January 2026
Business Value White Paper
Sponsored by Google

The Business Value of Google Threat Intelligence

Christopher Kissel
Research Vice President,
Security and Trust Products, IDC

Monika Soltysik
Senior Research Analyst,
Security and Trust Products, IDC

Ladislav Kinda
Consultant,
Business Value Strategy Practice, IDC

Table of Contents

Click any title to navigate directly to that page.

Business Value Highlights

Click to jump to related content. Click "Return to Highlights" to get back to this page.

$7.5 million annual average benefit per organization

46% more efficient cyberthreat intelligence (CTI) teams

400% three-year return on investment

6-month payback on investment

36% more efficient SOC teams

139% more threats identified proactively

68% reduction in threat dwell time

47% faster to perform forensic analysis

34% overall reduction in organizational security risk

$2.9 million in annual costs associated with security incidents avoided

87% reduction in annual downtime hours caused by security incidents

77% faster mean time to detect

66% more satisfied process users due to functionality

Executive Summary

Google Threat Intelligence delivers measurable business value by combining Mandiant's frontline expertise, the global reach of the VirusTotal community, Google threat insights, and AI-driven analytics.

Google customers report that Google Threat Intelligence has enabled significantly faster threat detection and response, improved security team efficiency, and enhanced risk mitigation through AI-powered context and automation. Based on these interviews, IDC found that organizations experienced measurable operational gains — including substantial reductions in mean time to detect (MTTD) and mean time to respond (MTTR), fewer false positives, and higher analyst productivity — all of which contribute to greater organizational resilience and confidence in security operations.

These operational improvements translate into significant business outcomes, such as shorter disruption periods, lower incident-related costs, and improved executive confidence in security posture and decision-making. IDC projects that organizations leveraging Google Threat Intelligence can realize strong ROI within a short payback period, underscoring the tangible business value of an intelligence-led, AI-augmented approach to modern security operations.

IDC conducted research that explored the value and benefits for organizations using Google Threat Intelligence to improve overall organizational cybersecurity, threat detection, threat intelligence, and system stability and reliability by:

- Providing robust improvements in the productivity of security teams with streamlined workflows and reduced manual effort across security operations centers (SOCs), CTI, and incident response functions
- Enabling faster detection and response to threats, thereby helping teams to respond to threats quickly and decisively
- Providing the intelligence to be more proactive; helping build the security strategy based on threat actor targeting, TTPs, and active campaigns; and identifying threats proactively, often before they reach internal systems
- Helping to reduce the downtime that security incidents cause, thereby serving to minimize disruption and preserve and optimize overall business unit productivity
- Supporting better strategic security decision-making by providing clear, actionable insights to enhance executive-level visibility and confidence with respect to overall cybersecurity postures

Situation Overview

Organizations now face a dual challenge: managing an expanding attack surface while contending with a shortage of skilled security personnel capable of synthesizing the vast volumes of data that modern hybrid IT environments generate. Adversaries leveraging automation, AI, and advanced evasion techniques are increasingly exploiting this operational gap to overwhelm traditional defenses and accelerate the pace of attacks. In response, SOCs are shifting toward intelligence-led and increasingly automated operations — powered by contextual threat intelligence and generative AI. The ability to understand, prioritize, and act on relevant threats in real time is now a critical differentiator for organizations seeking to minimize cyber-risk and operational disruption.

IDC's research indicates that integrating high-fidelity threat intelligence with automated detection and response significantly improves security posture. However, achieving this integration has traditionally been fragmented across multiple tools and data sources. Google Threat Intelligence exemplifies this market transition by unifying global-scale telemetry, advanced analytics, and expert-driven intelligence under one AI-enhanced framework. This approach enables organizations to move from reactive threat management to proactive, intelligence-led defense.

Google Threat Intelligence Overview

Google Threat Intelligence unifies Mandiant's frontline incident response expertise, VirusTotal's global malware and AI, and Google's visibility across the internet into a single, AI-enriched platform. By fusing these capabilities with Google's vast telemetry and analytics infrastructure, Google Threat Intelligence transforms the challenge of operationalizing threat intelligence into a proactive defense strategy. The result is an end-to-end intelligence ecosystem that empowers SOCs to detect, investigate, and respond to threats with greater speed, accuracy, and context.

The solution draws on a diverse set of intelligence sources that provides the breadth and depth necessary to understand and respond to modern threats.

These sources include:

- **Google threat insights** gathered by monitoring attacks and protecting over 4 billion devices and 1.5 billion mailboxes worldwide, providing visibility into global attack activity
- **Open source intelligence** covering malware trends, vulnerabilities, and emerging adversarial behaviors
- **Crowdsourced intelligence from VirusTotal,** offering real-time visibility into indicators of compromise and emerging attack campaigns
- **Frontline intelligence from Mandiant,** delivering context and attribution drawn from global incident response engagement
- **Human-curated intelligence** from Google Threat Intelligence Group and Mandiant, offering insight into adversary motivations, tactics, techniques, procedures, and likely targets
- **Gemini AI integration** that automates correlation, investigation, and summarization, reducing manual effort and enabling analyst augmentation

Together, these capabilities enable organizations to:

- Detect and prioritize real threats faster through contextual correlation
- Reduce investigation timelines and false positives using AI-powered triage
- Empower less experienced analysts with guided, AI-driven insights
- Strengthen analyst confidence when taking action on validated intelligence
- Seamlessly integrate AI and human expertise to improve overall security posture
- Enhance visibility and collaboration across hybrid and multicloud environments
- Refine telemetry for different departments to use effectively (for example, the CISO, the compliance department, and the line of business)

IDC's interviews with Google Threat Intelligence customers — including organizations in finance, manufacturing, and managed security services — demonstrate tangible improvements in detection accuracy, operational efficiency, and overall business resilience.

The Business Value of Google Threat Intelligence

Study Firmographics

The project included seven interviews with organizations that use Google Threat Intelligence and have experience with and/or knowledge about its benefits and costs. IDC conducted one of these interviews with a Google Threat Intelligence partner.

Table 1 (below) provides a firmographic overview of the organizations interviewed, spanning verticals such as healthcare, insurance, logistics, shipping, retail, and telecommunications. These organizations were located in the United States, Canada, and France. They vary in size, with employee counts ranging from 1,600 to 150,000 and annual revenues ranging from $15 million to $35 billion. On average, they employ 49,100 people, have 6,100 IT staff, run 140 business applications, and generate $12.3 billion in annual revenue. This diversity underscores the broad applicability of Google Threat Intelligence across sectors and organizational scales.

Table 1

Firmographics of Interviewed Organizations

Firmographics	Average	Median	Minimum	Maximum
Number of employees	49,100	40,000	1,600	150,000
Number of IT staff	6,100	2,000	40	32,500
Total number of business applications	140	145	25	250
Annual revenue	$12.3B	$3.0B	$15.0M	$35.0B
Countries	United States (5), Canada, France			
Industries	Healthcare (2), Insurance, Logistics, Shipping, Retail, Telecommunication			

n = 7; Source: IDC Business Value In-Depth Interviews, September 2025

Choice and Use of Google Threat Intelligence

The organizations that IDC interviewed described the expectations and desired outcomes in their selection of Google Threat Intelligence. These included up-leveling cybersecurity, threat detection, threat intelligence, and system stability and reliability. In general, organizations selected Google Threat Intelligence because it provided capabilities that they could not replicate internally. A major factor was that Google Threat Intelligence combined global adversary insights with curated indicators, enabling earlier detection of phishing, ransomware, and brand impersonation campaigns. Its integration with existing security tools enriched alerts with context, thereby reducing noise and improving prioritization. Features and services such as Digital Threat Monitoring and Attack Surface Management provided visibility into external risks, while Private Scanning accelerated initial incident response. These capabilities collectively shifted teams from reactive firefighting to proactive defense and strategic planning.

In its comments to IDC, a healthcare provider emphasized the board-driven push for stronger security and praised Google Threat Intelligence's incident response capabilities. A shipping company highlighted Google Threat Intelligence's superior threat insights compared to other vendors, which helped its SOC detect previously missed incidents. Another healthcare organization cited its longstanding relationship with Mandiant, noting the value of frontline intelligence and global threat visibility that Google Threat Intelligence offers — especially critical in healthcare environments:

Healthcare:

"This initial impulse came from our board, a push to improve our security posture and have clear plans in case of an incident. After evaluating options, we chose Google Threat Intelligence. In case of a breach, they're among the best. In healthcare, security is critical — it's worth the investment."

Shipping:

"We had a clear need for Google Threat Intelligence — our SOC was missing key incidents. We found most vendors offered similar intel. Google Threat Intelligence stood out by providing deeper, more enriched insights, which proved valuable and led to our decision."

Healthcare:

"A big part of this is our long-standing relationship with Mandiant. We've consistently seen value in its frontline insights from helping companies respond to breaches. Its global exposure and research give it a perspective we simply can't match internally. That broader threat intelligence is incredibly valuable, especially in healthcare."

Table 2 (below) outlines how interviewed organizations used Google Threat Intelligence across their respective environments. On average, the solution supported nearly 95 environments per organization, indicating broad deployment. These organizations operated an average of 3.3 datacenters and 143 sites or branches and protected approximately 79,800 user devices and 106,700 total endpoints. The data highlights the extensive scale and reach of Google Threat Intelligence within a variety of complex IT infrastructures.

Table 2
Google Threat Intelligence Usage

Google Threat Intelligence	Average	Median
Environments supported by Google Threat Intelligence	94.8	87.0
Number of datacenters	3.3	3.0
Number of sites/branches	143.2	130.0
Number of user devices protected	79,800	110,000
Number of total endpoints protected	106,700	62,500

n = 7; Source: IDC Business Value In-Depth Interviews, September 2025

Business Value and Quantified Benefits

IDC found that the interviewed organizations realized significant value with Google Threat Intelligence, allowing them to improve business results and maximize their ROI in the platform.

The companies interviewed reported substantial operational and strategic benefits after adoption. Across security operations, Google Threat Intelligence enabled significant efficiency gains — reducing false positives, streamlining threat investigation, and automating detection workflows. CTI teams saw a significant reduction in staffing needs for equivalent workloads, while SOC and incident response teams experienced major

productivity improvements. These gains translated into millions in annual cost savings, enhanced efficiency, and faster response times, with major reductions in MTTD and MTTR.

Interviewed organizations noted that the core value of Google Threat Intelligence lies in its ability to turn raw telemetry into actionable intelligence. By embedding curated detections and completed reports into Google Security Operations (SecOps) and other SIEM solutions, Google Threat Intelligence provided analysts with immediate context on threat actors, campaigns, and likely attack paths. This reduced investigative guesswork and shortened the time from detection to containment. Organizations reported that these capabilities not only improved operational efficiency but also enhanced confidence in decision-making because teams could act on validated intelligence rather than incomplete or ambiguous signals. Beyond these operational improvements, Google Threat Intelligence delivered strategic value by enhancing executive decision-making and reducing overall cybersecurity risk.

Interviewed organizations cited improved visibility into threats, better prioritization of alerts, and enriched intelligence that supported board-level reporting:

Retail:

"Google Threat Intelligence gives us early visibility into phishing, malware, and brand impersonation. Its AI-powered insights help protect over 200 consumer-facing applications by detecting malicious domains, fake apps, and phishing kits, delivering actionable intelligence that's critical for securing our digital presence."

Insurance:

"Google Threat Intelligence enables proactive threat detection and smarter alert triage by correlating activity across platforms. It reduces false positives and accelerates incident response. When our SOC spots suspicious behavior, Google Threat Intelligence links it to known threats, triggering immediate containment, minimizing risk, preventing lateral movement, and delivering measurable cost benefits."

Telecommunications:

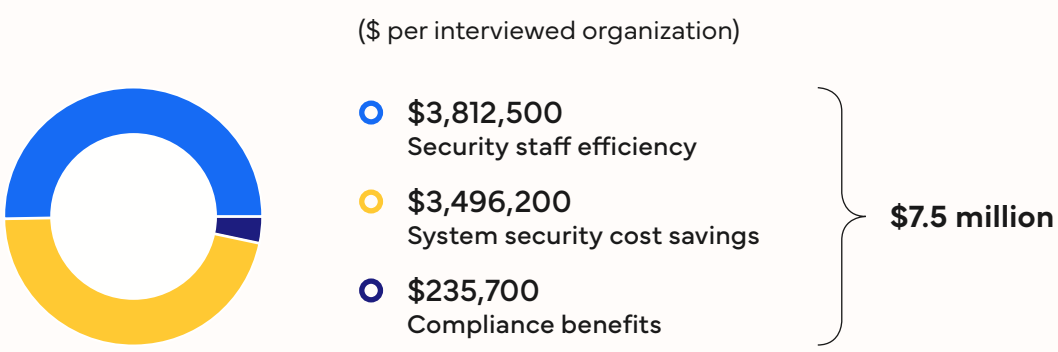
"We've used Google Threat Intelligence for attack path simulation, autonomous threat hunting, and gaining a clearer view of the threat landscape. It's quick to deploy, requires minimal intrusion, and works seamlessly across environments — including multicloud setups. Ease of deployment was a key advantage."

Figure 1 (below) presents IDC's calculations of cumulative customer benefits after the adoption of Google Threat Intelligence. As shown, IDC quantified the average annual benefits at $7.5 million per organization.

Figure 1

Average Annual Benefits Per Organization

See this figure data in an accessible table format.



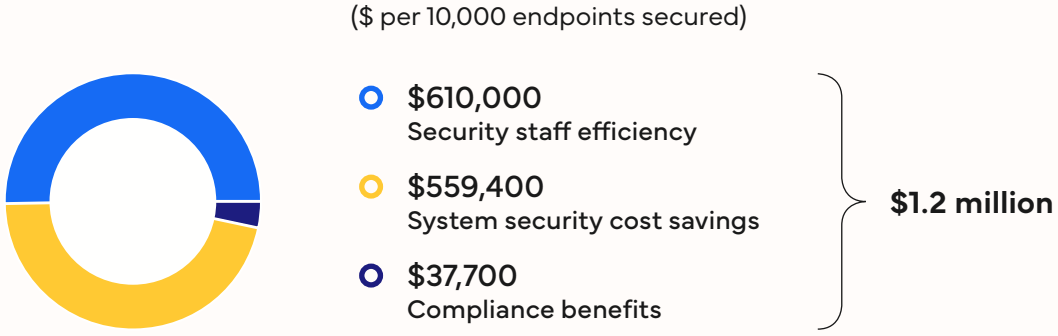
n = 7; Source: IDC Business Value In-Depth Interviews, September 2025

Figure 2 (below) presents a normalized breakout of these same Business Value calculations. As shown, IDC calculated benefits of $1.2 million per 10,000 endpoints secured.

Figure 2

Average Annual Benefits Per 10,000 Endpoints Secured

See this figure data in an accessible table format.



n = 7; Source: IDC Business Value In-Depth Interviews, September 2025

Security Team Efficiency Benefits

IDC used its Business Value methodology to evaluate a series of specific benefits for security team efficiency using Google Threat Intelligence. Data from the study participants showed that Google Threat Intelligence enhanced the efficiency and effectiveness of cybersecurity teams. SOCs, CTI teams, and incident response units all reported significant reductions in staffing needs — up to 46% in some cases — as a direct result of Google Threat Intelligence's automation, enriched threat indicators, and streamlined workflows. These improvements translated into significant efficiency gains, with SOC teams alone gaining approximately $2.84 million worth of efficient time per year.

Google Threat Intelligence's high-fidelity threat enrichment reduced false positives and rework, enabling faster and more accurate threat detection and response. The use of automation and curated intelligence significantly reduced manual effort across SOC and CTI teams. Specialized groups and use cases within the interviewed organizations' cybersecurity environments, such as IoT and maritime security, saw the largest gains because Google Threat Intelligence replaced time-consuming hunting with automated enrichment and prioritized alerts. Finished intelligence provided immediate context, so that analysts could act confidently without building hypotheses from scratch. This shift allowed teams to reallocate time to proactive defense and strategic projects, improving overall security posture without requiring additional staff or increasing operational costs.

IDC's evaluation for cybersecurity teams started with CTI teams. Organizations reported a 46% increase in CTI team efficiency, resulting in annual efficient staff time gains worth $914,400 **(Table 3, below)**. Driving these improvements were Google Threat Intelligence's global adversary profiles and campaign insights, which accelerated detection engineering and investigative tasks. By eliminating the need for manual research and enabling faster, more informed decision-making, Google Threat Intelligence significantly enhanced the efficiency of these teams.

Table 3

Cyber Threat Intelligence Team Efficiency

Team Efficiency	Before Google Threat Intelligence	With Google Threat Intelligence	Difference	Benefit
Total FTE count	19.9	10.7	9.2	46%

Table 3 continued next page

Table 3 continued

Team Efficiency	Before Google Threat Intelligence	With Google Threat Intelligence	Difference	Benefit
Value of staff time per year	$1,987,800	$1,073,400	$914,400	46%

n = 7; Source: IDC Business Value In-Depth Interviews, September 2025

SOC teams also reported substantial efficiency gains with Google Threat Intelligence. **Table 4 (below)** highlights the efficiency improvements achieved, with organizations reporting a 36% additional gain in overall staff efficiency. This translated into an annual efficient time gain of $2.84 million. They attributed these gains to Google Threat Intelligence's high-fidelity enrichment capabilities, which significantly reduced false positives and rework. As a result, SOC analysts were able to act more decisively on real threats, minimizing unnecessary escalations and improving their overall operational effectiveness.

Table 4

Security Operations Center Team Efficiency

Team Efficiency	Before Google Threat Intelligence	With Google Threat Intelligence	Difference	Benefit
Total FTE count	78.6	50.2	28.4	36.2%
Value of staff time per year	$7,862,200	$5,018,700	$2,843,500	36.2%

n = 7; Source: IDC Business Value In-Depth Interviews, September 2025

Table 5 (next page) details the efficiency improvements that incident response teams achieved, indicating a 23% increase in efficiency and an annual staff time benefit of $693,500. They attributed these gains to Google Threat Intelligence's private scanning capabilities and vector clues, which helped guide containment decisions from the outset of an incident.

Table 5

Incident Response Team Efficiency

Team Efficiency	Before Google Threat Intelligence	With Google Threat Intelligence	Difference	Benefit
Total FTE count	29.2	22.3	6.9	23.7%
Value of staff time per year	$2,920,000	$2,226,500	$693,500	23.7%

n = 7; Source: IDC Business Value In-Depth Interviews, September 2025

Threat Management Process Benefits

IDC also researched threat management process benefits. Organizations using Google Threat Intelligence reported that the platform significantly streamlined these processes by providing enriched indicators and comprehensive visibility across endpoints, networks, and other elements. This allowed teams to reduce time spent on retroactive threat hunting and begin investigations with a clearer understanding of their objective. Google Threat Intelligence's integration of expert-driven intelligence and automated workflows helped minimize manual effort, enabling faster and more confident incident response. The consolidation of threat data into a single pane of glass also improved situational awareness and reduced the number of incidents requiring extensive investigation. Additionally, Google Threat Intelligence's built-in threat intelligence analysis reduced the need for separate threat feeds and dedicated analysts to evaluate external data, saving time and resources.

Organizations across healthcare, telecommunications, and insurance verticals emphasized how Google Threat Intelligence's proactive controls and enriched advisories improved their ability to detect, analyze, and respond to threats, as these comments show:

Healthcare:

"Having those indicators significantly reduces the time we spend on retroactive threat hunting. Once an incident occurs, Google Threat Intelligence gives us a clear, comprehensive view of what to look for across endpoints, networks, and other vectors. It provides a strong starting point and a sense of completeness, giving us confidence that our coverage is as thorough as possible."

Telecommunications:
"Google Threat Intelligence enabled more proactive controls and reduced the number of incidents we need to handle. When a security event does occur, Google Threat Intelligence helps us quickly investigate by pulling logs from all devices and endpoints into a single pane of glass. That visibility streamlines response and minimizes manual effort."

Insurance:
"Google Threat Intelligence is enriched by expert-driven data. Analysts feed insights directly into the platform, improving the quality of threat advisories across our campaigns. From incident response to program transformation, it adds depth and value to our overall threat intelligence effort."

Healthcare:
"There are two key benefits. First, we don't need to purchase and manage separate threat feeds or dedicate analysts to evaluate them — Google Threat Intelligence is already integrated and delivers actionable results. Second, its built-in workflows reduce manual effort, saving time and streamlining threat analysis across endpoints and devices."

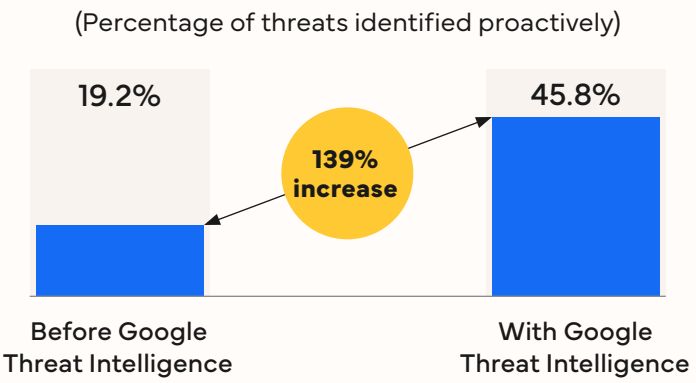
Interviewed companies emphasized Google Threat Intelligence's ability to accelerate threat prioritization and containment. They reported that the platform enabled earlier isolation and more targeted analysis, significantly reducing the timeline and impact of security incidents. **Specifically, Google Threat Intelligence helped teams contain incidents 43% faster and perform forensic analysis 47% faster, minimizing downtime and exposure to fraud.**

As one retail organization noted:
Ultimately, faster correction leads to earlier containment, which means a smaller blast radius. That directly reduces damage, lowers incident severity, cuts downtime, and limits fraud exposure. Quick threat identification and response are key to minimizing the impact of each incident.

Interviewed companies told IDC that Google Threat Intelligence had a positive impact on proactive threat identification, with a 139% increase in the proactive identification of threats after deployment **(Figure 3, next page)**. This improvement stemmed from the platform's ability to leverage external intelligence to detect and prevent incidents before they infiltrate internal environments. By identifying threats earlier in the attack life cycle, companies significantly reduced downstream workload and improved their overall security posture.

Figure 3

Proactive Threat Identification Benefit

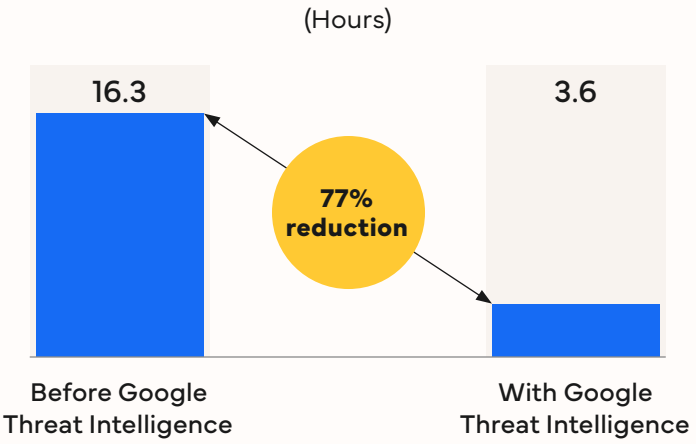


n = 7; Source: IDC Business Value In-Depth Interviews, September 2025

Figure 4 (below) highlights the impact of Google Threat Intelligence adoption on MTTD windows. Google Threat Intelligence helped organizations reduce their MTTD window by 77%, decreasing the average detection time from 16.25 hours to just 3.61 hours. They attributed this improvement to Google Threat Intelligence's built-in threat detection capabilities, which streamlined investigation processes, ultimately helping security teams to focus on the most critical alerts.

Figure 4

Mean-Time-to-Detect Benefit

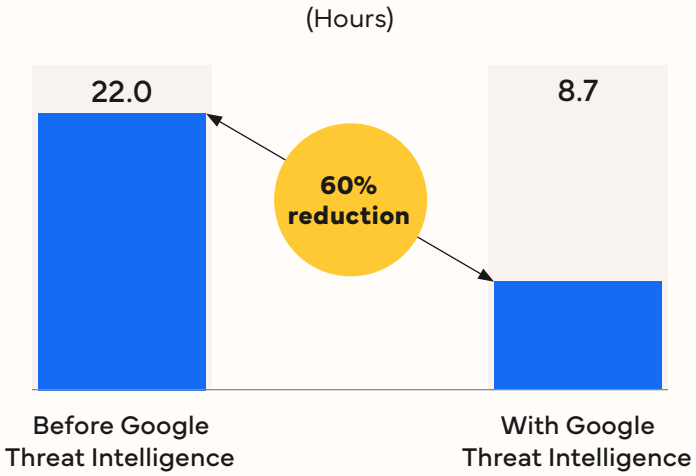


n = 7; Source: IDC Business Value In-Depth Interviews, September 2025

Similarly, MTTR metrics also improved after the adoption of Google Threat Intelligence, leading to a 60% reduction and a decrease in average recovery time from 22 hours to 8.7 hours **(Figure 5, below)**. Organizations attributed this substantial improvement to intelligence-driven playbooks, which guided teams through evidence collection and recovery steps with greater precision and speed. By streamlining the recovery process, organizations were able to restore systems more efficiently, minimize business disruption, and reduce the operational and financial impact of security incidents.

Figure 5

Mean-Time-to-Detect Benefit



n = 7; Source: IDC Business Value In-Depth Interviews, September 2025

Table 6 (next page) presents the measurable impact of Google Threat Intelligence on reducing downtime. It helped reduce the number of monthly downtime incidents by 60% and cut the average time needed to resolve each incident by around 66%. This led to a significant 86% reduction in annual downtime hours. Financially, these improvements equated to an annual cost saving of $19.3 million, or $2.9 million when adjusted for a 15% operational margin.

Table 6

Security Incident–Caused Downtime Reduction

Downtime	Before Google Threat Intelligence	With Google Threat Intelligence	Difference	Benefit
Number of downtime incidents per month	0.21	0.08	0.13	60.0%
Time to resolve per incident	18 hours	6 hours	12 hours	66.7%
Hours of downtime annually	45	6	39	86.7%
Annual cost of downtime	$22,297,500	$2,973,000	$19,324,500	86.7%
With 15% operational margin assumption	$3,344,600	$445,900	$2,898,700	86.7%

n = 7; Source: IDC Business Value In-Depth Interviews, September 2025

Compliance teams also saw robust improvements, including a 23% gain in compliance staff efficiency. This translated into an annual efficient time gain worth $125,200 annually **(Table 7, below)**. Driving these improvements was Google Threat Intelligence's delivery of finished intelligence and the benefit of clearer key performance indicators, which streamlined audit preparation and leadership reporting processes, ultimately reducing rework cycles and enhancing overall compliance readiness.

Table 7

Compliance Staff Efficiency

Efficiency	Before Google Threat Intelligence	With Google Threat Intelligence	Difference	Benefit
Total FTE count	7.7	5.9	1.8	23.3%
Value of staff time per year	$536,600	$411,400	$125,200	23.3%

n = 7; Source: IDC Business Value In-Depth Interviews, September 2025

Study participants reported that greater compliance staff efficiency, in turn, led to an annual reduction of $150,000 in fines and penalties associated with compliance violations. By improving visibility and preparedness, Google Threat Intelligence helped organizations avoid missteps during incidents, thereby minimizing the risk of being blindsided by regulatory penalties and reinforcing a more robust corporate compliance posture **(Table 8, below)**.

Table 8

Compliance-Related Costs Reduction

Annual Compliance Costs Reduction	
Reduction of compliance-related fines and penalties	$150,000

n = 7; Source: IDC Business Value In-Depth Interviews, September 2025

The Strategic Impact of Google Threat Intelligence

Google Threat Intelligence helped executives make informed decisions by translating complex cybersecurity data into clear, actionable insights. It improved reporting clarity, streamlined data analysis, and increased confidence in strategic choices.

Leadership gained better visibility into risk posture, enabling more effective oversight and proactive responses to emerging threats:

Healthcare:

"When cyberthreats make headlines, our executives need a clear, digestible context. The finished intelligence from Google Threat Intelligence helps translate complex security topics into briefings they can act on, making it a valuable tool for executive-level awareness and decision-making."

Telecommunications:

"While the board isn't concerned with the specific tools we use, Google Threat Intelligence supports our ability to clearly report on our security posture. It helps us communicate whether we're operating within acceptable risk levels, which is essential for executive oversight and strategic decision-making."

Logistics:

"Google Threat Intelligence supports our executive reporting by streamlining data collection, analysis, and interpretation. Its platform integrates various data sources — including video and endpoint logs — and applies analytics to deliver clear, actionable insights. This helps us present complex security information in a way that's comprehensive and digestible for leadership."

Retail:

"We've seen a measurable improvement in strategic decision-making; our confidence level has increased from around 70%–75% to closer to 90%. That 10%–15% gain reflects stronger visibility and more proactive insights. It's also evident in the positive feedback we're getting from the C-suite, who now have more clarity and confidence in our security posture."

IDC's analysis shows that Google Threat Intelligence contributed to a 33% reduction in overall cybersecurity risk and a 34% increase in confidence when making strategic cybersecurity decisions. **Table 9 (below)** highlights the cost savings organizations achieved by consolidating their cybersecurity tools. On average, the seven interviewed organizations reported an annual reduction of $1.18 million in cybersecurity tool costs via native intelligence capabilities and integrated workflows. This allowed companies to eliminate redundant tools and reduce reliance on external solutions.

A logistics organization framed the benefit this way:

Previously, we relied on multiple applications to integrate our security tools. Now, with Google Threat Intelligence, everything runs on a single AI-powered platform. This has significantly improved efficiency and productivity and reduced costs.

Table 9

Previous Solutions Cost Reduction/Consolidation

Annual Previous Solutions Cost Reduction	
Cybersecurity tools cost reduction	$1,183,300

n = 7; Source: IDC Business Value In-Depth Interviews, September 2025

IDC then examined the role of AI — specifically Google Gemini — in enhancing threat investigation and response. On average, 34% of threat investigations incorporated Google Gemini, which provided AI-powered summarization and querying capabilities. These features accelerated the analysis of complex cases, allowing teams to process large data sets more efficiently while still applying human oversight for accuracy and governance.

A retail organization noted that:
AI plays a major role; it helps flag threats quickly and analyze large data sets efficiently. Adversary profiles, domain and brand monitoring, the dark web, and breach intelligence are all key features. We get alerts on leaked credentials tied to employees or partners across dozens of applications and thousands of users. Machine learning helps correlate our assets with threat vectors, making the intelligence highly actionable.

Partner Benefits

The one Google partner that IDC interviewed for this project shared its journey of adopting Google Threat Intelligence, highlighting how it enhanced its SOC capabilities, enriched threat detection, and improved incident response.

The partner's experience reflects the value of integrated intelligence in delivering faster, more informed decisions and stronger security outcomes for its customers:

Background information:
"We have been a Google SecOps partner for nearly two years now. The first decision to further develop our SOC as a service for our partners, we moved to the cloud, to Google SecOps, and Google Threat Intel."

Initial adoption:
"When we were getting more mature with the service, we thought about enrichment and the integration of threat intelligence. VirusTotal is one of the biggest players in this field, and it's part of the Google company right now. It was a given way to look at Google Threat Intelligence and to use it in our services for enrichment for our customers."

Use cases for customers:
"We're using this for enrichment to make our detection more efficient, give our customers more insights, and give our analysts more insight to decide faster or a better base to assess whether something is really a true positive or a false positive."

Security impact for customers:

"We also use Google Threat Intelligence in IR cases where it gives us insights about the environment of the customer seen from the outside. That way we can identify faster whether there are big gaps in the security posture or whether there is already leaked data, credentials, and stuff like this."

Mandiant Impact

In addition, Google Threat Intelligence is complemented by the capabilities offered by Mandiant threat intelligence services. The use of Gemini AI further strengthens Google Threat Intelligence capabilities, enabling proactive threat identification and reducing downtime incidents. Customers emphasized Mandiant's global threat visibility and frontline research as key differentiators, providing early warnings of advanced persistent threats and adversary tactics. The operationalized intelligence and playbooks delivered by Mandiant Intelligence experts helped organizations respond to incidents more quickly and effectively, reducing containment and investigation times.

These Mandiant threat intelligence services also improved overall risk posture and executive confidence, with customers noting that Mandiant's customized insight enhanced board-level reporting and strategic decision-making. Mandiant customers also noted that:

One key advantage was the strategic, operational, and technical intelligence expertise Mandiant consultants and intelligence analysts contributed.

Mandiant services support real-time detection, threat hunting, and incident response workflows. Beyond that Mandiant expertise strengthened the end-to-end security life cycle readiness by helping define policies and processes, acting as a force multiplier for existing Google Threat Intelligence capabilities.

An unexpected benefit [of Mandiant Threat Intelligence services] was the depth of insight gained through integration with the Mandiant platform. We hadn't anticipated how much detailed external threat intelligence it would provide. It revealed risks we weren't previously aware of, enhancing our overall security posture and delivering efficiency gains we hadn't initially planned for.

Mandiant brings unmatched credibility and APT research. Its intelligence helps us understand who is targeting our brands and why.

Mandiant threat intelligence services with Google Threat Intelligence and our internal threat data gave us a complete picture — fewer surprises, faster response, and better board reporting.

ROI Summary

Summing up the financial and business-related benefits presented for the study participants' use of Google Threat Intelligence, IDC calculated an average three-year ROI. As shown in **Table 10 (below),** IDC projects that these organizations will achieve three-year discounted benefits worth an average of $17,770,600 per organization, with improved security staff efficiency, reduced downtime, and enhanced threat detection and response capabilities as drivers. These benefits compare with the total three-year discounted costs of $3,554,200 per organization. IDC projects this level of benefit and investment to result in an average three-year ROI of 400%, with a payback period of just six months.

Table 10

Three-Year ROI Analysis

Three-Year ROI Analysis	Per Organization	Per 10,000 Protected Endpoints
Discounted benefits	$17,770,600	$2,843,300
Discounted investment	$3,554,200	$568,700
Net present value (NPV)	$14,216,400	$2,274,600
ROI	**400%**	**400%**
Payback	**6 months**	**6 months**
Discount factor	12%	12%

n = 7; Source: IDC Business Value In-Depth Interviews, September 2025

Challenges/Opportunities

Google Threat Intelligence presents several key opportunities for organizations seeking to modernize their security operations and leverage AI at scale. By combining Mandiant's frontline intelligence, VirusTotal's extensive malware library, and threat insights from Google's global visibility, Google Threat Intelligence delivers broad and deep visibility into the threat landscape. Through native integration with Google SecOps and robust APIs

and off-the-shelf integrations with hundreds of security vendors, operationalization can be streamlined, creating a unified foundation for intelligence-led automation. The platform's integration with Gemini AI enhances the efficiency of SOCs by accelerating investigation workflows, reducing alert fatigue, and enabling contextual correlation across hybrid environments. IDC sees a strong opportunity for organizations to use Google Threat Intelligence as a central intelligence hub, improving visibility, consistency, and collaboration across threat detection, investigation, and response functions. Customers surveyed have demonstrated meaningful efficiency gains, including measurable reductions in MTTD and MTTR and improved analyst confidence through guided, AI-driven workflows.

However, as organizations scale AI-driven operations, they must address several challenges to fully realize the value of Google Threat Intelligence.

- **Integration and data strategy:**
  Enterprises with fragmented tool ecosystems may face complexity in unifying threat data across multiple telemetry sources. While Google Threat Intelligence's native integration with Google SecOps mitigates much of this friction, IDC recommends establishing standardized data models and governance frameworks early in the deployment process.
- **AI readiness and privacy considerations:**
  Gemini AI brings automation and contextual analysis, but organizations must ensure alignment with AI governance and regional compliance frameworks (such as GDPR in EMEA). Early adopters noted that localized data residency requirements can limit access to certain AI-driven features, requiring adaptive deployment planning.
- **Operational maturity and skills evolution:**
  SOCs transitioning from manual or semi-automated workflows may need to upskill staff in AI-driven investigation techniques and contextual intelligence interpretation. However, Google Threat Intelligence's guided interface and AI-assisted triage reduce this barrier, enabling faster adoption.

IDC expects continued growth in the adoption of AI-powered threat intelligence platforms as security operations evolve toward automation and intelligence-led decision-making. Google's ability to fuse global telemetry, contextual analytics, and generative AI positions it strongly to capitalize on this market opportunity and advance industry benchmarks for security efficiency and visibility.

Conclusion

The performance metrics that Google Threat Intelligence achieved are impressive: a 400% ROI, 139% more threats identified proactively, and a 68% reduction in dwell time, among many others. On the face of it, the combination of threat intelligence from VirusTotal, Mandiant, and Google, together with Gemini AI, helps to provide the proper context for threat detection and response, security posture hardening, and even proactive threat mitigation tactics.

To improve MTTD and MTTR, companies have to find efficiencies anywhere and everywhere. The strength of Google Threat Intelligence is its provision of a centralized platform that unifies threat research, telemetry analytics, and AI-driven automation across the detection and response life cycle. IDC's analysis finds that organizations using Google Threat Intelligence achieve faster detection and response, greater SOC efficiency, and measurable risk reduction. These outcomes not only strengthen operational resilience but also deliver tangible business value by minimizing downtime, reducing incident-related costs, and improving executive confidence in overall security posture.

Appendix A: Methodology

IDC utilized its standard ROI methodology for this project. This methodology is based on gathering data from current users of Google Threat Intelligence as the foundation for the model.

Based on interviews with organizations using Google Threat Intelligence, IDC performed a three-step process to calculate the ROI and payback period:

1. **Gathered quantitative benefit information during the interviews using a before-and-after assessment of the impact of Google Threat Intelligence.** In this study, the benefits included IT cost reductions and avoidances, staff time savings and productivity benefits, and revenue gains.

2. **Created a complete investment (three-year total cost analysis) profile based on the interviews.** Investments go beyond the initial and annual costs of using Google Threat Intelligence and can include additional costs related to migrations, planning, consulting, and staff or user training.

3. **Calculated the ROI and payback period.** IDC conducted a depreciated cash flow analysis of the benefits and investments for the organizations' use of Google Threat Intelligence over a three-year period. ROI is the ratio of the NPV and the discounted investment. The payback period is the point at which cumulative benefits equal the initial investment.

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

- Time values multiplied by burdened salary (salary + 28% for benefits and overhead) quantify efficiency and productivity savings. For this analysis, IDC has used assumptions of an average fully loaded $100,000 per year salary for IT staff members and an average fully loaded salary of $70,000 for non-IT staff members. IDC assumes that employees work 1,880 hours per year (47 weeks x 40 hours).

- IDC calculates the net present value of the three-year savings by subtracting the amount that the organization would have realized by investing the original sum in an instrument yielding a 12% return to allow for the missed opportunity cost. This accounts for the assumed cost of money and the assumed rate of return.

- Further, because Google Threat Intelligence requires a deployment period, the full benefits of the solution are not available during deployment. To capture this reality, IDC pro rates the benefits on a monthly basis and then subtracts the deployment time from the first-year savings.

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

Appendix B: Accessible Data Tables

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

Figure 1 Accessible Data

Average Annual Benefits Per Organization

Average Annual Benefits	Per Organization
Security staff efficiency	$3,812,500
System security cost savings	$3,496,200
Compliance benefits	$235,700
Total	**$7.5 million**

n = 7; Source: IDC Business Value In-Depth Interviews, September 2025

Return to figure

Figure 2 Accessible Data

Average Annual Benefits Per 10,000 Endpoints Secured

Average Annual Benefits	Per Organization
Security staff efficiency	$610,000
System security cost savings	$559,400
Compliance benefits	$37,700
Total	**$1.2 million**

n = 7; Source: IDC Business Value In-Depth Interviews, September 2025

Return to figure

About the IDC Analysts

Christopher Kissel

Research Vice President, Security and Trust Products, IDC

Chris Kissel is a research vice president in IDC's Security and Trust Products group, responsible for cybersecurity technology analysis, emerging trends, and market share and forecast reporting. Kissel's primary research area is security operations and AI security analytics. The major technology groups within this practice are SOAR, firewall automation, network detection and response, threat detection and investigation response, threat intelligence, and cloud-native XDR. Kissel also contributes to the IDC SIEM and exposure management practices. The AI analytics service effectively covers the processes security operations analysts employ to monitor, detect, remediate, and mitigate threat actors attempting to attack a network and how AI algorithms can be used to enhance detection and response processes.

More about Christopher Kissel →

Monika Soltysik

Senior Research Analyst, Security and Trust Products, IDC

Monika Soltysik is a senior research analyst in IDC's Security Products group, responsible for managing security vendor revenue estimates, with a particular emphasis on the Security Analytics submarkets. She contributes to research on SOC analytics, automation, and cloud-native XDR, with a primary focus on threat intelligence.

More about Monika Soltysik →

About the IDC Analysts (continued)

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

Google Threat Intelligence combines Google's large-scale visibility, Mandiant's frontline incident response expertise, and VirusTotal's crowdsourced malware telemetry into a single solution. It is designed to provide security teams with comprehensive, contextualized information on threat actors, malware, and their tactics, techniques, and procedures (TTPs).

The platform uses AI to analyze and synthesize vast amounts of threat data, helping analysts to identify relevant threats, automate research tasks, and understand malicious code more quickly. Capabilities include deep and dark web monitoring, vulnerability intelligence, and threat profiles tailored to an organization's specific risks. This approach aims to equip security operations with the actionable intelligence needed to anticipate, hunt, and respond to threats.

For more information, visit https://cloud.google.com/security/products/threat-intelligence.

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.

idc.com @idc @idc

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.