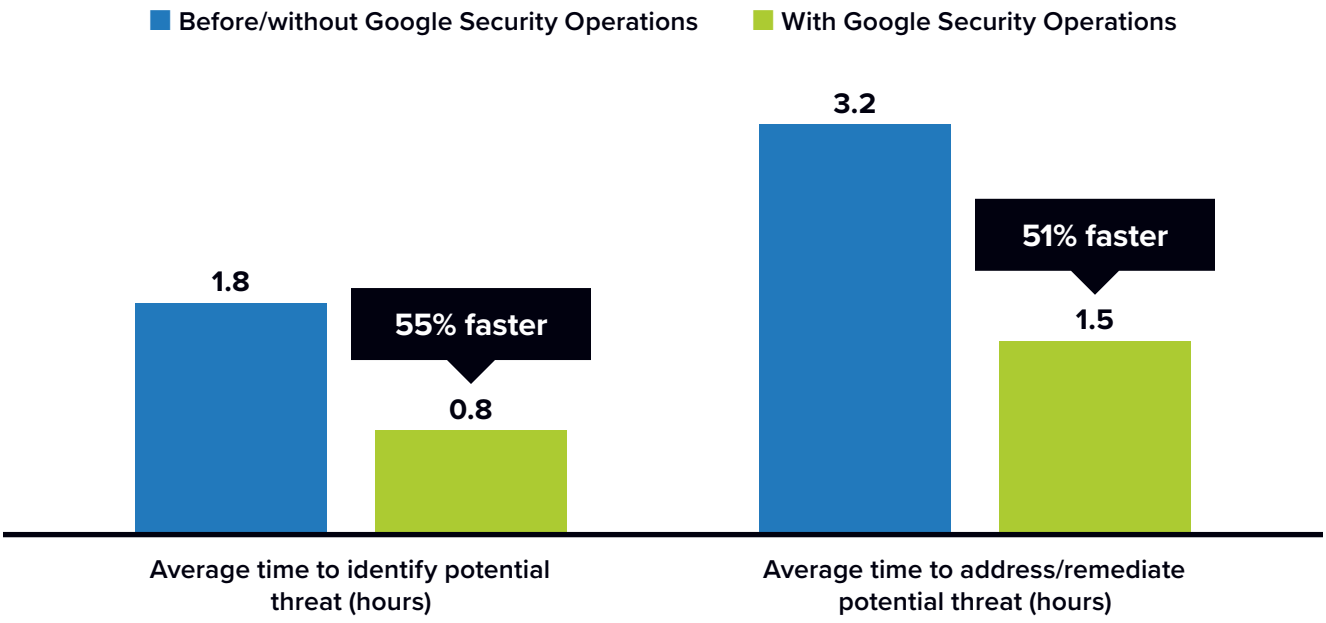
In addition to proactively identifying more threats with Google Security Operations, study participants also reported improving their threat response and remediation capabilities. A VP at an interviewed North American banking customer with annual revenue of $25 billion to $50 billion explained: *"We have much faster turnaround for security resolution with Google Security Operations, which means we can minimize the impact of downtime … We can deliver much better service-level agreements to both internal and external users."* The same customer noted: *"Google Security Operations has a log file aggregation tool and the ability to search for events that can be done with greater scalability … This helps us reduce the time to remediate security issues. We've improved from needing around eight hours on average previously to around five hours per event with Google Security Operations."*

Figure 3 shows the key findings on the impact of Google Security Operations on study participants' threat response capabilities. On average, study participants reported identifying potential threats 55% faster and needing 51% less time to address or remediate potential threats. These gains in security capabilities translate directly into reducing the actual business and operational risk that such threats pose.

FIGURE 3

Impact on Threat Response Capabilities

(Number of hours)



n = 8; Source: IDC's Business Value In-Depth Interviews, October 2023

For an accessible version of the data in this figure, see Figure 3 Supplemental Data in Appendix 2.

Table 3 (next page) reports on the tangible impact for study participants of reducing security-related business risk and exposure. It shows that interviewed Google Security Operations customers understand the significant toll that major impactful security events can have, with an average total cost of $7.4 million per organization in lost revenue, direct remediation costs, and staff time costs. Interviewed organizations acknowledged that these types of security events do not occur with great frequency but noted that they have substantially reduced the likelihood with Google Security Operations. One interviewed customer commented: *"We're constantly looking for malicious behavior on the network or coming from external actors. Google Security Operations helps us look for this malicious activity and block it, and there's a dollar value attached to that. We've avoided around $2 million per year in real actual costs related to fraud."*

By bringing down the likelihood of being affected by such a major security event by 60%, IDC calculates that interviewed Google Security Operations customers will reduce security-related costs by an average of $470,800 per organization per year and also avoid $450,000 per year in related fines and penalties from regulatory bodies and customer service-level agreements.

TABLE 3

Impact on Cost of Major Security Incidents and Penalties

	Before/ Without Google Security Operations	With Google Security Operations	Difference	Benefit
Total cost per major impactful security event (average per interviewed organization)	$7.40M	$7.40M	NA	NA
Chance of major security event happening in any given year	45%	18%	27%	60%
Annual cost of major security events (average per interviewed organization)	$1.18M	$0.71M	$470,800	60%
Value of reduced fines/penalties per year (average per interviewed organization)	$450,000			

n = 8; Source: IDC's Business Value In-Depth Interviews, October 2023

Cost-Effective Data Ingestion Capacity

Prior to using Google Security Operations, study participants reported significant limitations in their ability to cost-effectively secure their growing volumes of operational data with their security solutions. In particular, they faced the dilemma of either facing cost increases that closely tracked their data volume growth or having to choose which data sources to put into their security platforms. This meant that they often either operated knowing that they had security blind spots or were forced to justify increased spending on their security operations.

For study participants, Google Security Operations has greatly reduced the extent to which cost factors into their ability to extend their security coverage. With Google Security Operations, study participants no longer face limits tied to licenses or number of data sources.

As a result, study participants benefit from limiting the connection between data volumes and the cost of their security solutions:

Eliminate data ingestion limit concerns:

"Data ingestion limits was the main issue with our previous solution. We had a license limit of 3TB a day, and we don't have to worry about that with Google Security Operations. We often didn't even use the 3TB because we were always trying to maintain that limit."

— VP, Security Operations Center, North America, banking, annual revenue of $1 billion to $2 billion.

Avoid incremental costs of additional storage capacity:

"We wouldn't have been able to increase the number of log sources with [our previous solution] … We would have had to pay incrementally for more storage space, which would be part of millions of dollars overall that we're avoiding with Google Security Operations."

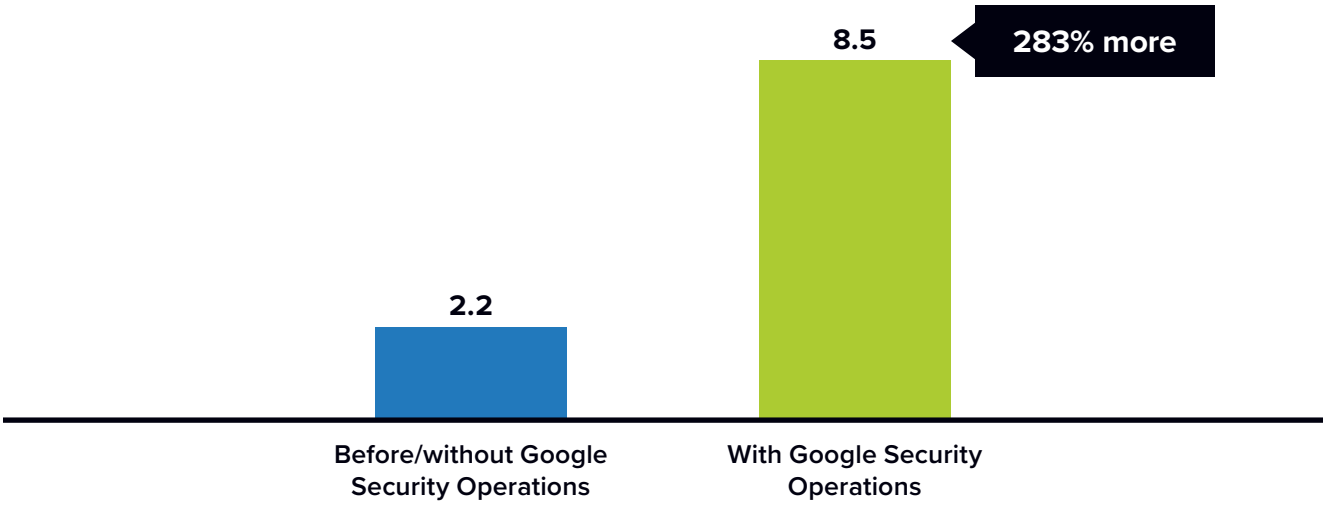
— Information and product security officer, North America, IT manufacturing, annual revenue of $5 billion to $10 billion.

Figure 4 shows the significant extent to which study participants have increased the amount of data they put into Google Security Operations compared with their previous solutions. By ingesting almost four times (283%) more data, they not only increase the scope of their security coverage but also provide more data from which Google Security Operations can draw correlations and conclusions.

FIGURE 4

Impact on Data Ingestion Volume

(TBs per day)



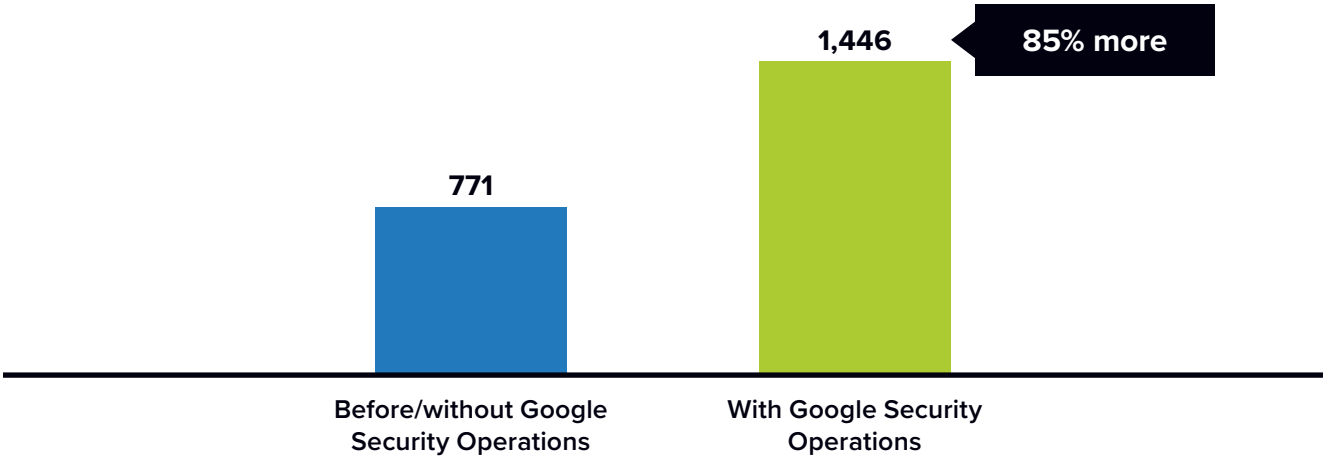
n = 8; Source: IDC's Business Value In-Depth Interviews, October 2023

Likewise, **Figure 5** reflects how Google Security Operations has allowed study participants to cover far more data logs on an ongoing basis. Again, by having an average of 85% more data logs covered with Google Security Operations, study participants have broader security coverage and a more unified approach to securing their operational data than with previous solutions.

FIGURE 5

Impact on Data Log Volume

(Number of data logs)



n = 8; Source: IDC's Business Value In-Depth Interviews, October 2023

More Efficient Security Operations Center Activities

Study participants linked significant efficiencies for their security operations teams, especially in the areas of security analysis and engineering, to their use of Google Security Operations.

Study participants cited the ease of using Google Security Operations, including user-friendly search capabilities and interface, as well as strong functionality in terms of delivering useful insights that help with prioritization and taking actions on potential security threats:

Efficiencies in running and scaling:

"We spend less time using and supporting Google Security Operations than our previous solution … With the old system, it was practically impossible to ingest this much data because it had a lot of limits, especially in terms of scalability. If we had tried to scale it, it likely would have collapsed."

— CIO, North America, software, annual revenue of $500 million to $1 billion.

Refocus on activities that create value:

"We've reorganized our security team with Google Security Operations. We used to have lots of people feeding and watering the SIEM platform, but all of that's pretty much done for us as part of what we get out of the box. So we have more people who are trying to work out how to get more business value out of our security platforms."

— CISO, EMEA, insurance, annual revenue of $1 billion to $5 billion.

Enhanced security team performance:

"We've got some pace of response numbers around the time from detection of the intelligence to response team, and they are well ahead with Google Security Operations of where we were and what others in the industry are capable of because we've moved it away from being human processes to being machine speed processes."

— CISO, EMEA, insurance, annual revenue of $1 billion to $5 billion.

As shown in **Table 4** (next page), interviewed Google Security Operations customers attributed substantial efficiencies for the security operations teams to use. On average, they reported a 45% efficiency for security analysis teams and 39% for security engineering teams, with an average efficiency across their impacted security operations teams of 42%. In total, this results in interviewed organizations having the time and focus of almost 15 more staff members to drive better security outcomes.

"We spend less time using and supporting Google Security Operations than our previous solution … With the old system, it was practically impossible to ingest this much data because it had a lot of limits, especially in terms of scalability. If we had tried to scale it, it likely would have collapsed."

CIO
North America software company, annual revenue of $500 million to $1 billion

TABLE 4

Impact on Security Team Efficiency

	Before/ without Google Security Operations	With Google Security Operations	Difference	Benefit
Security analysis teams				
Equivalent FTEs required for equivalent workloads (FTEs per organizations)	15.5	8.5	7.0	45%
Staff hours per 1,000 endpoints	707	388	319	45%
Security engineering teams				
Equivalent productivity level (FTEs per organizations)	6.8	4.1	2.7	39%
Staff hours per 1,000 endpoints	310	189	121	39%
Overall impact on security operations teams				
Equivalent FTEs required for same workloads*	34.4	19.9	14.5	42%
Staff hours per 1,000 endpoints per year	1,577	910	667	42%
Equivalent value of staff time requirements	$3.44M	$1.99M	$1.45M	42%

* Overall impact on security operations teams includes both security analyst and security engineering teams as well as other security operations center team members who work with Google Security Operations.

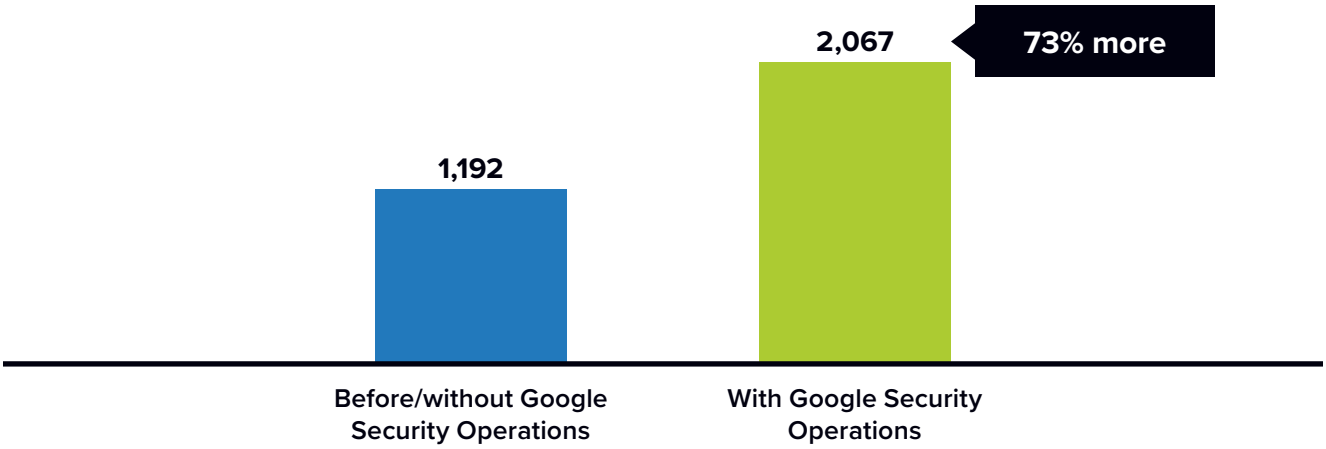
n = 8; Source: IDC's Business Value In-Depth Interviews, October 2023

These security team efficiencies translate to important gains in capacity, as shown in **Figure 6** (next page), with each security team member using Google Security Operations able to support 73% more endpoint devices.

FIGURE 6

Impact on Security Operations Team Capacity

(Number of endpoints per security operations team member)



n = 8; Source: IDC's Business Value In-Depth Interviews, October 2023

Business Benefits

Ultimately, improved security capabilities and security team efficiencies achieved through the use of Google Security Operations translate to better business results for study participants.

Interviewed Google Security Operations customers noted several common ways in which Google Security Operations has directly helped their business results, including improving customer perceptions of their security capabilities and increasing staff time available to focus on innovation and delivering customer-facing solutions and services:

Ability to implement business-impacting security capabilities:

"Google Security Operations has enabled us to do a number of things for the business through new detection capabilities, which protect us from business-facing fraud such as people pretending to be insurance companies … We could never have gotten to this before because we didn't have the data capability."

— CISO, EMEA, insurance, annual revenue of $1 billion to $5 billion.

Positive business impact of customer perception of strong security:

"If we cannot protect our customers' data, no one's going to want to do business with us. If we have high standards, other people can see that. A lot of [our competitors] have been hit by cyberattacks, and customers are looking now for companies that are more secure."

— CISO, EMEA, automotive, annual revenue of $5 billion to $10 billion.

Business benefits from innovation driven by strong security and performance:
"Google Security Operations has improved our business by driving innovation … We're able to innovate more because there are fewer issues, and we see higher performance."
— CIO, North America, software, annual revenue of $500 million to $1 billion.

Link between security posture and business outcomes:
"There's a reputational, performance, and time-to-market benefit of using Google Security Operations, so we spend less time creating new solutions and dealing with issues so that we spend more time on new products."
— VP, North America, banking, annual revenue of $25 billion to $50 billion.

Table 5 shows the business impact that study participants reported related to their use of Google Security Operations. On average, study participants cited revenue gains of $13.50 million per year per organization from gaining access to new customers and capturing incremental revenue gains from existing customers.

There's a reputational, performance, and time-to-market benefit of using Google Security Operations, so we spend less time creating new solutions and dealing with issues so that we spend more time on new products."

VP
North America banking company, annual revenue of $25 billion to $50 billion

TABLE 5

Business Productivity Benefits, Higher Revenue

Revenue Impact	Per Organization	Per 1,000 Endpoints
Higher revenue per year	$13.50M	$328,900
Assumed operating margin	15%	15%
Higher net revenue per year	$2.03M	$49,300

n = 8; Source: IDC's Business Value In-Depth Interviews, October 2023

ROI Analysis

Table 6 (next page) provides IDC's analysis of the benefits and investment costs related to study participants' use of Google Security Operations. IDC puts the total average discounted benefits achieved per organization over three years at $10.11 million ($246,400 per 1,000 endpoints), which compares with total discounted investment costs of $2 million per organization ($48,600 per 1,000 endpoints). These average benefits and investment costs would result in a three-year net present value of $8.11 million per organization ($197,800 per 1,000 endpoints) and an average three-year ROI of 407%, with organizations breaking even on their investment in an average of seven months.

TABLE 6

Three-Year ROI Analysis

	Per Organization	Per 1,000 Endpoints
Benefit (discounted)	$10.11M	$246,400
Investment (discounted)	$2.00M	$48,600
Net present value (NPV)	$8.11M	$197,800
ROI (NPV/investment)	407%	407%
Payback	7 months	7 months
Discount factor	12%	12%

n = 8; Source: IDC's Business Value In-Depth Interviews, October 2023

Challenges/Opportunities

The SIEM is core to modern security operations, enabling security teams to bring together data from all their respective security tools so that it can be correlated and analyzed in its entirety. As threat actors speed up their operations by outsourcing malware development and vulnerability discovery, defenders need to take advantage of every tool and bit of data that can help detect, investigate, and respond to cyberattacks.

To drive cybersecurity outcomes, executives should consider the following challenges as they plan to deploy a SIEM:

- What data to ingest is often a difficult but necessary decision due to the limits of the SIEM infrastructure or the cost to ingest all security data.
- As threat actors evolve, the SIEM needs to be updated with new detection rules to identify new types of attacks. Machine learning–based UEBA helps find anomalous patterns that signify previously unknown methods of attack.
- There are not enough skilled cybersecurity analysts to fill all the available positions; therefore, automation is necessary to handle all the work.

- Investigating each alert separately and then checking the available threat intelligence instead of looking at related contextualized alerts presented in their entirety slows analysts down.
- Waiting for queries to run during threat investigations or hunts translates to higher mean times to detect and respond.
- Analyst efficiency and best practice usage increases when remediation guidance is presented alongside the case.

Conclusion

Google Security Operations provides customers with the ability to ingest more of their desired data without an equal increase in cost, which allows them a greater ability to detect and respond to security threats. In turn, this reduces the probability of the occurrence of major security events.

Correlating threat intelligence and alerts helps security analysts operate more efficiently because the burden of doing the correlation themselves is removed. The ease and speed of searching through the large amounts of security data boosts the efficiency of security analysts, enabling them to handle more investigations. Customers are able to use threat intelligence and historical data to determine the best course of action when threats are identified.

Better security outcomes translate to business benefits, including a reputation for securing data, greater fraud protection, and the ability to spend time on developing new products. Customers report realizing an additional $13.5 million in revenue per year with Google Security Operations.

Taken together, these findings demonstrate the value proposition that interviewed Google Security Operations customers have achieved in terms of both cost savings and improved security and business outcomes. As a result, they are achieving significantly more in direct benefits from use than their investment costs, which IDC calculates will result in an average ROI of 407% over three years of using Google Security Operations.

Appendix 1: Methodology

IDC's standard Business Value methodology was utilized for this white paper. This methodology is based on gathering data from organizations that are currently using Google Security Operations as the foundation for the model. Based on interviews with these study participants, IDC has calculated the benefits and costs to these organizations related to their use of Google Security Operations. IDC conducted its quantitative analysis for this study by gathering benefit information during the interviews using a before-and-after assessment of the impact of using Google Security Operations. In this study, the benefits included reduced security solution costs, IT team efficiencies, reduced risk-related costs, and higher net revenue.

IDC Business Value assumptions are summarized below:

- Time values are multiplied by burdened salary (salary + 28% for benefits and overhead) to quantify efficiency and manager productivity savings. For the purpose of this analysis, based on the geographic locations of the interviewed organizations, IDC has used assumptions of an average fully loaded salary of $100,000 per year for IT staff members and an average fully loaded salary of $70,000 per year for non-IT staff members. IDC assumes that employees work 1,880 hours per year (47 weeks x 40 hours).
- Downtime values are a product of the number of hours of downtime multiplied by the number of users affected.
- The impact of unplanned downtime is quantified in terms of impaired end-user productivity and lost revenue.
- Lost productivity is a product of downtime multiplied by burdened salary.

Note: All numbers in this document may not be exact due to rounding.

Summary of Financial Benefits

Table 7 provides a summary of the financial benefits that interviewed customers attributed to their use of Google Security Operations, with average annual benefits coming to $4.28 million per organization in reduced security solution costs, security operations team efficiencies, reduced costs related to security events and fines, and increased net revenue.

TABLE 7

Summary of Financial Benefits

Category of Value	Average Quantitative Benefit	Calculated Average Annual Value
Cost of previous solution	Retiring/no longer using solutions costing $556,200 per year	$480,800
IT security operations center team efficiencies	Overall efficiencies of 42% worth 14.6 FTEs (salary of $100,000/year)	$1.26M
Reduced cost from major security events	Reduced likelihood of 60%, avoiding direct costs of $470,800 per year (lost revenue, remediation costs)	$406,900
Reduced cost from security-related fines/penalties	Avoiding direct costs of penalties/ fines of $450,000 per year	$389,000
Increased net revenue	Higher revenue of $13.5 million per year (15% margin)	$1.75M
Total average annual benefits	**$4.28M per organization**	

Note: Calculated average annual value includes 4.9 months deployment time in year 1.

n = 8; Source: IDC's Business Value In-Depth Interviews, October 2023

Appendix 2: Supplemental Data

This appendix provides an accessible version of the data for the complex figures in this document. Click "Return to original figure" below each table to get back to the original data figure.

FIGURE 1 SUPPLEMENTAL DATA

Average Annual Benefits per Organization

	$ per year per organization
Business productivity benefits	$1.75M
IT staff productivity benefits	$1.26M
Risk mitigation: user productivity benefits	$796,000
IT infrastructure cost reductions	$480,800
Total	**$4.29M**

n = 8; Source: IDC's Business Value In-Depth Interviews, October 2023

Return to original figure

FIGURE 3 SUPPLEMENTAL DATA

Impact on Threat Response Capabilities

	Before/without Google Security Operations	With Google Security Operations	Difference
Average time to identify potential threat (hours)	1.8	0.8	55% faster
Average time to address/remediate potential threat (hours)	3.2	1.5	51% faster

n = 8; Source: IDC's Business Value In-Depth Interviews, October 2023

Return to original figure

About the IDC Analysts

Michelle Abraham
Research Director, Security and Trust, IDC

Michelle Abraham is the research director in IDC's Security and Trust Group responsible for the Security Information and Event Management (SIEM) & Vulnerability Management practice. Michelle's core research coverage includes SIEM platforms, attack surface management, breach and attack simulation, cybersecurity asset management, and device and application vulnerability management alongside related topics.

More about Michelle Abraham

Matthew Marden
Research Vice President, Business Value Strategy Practice, IDC

Matthew is responsible for carrying out custom business value research engagements and consulting projects for clients in a number of technology areas with a focus on determining the return on investment (ROI) of their use of enterprise technologies. Matthew's research often analyzes how organizations are leveraging investment in digital technology solutions and initiatives to create value through efficiencies and business enablement.

More about Matthew Marden

Message from the Sponsor

Google Cloud

A modern, AI-powered security operations platform.

Google Security Operations is a modern, 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 Research, Inc.
140 Kendrick Street, Building B, Needham, MA 02494, USA
T +1 508 872 8200

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.