The Business Value of Sumo Logic

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

Michelle Abraham
Research Director, Security and Trust, IDC

Stephen Elliot
Group Vice President, I&O, Cloud Operations, and DevOps, IDC

Table of Contents

CLICK ANY HEADING TO NAVIGATE DIRECTLY TO THAT PAGE.

Executive Summary

Organizations' adoption of SaaS services and expansive multicloud application architectures continues to expand as threat actors take advantage of the complexity to seek out weaknesses that allow them entry and access to critical assets. The security information and event management (SIEM) and observability landscapes are evolving as the desire to ingest and analyze increasing amounts of structured and unstructured data has become crucial.

The continued increase in the adoption of SaaS and modular application architectures is generating a massive number of signals that can help identify, resolve, and predict security and performance problems that impact the customer experience (CX). Often, developer, security, and operations teams require the same data (metrics, logs, traces, events) to identify security and performance problems. In addition, these teams can accelerate and improve collaboration, automate more processes, and identify and resolve problems faster using a single platform. Add the use of advanced AI technologies to the unified data lake, and the value substantially increases across people, process, technology, and business outcomes.

IT organizations are evaluating opportunities to compress security, problem, and incident management teams, processes, and capabilities through advanced, real-time data collection and analysis that can be shared in context across teams.

However, cultural and organizational silo challenges must often be overcome to drive such a transformation. One common example is the rise of observability and the need to get several teams and stakeholders involved in identifying and resolving performance problems. Technology staff from security, DevOps, site reliability engineering, platform engineering, operations, and development teams often play a part in problem and incident management processes. Each team uses different expertise and perspectives and requires data to be displayed and organized in a way that makes sense to them in their role. An increasingly common scenario is when a cyberattack causes performance problems that impact an application and customer experience.

Containing, resolving, and preventing these attacks in the future across these separate teams is an opportunity for observability and DevOps teams to better collaborate with their security peers.

Business Value Highlights

Click the highlights below to navigate to content within this document.

- **376%** three-year ROI
- **4 months** to payback
- **$3.22 million** total revenue gained annually
- **60%** faster time to respond to security threats
- **45%** reduction in average duration of breach impact
- **36%** improvement in MTTI
- **39%** faster time to respond to troubleshooting issues
- **82%** reduction in unplanned downtime
- **25%** improvement in time to market products
- **28%** more efficient compliance teams

To overcome these organizational and data-centric challenges, leadership teams are using platforms that collect, analyze, and resolve common security and operational tasks. They are also focusing on business value outcomes and metrics as the foundation for modern security and observability use cases. The need to predict and prevent problems has never been more paramount as customers quickly move on from poorly performing digital services. Improved team collaboration and communications is one example. In fact, some of the results from the tighter alignment between security and operations teams are impressive; 19% more efficient security teams, 60% faster time to respond to security threats, 17% more efficient troubleshooting teams, 39% faster time to respond to troubleshooting issues, 82% reduction in unplanned downtime, and 19% improved customer satisfaction are just a few of the key outcomes. For observability outcomes, the prevention and reduction of unplanned downtime issues are critical outcomes, with a 42% reduction in the average time to identify issues that required troubleshooting. The number of support calls were reduced by 18%, and teams were able to scale better as they became more productive because of a more proactive posture. IDC calculated that this translated into an annual productivity-based business value of $993,300 for each organization.

To assess real-world business value, IDC conducted research that explored the value and benefits for organizations using Sumo Logic solutions to help their organizations with IT security and troubleshooting operations. The project included interviews with eight companies that had experience with or knowledge about its benefits and costs.

Based on extensive quantitative and qualitative data derived from these interviews, IDC calculates that study participants will realize significant business value of $5.16 million per organization with a very substantial 376% three-year return on investment by:

- Providing quicker and more effective identification and response to security threats and incidents
- Improving the overall efficiency and effectiveness of security-related teams, including core security operations, troubleshooting, and compliance
- Addressing troubleshooting issues with greater speed and efficiency, thereby minimizing actual or potential threats
- Reducing the incidence of unplanned downtime to improve end-user productivity and business results
- Leveraging these capabilities to make a strong security team, contributing to better business results

Situation Overview

Security operations center (SOC) and IT operations teams are almost always separate, each having their own unique set of tools, data, and processes. However, SIEM platforms have evolved from their compliance beginnings to be the data aggregation tool in a security operations center. With an increasing number of security tools being used to protect the hybrid multicloud environment of many organizations today, the ability to bring in the data output of those tools and use it for correlation and investigation is paramount. Threats are never-ending, and the lack of data to detect and analyze hampers the security team in being able to act quickly. Cloud security threats are increasing in both frequency and intensity as modern applications (containers, Kubernetes, microservices, cloud service, SaaS, etc.) and infrastructures create more complexity and a larger threat footprint. Executives are quickly realizing they must obtain better visibility, analysis, and visualization across these environments in a proactive approach to protect against potential threats. The identification of a security threat is no longer good enough; analyzing a more complete set of data that includes metrics, data, traces, and logs collected from across security, applications, cloud, and infrastructure sources provides SOC, DevOps, developers, and IT operations executives with a powerful observability platform to take proactive action against potential future issues.

The monitoring and observability of data from the breadth of applications and systems (metrics, logs, data, traces, operational technology) are valuable for many different technology teams. What's needed is a platform that can collect and analyze the data; generate insights related to performance, pattern detection, and threat analysis; and predict future issues based on the environment's behavior, even warning of potential problems. The combination of automation, the collection of large volumes and varieties of data, and the use of AI technologies for analysis is empowering teams to move from monitoring to observability and from a reactive to proactive posture. For the first time, observability teams are empowered to work with the SOC and security analysts to better understand and assist with solving performance issues because the data is relevant for both disciplines and their respective use cases. In addition, the data enables each role to become more productive by accelerating a focus on the data that matters for specific problems and providing an understanding of the dependencies of the data that relate to each technology role. The ability to drill down into a problem has never been more important, as security and application services have become extremely complex. Breaking down technology silos and using common data to resolve issues is fast becoming a requirement for modern security and observability teams. The reality is that security issues often cause service degradation problems, and a large percentage of data collected from both IT operations and the SOC can be used by both teams. As such, operational processes can be accelerated and improved, saving money while reducing the risk of a poor customer experience.

Sumo Logic Overview

Sumo Logic provides a cloud-based, machine-generated Big Data analytics platform that focuses on security and operations use cases. The unified platform provides log management and analytics services and automates the collection, processing, and analysis of various data types into actionable insights that help companies improve their overall security postures combined with a suite of related products. The company offers an Artificial Intelligence/Machine Learning (AI/ML), real-time platform that powers several capabilities across security and observability domains that take advantage of the data collection, open telemetry (OT), analytics, and automation to drive business outcomes for security, IT operations, and DevOps teams. The platform enables teams to accomplish observability troubleshooting and monitoring, cloud infrastructure security, compliance and audit, and SIEM.

Since expanding its footprint in 2018, Sumo Logic has used its auto-scaling capability to help customers bring in all security-related data to make finding the unknown unknowns easier. IDC survey research shows incident investigation and threat hunting are among the top use cases for a SIEM platform. Sumo Logic's ability to query both structured and unstructured data with the creation of schemas on the fly helps security teams search through all the data to find items that may not have appeared important at first glance. Alerts may be prioritized based on the global confidence score that is associated with the alert.

Part of finding the unknown unknowns is looking for anomalous behavior among users, assets, and network traffic. Sumo Logic has built user and entity behavior analytics (UEBA) into the SIEM. For customers that desire integrated response capabilities, Sumo Logic has integrated its security orchestration automation and response (SOAR) platform into the SIEM, enabling alert enrichment and the building of playbooks.

It is often hard for customers to keep up with the requirement to tune the SIEM to reduce the noise and false positives coming from the environment. Sumo Logic is able to recommend adjustments to detection logic with ML engines.

Ensuring application reliability with modern cloud-native monitoring and observability aligns with increasing the security posture of an organization. Reducing downtime and solving customer-impacting issues faster with an integrated observability platform for all application and security data enables a unique end-to-end view of services, providing a unified analytic platform that can expedite the time to problem identification and resolution. In addition, breaking down security and IT operations silos with a modern log management solution can improve monitoring and troubleshooting, increasing an organization's security posture through the use of key insights.

The Business Value of Sumo Logic

Study Firmographics

IDC conducted research that explored the value and benefits of using Sumo Logic to improve organizations' overall security operations. The project included interviews with eight organizations that were using this solution and had experience with or knowledge about its benefits and costs. During the interviews, companies were asked a variety of quantitative and qualitative questions about the Sumo Logic solution's impact on their IT and security operations, core businesses, and costs.

Table 1 presents the aggregated firmographics of interviewed organizations. The organizations that IDC interviewed had a base of 10,150 employees with an annual revenue of $3.8 billion. While these numbers might reflect a typical enterprise, the range shows there were some smaller organizations included as part of the sample. This workforce was supported by an IT staff of 453 managing 290 business applications. There was a good mix of vertical markets represented — the financial services, information technology, education, media and entertainment, and travel and leisure sectors. (*Note: All numbers cited represent averages.*)

TABLE 1

Firmographics of Interviewed Organizations

	Average	Median	Range
Number of employees	10,150	5,500	800–30,000
Number of IT staff	453	275	13–2,000
Number of external users/customers	19.7M	527,500	350–150.00M
Number of business applications	290	150	22–1,100
Annual revenue	$3.80B	$2.01B	$108.60M–$11.00B
Industries	Financial services (2), information technology (2), education (2), media and entertainment, travel and leisure		

n = 8; Source: IDC Business Value In-Depth Interviews, September 2023

Choice and Use of Sumo Logic

The organizations interviewed by IDC described their rationale for selecting Sumo Logic to serve as a foundation for managing rapidly evolving security threats. Study participants commented that Sumo Logic gave their organizations the ability to handle large amounts of unstructured data and logs. Organizations appreciated that it helped them better deal with issues pertaining to user and infrastructure monitoring as well as cloud migration and security. In addition, interviewed organizations appreciated that the solution provided a quantum jump in improvement over and above their previous solution, which they found hard to maintain and manage.

Study participants elaborated on these and other selection criteria:

Could deal with a lot of unstructured data/logs (Director of IT Operations, Financial services):

"We went through a couple of different solutions before Sumo. We like Sumo better because it is better with our unstructured logs. Sumo gives us the ability to deal with a very diverse set of logs. We do a lot of unstructured logging."

Was having issues with user monitoring and cloud migration (Data and Machine Learning Engineer, Education):

"We use Sumo Logic for software development and cloud, as well as for cloud security and analytics. We also use it for end-user monitoring and also cloud migration, as well as infrastructure monitoring. The single event was that we were not getting any analytics or visibility into what our users were doing in real time. And we were also having issues with cloud migration."

Was struggling to go through multiple sources of data to understand issues (Vice President, Infrastructure Services, Education):

"We couldn't get all the information we needed in one place. So we had something happen to us, but there were like days and days of analysis and multiple logs that wouldn't happen now with Sumo Logic."

Previous solution was hard to maintain and manage (Executive Director, Information Technology, Media and entertainment):

"We chose Sumo because the maintenance cost of the old tool was extremely high, because I think it was hosted internally, and overall deployment was getting harder and harder. Even just to get core logs from the internal platform was much harder."

Wanted everything in one place while having a solution that could scale (Director of IT, Financial services):

"Primary reason for choosing Sumo Logic was for our log collection and ingestion. We wanted to make sure that we could get everything we needed in there. Integration with other tools is always obviously a consideration as well. Finally, scaling was an obvious question because if you can't grow with it, it won't work."

Table 2 describes the organizational usage associated with interviewed companies' deployment of Sumo Logic offerings. There is a substantial Sumo Logic footprint across all companies, with 63% of revenue and 7,075 internal users supported by 204 applications running through Sumo Logic. On average, across all companies there were five datacenters and 595 data sources. Additional metrics are presented.

TABLE 2

Sumo Logic Environment

	Average	Median
Number of business applications	204	100
Growth of business application	7%	8%
Number of datacenters	5	3
Number of day-to-day users of Sumo Logic	802	168
Number of data sources	595	600
Ingestion amount per year (TB)	312	63
Number of internal employees using applications supported by Sumo Logic	7,075	3,000
Percentage of revenue supported by applications supported by Sumo Logic	63%	100%

n = 8; Source: IDC Business Value In-Depth Interviews, September 2023

Multiple Sumo Logic products were the focus of this study. As shown in **Table 3,** the greatest usage in the companies interviewed was log analytics (88%), cloud security analytics (75%), and SIEM (63%). Additional metrics are presented.

TABLE 3

Sumo Logic Environment

	Percentage of Organization Using
Log analytics	88%
Cloud security analytics	75%
SIEM	63%
Infrastructure monitoring	50%
APM/observability	50%
End-user monitoring	25%
SOAR	13%

n = 8; Source: IDC Business Value In-Depth Interviews, September 2023

Business Value and Quantified Benefits

IDC's Business Value model quantifies the benefits for organizations using Sumo Logic's offerings to limit their organizational risk by providing quicker and more effective identification and response to security threats and other potential incidents. In part, this was accomplished by improving the overall efficiency and effectiveness of security- and troubleshooting-related teams, including core security operations, troubleshooting, and compliance teams.

The solution set helped companies participating in the study address troubleshooting issues with greater speed and efficiency, thereby minimizing any actual or potential threats. In addition, they were able to reduce incidences of unplanned downtime, which, in turn, improved end-user productivity. All of these benefits helped improve business operations and produce better business results for interviewed organizations.

In their comments to IDC, study participants described these benefits in detail:

Sumo Logic is automating several monitoring activities (Director of IT, Financial services):

"Everything we do is based on what we can automate and what can no longer be manual. So we're absolutely more efficient and more effective with Sumo Logic. We're doing things like synthetic monitoring and real user monitoring, but now we spend a lot less effort on it."

Single view of data enables more collaboration between teams (Senior Director for Technology, Information technology):

"[Having a combined security and observability solution with Sumo Logic] is very valuable to be able to send all of our data to one place for both purposes. And the ability for our engineers across security and development teams to collaborate is significantly improved because they are both using the same tool. The collaboration benefit, a lot of that, is because people are more productive because we send the data to one place."

Have improved access to data in a combined solution (Vice President, Infrastructure Services, Education):

"Let's say there's been a breach, an issue that we have to look into. We can see how far back, generally, to understand the extent of it. I'd say that all of the value that we get is because we have a combined solution. That was the whole point of getting Sumo Logic, by having the security and observability in the same tool."

Easier to manage cloud infrastructure and integration with multiple applications (Data and Machine Learning Engineer, Education):

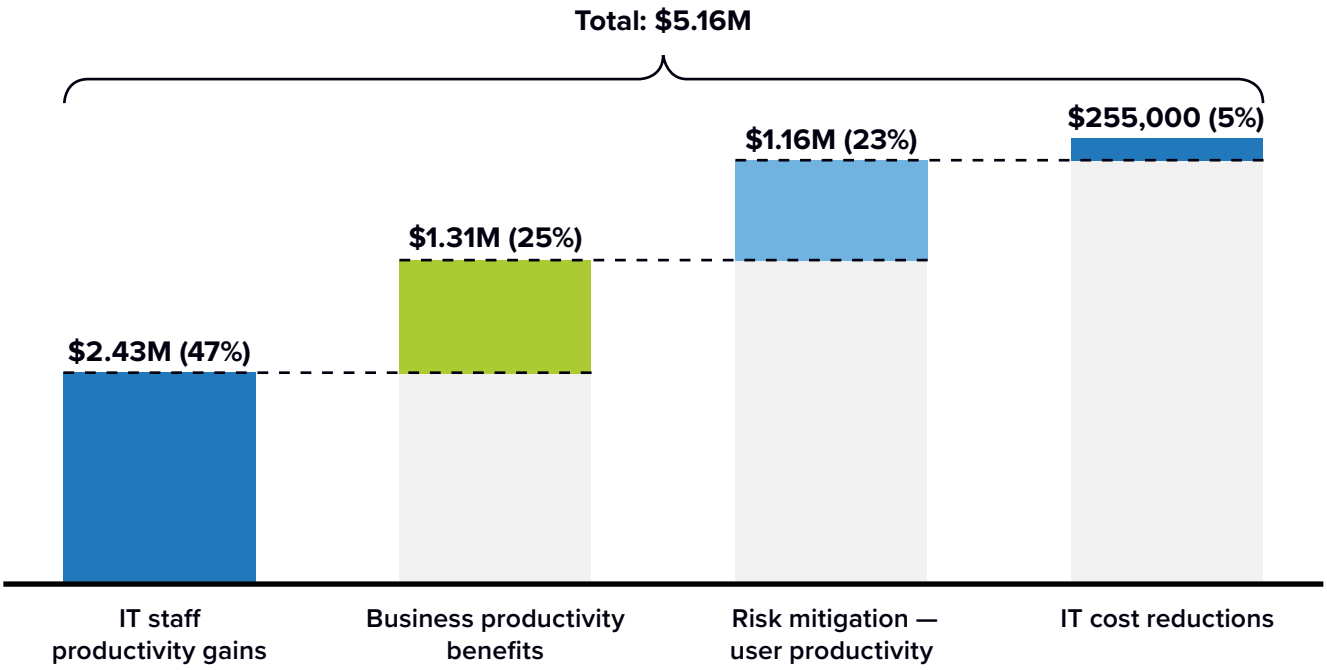
"The most significant benefit is having observability in your infrastructure. So for us, it's important to have the ability to manage the cloud from a more high-level standpoint. We also appreciate that Sumo Logic is more integrated, not just with our apps but with the tools as well. It gives us a single pane."

Based on interviews with the eight intensive users of Sumo Logic, IDC quantified the value study participants will receive as a three-year return on investment (ROI) of 376% and an annual average total of $5.16 million for each organization (or $643,400 per 100 regular users of Sumo Logic), as shown in **Figure 1** (next page).

FIGURE 1

Annual Average Benefits per Organization

($ per organization)



n = 8; Source: IDC Business Value In-Depth Interviews, September 2023

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

Improvements in Security and Troubleshooting Operations

Digital transformation's momentum has emphasized the need for better data security and integrity in many companies and vertical markets. To meet these challenges, organizations need to proactively implement technology solutions that can optimize their overall security posture. However, IDC studies show that many enterprises continue to face major gaps in their cybersecurity strategies.

Although organizations have invested in a broad range of cybersecurity tools and strategies, a significant number fall short in areas such as remote endpoint security, identity and access management controls, application and software supply chain security, remediation and response, and GRC. This is why enhancing cybersecurity is a matter of identifying additional tools and practices that can address these gaps and then adopting them.

The Sumo Logic security and resilience services are designed to address these needs and include a security and observability tools platform. These tools provide an integrated cyber-resilience approach that enables companies to anticipate, protect against, and quickly and effectively recover from adverse cyberevents if and when they occur. With the shift to hybrid work and an increasingly sophisticated and constantly changing threat landscape, organizations must also ensure robust continuity and recovery in the face of any disruption.

In their extensive comments to IDC, interviewed organizations confirmed that Sumo Logic's solutions addressed many of the security and observability challenges they were grappling with. They noted that Sumo Logic made it easier to create optimized processes for security teams with consolidated monitoring across all internal applications. They also clearly appreciated that Sumo Logic provided better insights into potential cyberattacks via the characteristics of log-in behavior. In addition, companies pointed out that platform functionality better enabled their business applications to be reliable and available.

Study participants elaborated on these and other benefits:

Easier to create optimized processes for security teams (Executive Director, Information Technology, Media and entertainment):

"Our security operations use Sumo Logic to have consolidated monitoring across all the internal apps. So, when any threat detection hits Sumo Logic, we now have an optimized process that they can actually report from."

Sumo Logic provides better insights into potential cyberattacks (Team Service Architect, Information technology):

"Sumo Logic has really helped us track cyberthreats because in addition to us monitoring the characteristics of our products, they are also looking at the characteristics of our log-in behavior, and they identify the anomalies. So, as soon as they see that our log behavior is outside of the trend that we typically show, they immediately inform us of anomalies and where to look for trends and issues."

Applications are more reliable because teams can be more proactive (Vice President, Infrastructure services, Education):

"Sumo Logic has helped improve our application reliability because we're more proactive. And also, when there's an issue, we don't have a lot of recurrence because we fix it for real."

Automation leading to more efficient teams (Director of IT, Financial services):

"Our staff is able to benefit from having more features with the automation Sumo Logic offers us. That's where they're saving the time managing this simplified environment. I think Sumo Logic gives us that."

Staff is able to free up time to work on other operational and business projects (Data and Machine Learning Engineer, Education):

"Our security staff is able to work on more high-level goals/strategies. They've been able to build out the security data lake, a new search and use more cost-effective applications. That's been able to increase visibility of our transactions."

To get a full and complete picture of the impacts of Sumo Logic's broad range of security and observability capabilities, IDC evaluated specific ways that the solution set improved the performance of various teams, beginning with security. Interviewed companies told IDC that, after adoption, their security teams gained much better visibility into potential issues allowing them to proactively address them.

Table 4 quantifies these impacts. After adoption, interviewed companies saw a 19% improvement in team efficiency. In real-world terms, this meant that, after adopting Sumo Logic, 2.7 FTEs were freed up from a team of 13.8 FTEs to work on other activities. IDC calculated that this translated into an annual productivity-based business value of $266,300 for each organization.

TABLE 4

Security Team Impact

	Before Sumo Logic	With Sumo Logic	Difference	Benefit
Security teams — FTEs per organization per year	13.8	11.1	2.7	19%
Staff time cost per year	$1.38M	$1.11M	$266,300	19%

n = 8; Source: IDC Business Value In-Depth Interviews, September 2023

Interviewed companies also reported that their security teams were able to identify and respond to issues quickly with Sumo Logic. **Table 5** (next page) quantifies these benefits; interviewed companies saw a substantial improvement in the time required to detect threats (65% faster), coupled with a 60% improvement in the time required to respond and remediate.

Drilling down further into these capabilities, study participants reported that Sumo Logic helped their companies reduce the actual number of threats they experienced. IDC evaluated the impacts of adoption by identifying and measuring several security-relevant key performance indicators (KPIs) that confirmed and amplified the data presented in **Table 5** (next page). After adoption, companies were able to respond to threats 34% faster. In addition, they could identify 20% more threats and saw a 10% reduction in the number of threats they experienced (see **Figure 2,** next page).

TABLE 5

Security Impact

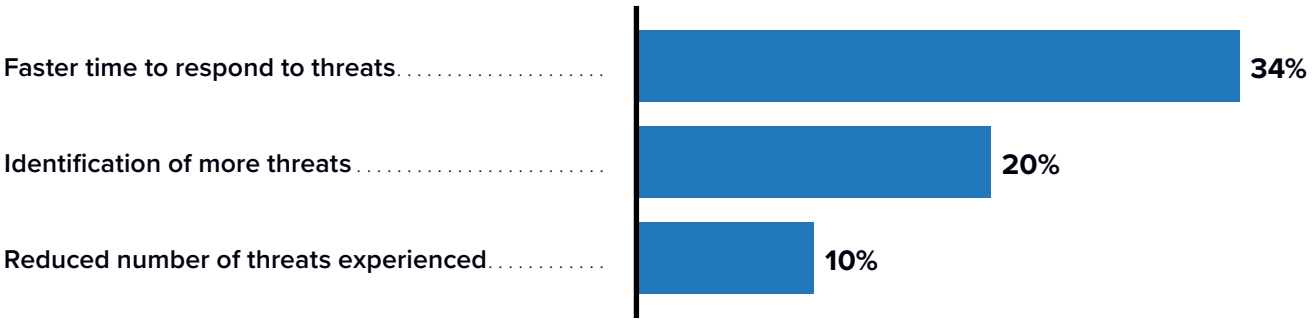
	Before Sumo Logic	With Sumo Logic	Difference	Benefit
Mean time to detect (MTTD) (hours)	1.6	0.6	1.1	65%
Mean time to respond (MTTR) (hours)	0.8	0.3	0.5	60%
Investigated incidents per analyst per day	7.2	9.4	2.1	29%

n = 8; Source: IDC Business Value In-Depth Interviews, September 2023

FIGURE 2

Security KPIs

(Percentage improvement)



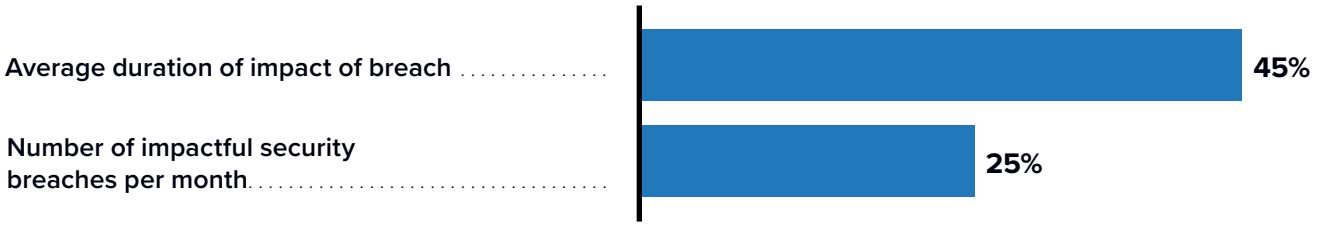
n = 8; Source: IDC Business Value In-Depth Interviews, September 2023

Looking more closely at impacts for specific incidents, study participants reported fewer security breaches that impacted their businesses while the duration of any breaches that did occur diminished. After adoption, the average duration of the impact of breaches was reduced by 45%. In addition, the number of impactful security breaches per month was reduced by 25% (see **Figure 3,** next page).

FIGURE 3

Security Incidents Impact

(Percentage reduction)



n = 8; Source: IDC Business Value In-Depth Interviews, September 2023

Troubleshooting teams also experienced important benefits from Sumo Logic's observability offerings. Sumo Logic provided these teams with a single-pane-of-glass view of the entire spectrum of their infrastructure and applications. This meant that these teams were able to be more efficient in how they approached potential issues. As shown in **Table 6,** after adoption, interviewed companies saw a 17% improvement in team efficiency. This meant that 13.9 FTEs were freed up from a team of 81 FTEs to focus on other more strategic activities. IDC calculated that this translated into an annual productivity-based business value of $1.39 million for each organization.

TABLE 6

Troubleshooting Team Impact

	Before Sumo Logic	With Sumo Logic	Difference	Benefit
Troubleshooting teams — FTE per organization per year	81.0	67.1	13.9	17%
Staff time cost per year	$8.10M	$6.71M	$1.39M	17%

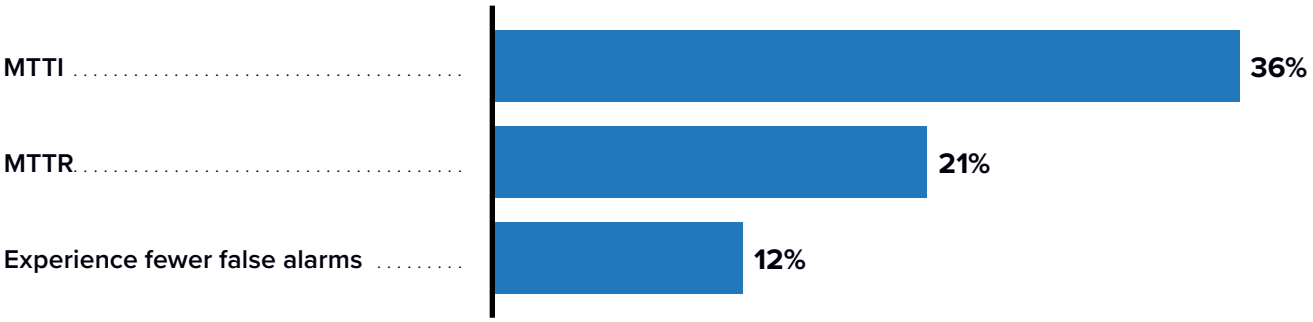
n = 8; Source: IDC Business Value In-Depth Interviews, September 2023

IDC examined the troubleshooting benefit further by evaluating several KPIs characterizing typical workflows. Organizations told IDC that Sumo Logic was able to help their troubleshooting teams tackle issues more expeditiously than with previous approaches. After adoption, MTTI improved by 36% while MTTR improved by 21% (see **Figure 4**).

FIGURE 4

Troubleshooting KPIs

(Percentage improvement)



n = 8; Source: IDC Business Value In-Depth Interviews, September 2023

Continuing with troubleshooting benefits, troubleshooting teams experienced fewer problems on their watch and, when they did occur, it took them less time to understand and resolve them, confirming the efficiencies presented (refer back to Table 6). **Table 7** (next page) shows that interviewed companies saw a 13% reduction in the number of issues to troubleshoot per week coupled with a 42% reduction in the average time to identify issues that required troubleshooting.

TABLE 7

Troubleshooting Team Objectives

	Before Sumo Logic	With Sumo Logic	Difference	Benefit
Number of issues to troubleshoot per week	123.3	107.9	15.4	13%
Average time to identify issue that requires troubleshooting (hours)	3.0	1.7	1.2	42%
Average time in total to troubleshoot per issue (hours)	3.5	2.1	1.4	39%

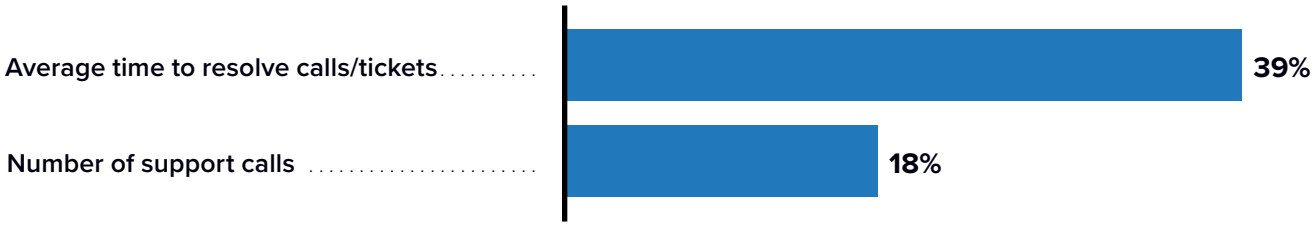
n = 8; Source: IDC Business Value In-Depth Interviews, September 2023

In a related area, study participants reported that their organizations experienced fewer help desk issues and tickets after the adoption of Sumo Logic. This improvement was directly linked to seeing fewer incidents affecting business-critical applications and workloads. IDC quantified these benefits, as shown in **Figure 5.** After adoption, *the average time to resolve calls/tickets* was reduced by 39%. In addition, *the number of support calls* was reduced by 18%.

FIGURE 5

Help Desk Impact

(Percentage reduction)



n = 8; Source: IDC Business Value In-Depth Interviews, September 2023

IT teams involved in security and other issues also experienced positive impacts. Organizations told IDC that Sumo Logic is making their IT teams more efficient because of its automation features and functionality. After adoption, interviewed companies saw a 21% improvement in team productivity, essentially adding 9.8 FTEs to staff capacity. IDC calculated that this translated into an annual productivity-based business value of $993,300 for each organization (see **Table 8**).

TABLE 8

IT Team Impact

	Before Sumo Logic	With Sumo Logic	Difference	Benefit
IT team productivity impact — FTEs	48.9	38.1	9.8	21%
Staff time cost per year	$4.80M	$3.81M	$993,300	21%

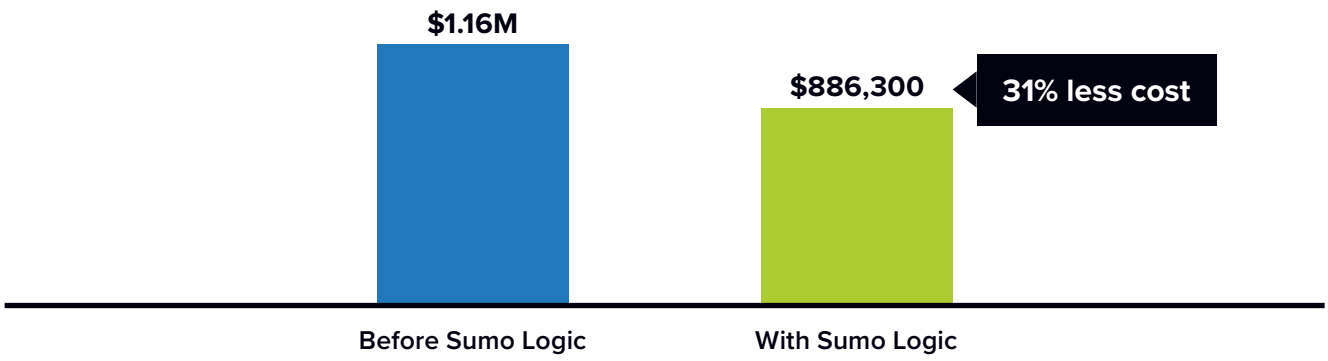
n = 8; Source: IDC Business Value In-Depth Interviews, September 2023

IDC then evaluated the cost-effectiveness of the Sumo Logic solution set. Interviewed organizations noted that they were able to save on security and observability solution costs by switching to Sumo Logic's consolidated offerings. As shown in **Figure 6**, annual costs for Sumo Logic were 31% lower overall compared with previous or alternative solutions.

FIGURE 6

Security and Observability Solution Cost Savings per Year

($ Cost Savings per Year)



n = 8; Source: IDC Business Value In-Depth Interviews, September 2023

Business Improvements with Sumo Logic

Interviewed companies told IDC that, after adopting Sumo Logic security and resilience services, they experienced direct and measurable benefits for their business operations and results. In their detailed comments to IDC, interviewed companies noted that, with Sumo Logic, business units felt more confident in their ability to scale up and provide a consistent user experience (UX). This, over time, served to ultimately improve customer satisfaction levels. They also noted that customer experience was greatly improved because of improvements in application performance and the newfound ability of their AppDev teams to roll out new applications to customers and end users more quickly.

Study participants elaborated on these benefits:

Business feels more confident in their ability to scale up and provide consistent UX (Team Service Architect, Information technology):

"It's helping us improve our customer satisfaction because we can be more proactive when it comes to incidents. Since we're a service provider, we run instances for our clients. And Sumo helps us identify issues, identify causes of production incidents, prevent production incidents, and improve scalability that's closer to the load curve. It helps with scalability because we have better insights as to what the characteristics of the load are and the required resources in the cloud that we need. That helps us save money in the cloud, but more importantly I think, it helps us provide a consistent user experience in terms of responsiveness."

More opportunities for developers and security teams to collaborate (Data and Machine Learning Engineer, Education):

"We're seeing more capabilities through Sumo Logic because they've been able to have a more cross-team collaboration between development and security teams. As a result, the developers are more productive — by like 20%."

Compliance teams have easier access to data they need for audits (Team Service Architect, Information technology):

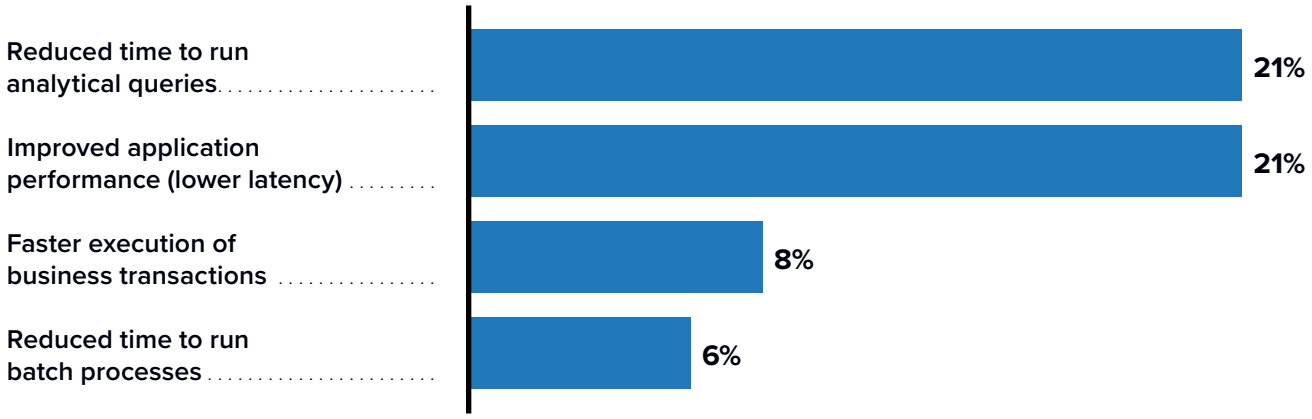
"We have a lot of compliance data from customers that our compliance teams would otherwise have to sift through and manage. But now we have all of that done in Sumo Logic with policies."

It's a truism of modern business that application development is a critical area. Study participants reported that their organizations were seeing improved performance for applications being monitored by Sumo Logic. As shown in **Figure 7** (next page), after adoption, the greatest improvements were seen in *reduced time to run analytical queries* (21%), *improved application performance* (21%), and faster execution of business transactions (8%).

FIGURE 7

Performance Impact

(Percentage reduction)



n = 8; Source: IDC Business Value In-Depth Interviews, September 2023

Another major benefit reported by study participants was a substantial reduction in unplanned downtime. Interviewees told IDC that Sumo Logic was able to give them the visibility and tools to both manage and mitigate unplanned downtime. **Table 9** (next page) provides metrics on these impacts; there was a substantial reduction in the annual frequency of downtime events (63%). In addition, the time required to resolve downtime events when they did occur was cut by 52%. These two improvement areas meant that the amount of user time lost to unplanned downtime was reduced by 82%.

TABLE 9

Unplanned Downtime Impact

	Before Sumo Logic	With Sumo Logic	Difference	Benefit
Frequency per year	41.3	15.2	26.1	63%
Time to resolve (hours)	3.5	1.7	1.8	52%
Hours lost per user	5.8	1.0	4.8	82%
FTE impact — lost productivity due to unplanned outages	22.0	3.9	18.1	82%
Value of lost productivity	$1.54M	$275,200	$1.27M	82%

n = 8; Source: IDC Business Value In-Depth Interviews, September 2023

Study participants mentioned that Sumo Logic gave them better visibility into the entire data repository, thereby helping both IT and the business units they support to ensure better compliance. Organizations reported saving $167,000 in compliance-related costs. **Table 10** quantifies these impacts. After adoption, interviewed companies saw a 28% improvement in team efficiency, which meant that about 1.2 FTEs were freed up. IDC calculated that this translated into an annual productivity-based business value of $85,000 for each organization.

TABLE 10

IT Team Impact

	Before Sumo Logic	With Sumo Logic	Difference	Benefit
Compliance teams — equivalent FTEs	4.3	3.0	1.2	28%
Staff time cost per year	$297,500	$213,000	$85,000	28%

n = 8; Source: IDC Business Value In-Depth Interviews, September 2023

IDC then drilled down further on application development benefits. Companies told IDC that Sumo Logic was able to improve both the quality and delivery of new applications. After adoption, change failure rates were improved 28%. In addition, change lead time (i.e., how long it takes to ship a change) improved 27%, as shown in **Figure 8.**

FIGURE 8

Development KPIs

(Percentage improvement)

n = 8; Source: IDC Business Value In-Depth Interviews, September 2023

Overall and in combination, all these benefits improved business operations and results. Companies reported that Sumo Logic helped their organizations improve their time to market because they gained more confidence in the infrastructure and/or applications supporting the business. Adoption resulted in a 25% improvement in time to market for services and products and a 16% improvement in business processes by reducing errors (see **Figure 9**).

FIGURE 9

Business KPIs

(Percentage improvement)

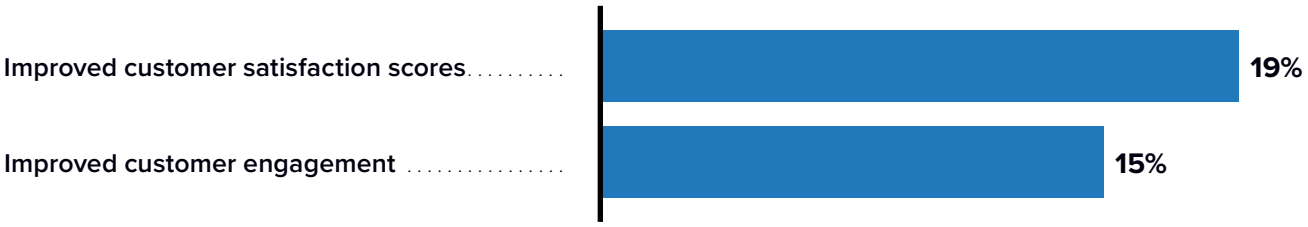
n = 8; Source: IDC Business Value In-Depth Interviews, September 2023

Customer satisfaction also improved. Organizations told IDC that they were able to provide better UX/CX, which ultimately served to better customer satisfaction scores (see **Figure 10**).

FIGURE 10

Customer Satisfaction Impact

(Percentage improvement)



n = 8; Source: IDC Business Value In-Depth Interviews, September 2023

Because companies experienced greater confidence in the infrastructure and IT operations supporting their business efforts, organizations felt more comfortable introducing new products and/or applications. Study participants were able to capture additional revenue from a variety of improvements including improved customer satisfaction; increased effectiveness and productivity of teams supporting core operations; and the ability to bring new products to market more quickly.

IDC quantified these revenue gains (see **Table 11,** next page). On a per-organization basis, IDC's calculations for revenue recognized from better addressing business opportunities amounted to $3,215,000 in total additional annual revenue for each organization. In addition, IDC's financial model applies a 15% operating margin assumption, resulting in average net revenue gains of $482,300 per interviewed organization.

TABLE 11

Business Operations and User Impact

Business Impact — Revenue From Better Addressing Business Opportunities	Per Organization	Per 100 Day-to-Day Users
Total additional revenue per year	$3.22M	$401,000
Assumed operating margin	15%	15%
Total recognized revenue — IDC model, per year	$482,300	$60,200

n = 8; Source: IDC Business Value In-Depth Interviews, September 2023

Continuing with the summary of quantified business benefits, companies reported that their end users were more productive. IDC attributes this to the fact that, overall, they had more reliable applications and supporting infrastructure for their day-to-day work and also experienced less disruptive impacts from either planned or unplanned downtime. **Table 12** quantifies these benefits showing that, after deployment, 2,800 productive hours were gained, resulting in a substantial annual business value of $695,500.

TABLE 12

End-User Impact

	Per Organization
Number of users impacted	814.3
Average productivity gains	1.20%
Productive hours gained per organization	2,800
Productive hours gained per user	2.6
End-user impact — FTE equivalent per organization per year	9.9
Value of end-user time	$695,500

n = 8; Source: IDC Business Value In-Depth Interviews, September 2023

ROI Summary

IDC's analysis of the financial and investment benefits related to study participants' use of Sumo Logic is presented in **Table 13**. IDC calculates that, on a per-organization basis, interviewed organizations will achieve total discounted three-year benefit of $12.3 million based on improved cybersecurity, better IT and security team productivity, and improved business results. These benefits compare with projected total discounted investment costs over three years of $2.58 million on a per-organization basis. At these levels of benefits and investment costs, IDC calculates that these organizations will achieve a three-year ROI of 376% and break even on their investment in approximately four months.

TABLE 13

Business Operations and User Impact

	Per Organization	Per 100 Day-to-Day Users
Benefit (discounted)	$12.30M	$1.53M
Investment (discounted)	$2.58M	$321,400
Net present value (NPV)	$9.69M	$1.21M
ROI (NPV/investment)	376%	376%
Payback	4 months	4 months
Discount factor	12%	12%

n = 8; Source: IDC Business Value In-Depth Interviews, September 2023

Challenges/Opportunities

There are some common challenges faced by technology and SOC organizations as they look to align these teams and processes to achieve common business results.

Challenges faced by technology and SOC organizations include:

- Each group typically has their own tools, budgets, and processes; historically, they have not collaborated to drive common business outcomes.
- Leadership teams must understand that collaboration across the SOC and IT operations teams is an increasing requirement for securing and enabling high-performing digital services; the pace of change and complexity outpaces a traditional silo operating model.
- SOC, IT operations, and development silos often have fragmented problems and change processes and tool chains, resulting in costly problem management processes with poor team collaboration.
- Development teams often don't have the expertise or background in maintaining the security or performance of the digital services they create; these drive higher costs and increase business risks.

Today's organizations are facing cybersecurity threats from nation-state actors and criminal gangs that aggressively target all organizations, most often for profit. Threat actors are continually adjusting their tactics to the defenses they face, looking to exploit weaknesses in areas that are left unguarded. The complexity of today's IT environment has given rise to a number of new security solutions that detect and respond to threats that were not as prevalent several years ago. Managing and correlating the alerts and detections from these tools is the job of the SIEM, so the SIEM has to keep up with the amount of data.

It is not enough to ingest the data but to make sense of it by recognizing patterns of activity in the alerts so action can be taken to stop the adversary before damage is done. Too often, the threat actor is able to find an unknown gap that is not being monitored, and then it is too late. A SIEM needs to detect the unknown and offer automated actions that help security teams move faster than the adversary.

Conclusion

The business value of aligning and using common metrics, logs, data, and events in a unified platform for security and IT operations teams is clear and impactful. The value and outcomes span multiple value streams such as the impact on multiple teams and their level of productivity, an improvement in security capabilities and a more proactive and predictive posture, and an increase in operational excellence with improved digital service performance. The cost savings and optimization opportunities also span the people, process, and technology fields. Teams accomplish tasks faster, processes can be automated and streamlined across teams using a single data platform, and AI can be used to drive actions and reduce the time to problem identification and resolution. Technology organizations and leadership teams should be considering how security, development, and IT can provide business outcomes in a more collaborative model utilizing a singular technology platform.

Appendix 1: Methodology

IDC's standard ROI methodology was utilized for this project. This methodology is based on gathering data from current users of Sumo Logic.

Based on interviews with these organizations, 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 Sumo Logic.** 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 Sumo Logic 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 Sumo Logic over a three-year period. The ROI is the ratio of the net present value (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 a number of assumptions, which are summarized as follows:

- Time values are multiplied by burdened salary (salary + 28% for benefits and overhead) to quantify efficiency and productivity savings. For the purposes of 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).
- The net present value of the three-year savings is calculated by subtracting the amount that would have been realized by investing the original sum in an instrument yielding a 12% return to allow for the missed opportunity cost. This accounts for both the assumed cost of money and the assumed rate of return.
- Further, because Sumo Logic requires a deployment period, the full benefits of the solution are not available during deployment. To capture this reality, IDC prorates the benefits on a monthly basis and then subtracts the deployment time from the first-year savings.

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

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

Annual Average Benefits per Organization

	Average Annual Benefits per Organization
IT staff productivity gains	$2.43M
Business productivity benefits	$1.31M
Risk mitigation — user productivity	$1.16M
IT cost reductions	$255,000
Total	**$5.16M**

n = 8; Source: IDC Business Value In-Depth Interviews, September 2023

Return to original figure

About the IDC Analysts

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 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

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

Stephen Elliot

Group Vice President, I&O, Cloud Operations, and DevOps, IDC

Stephen Elliot manages multiple programs spanning IT Operations, Enterprise Management, ITSM, Agile and DevOps, Application performance, Virtualization, Multicloud Management and Automation, Log Analytics, Container Management, DaaS, and Software Defined Compute. Stephen advises Senior IT, Business, and Investment Executives globally in the creation of strategy and operational tactics that drive the execution of Digital Transformation and business growth.

More about Stephen Elliot

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

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.