Smarter security starts with the right data

How leading teams are reducing costs without losing visibility

RESEARCHED BY

OMDIA

COMMISSIONED BY

splunk> a cisco company

EXECUTIVE SUMMARY

- Security teams face increasing pressure to reduce costs while maintaining visibility and performance across complex, hybrid environments. Budget constraints, evolving threats, and data growth are forcing teams to rethink their monitoring and analytics strategies.
- Current cost-cutting methods, like reducing data ingestion or coverage areas, often backfire—increasing risk and operational blind spots. Many organizations struggle to balance savings with effective threat detection and compliance.
- Forward-looking teams are investing in scalable, platform-agnostic approaches like data tiering, federated analytics, and automation to protect performance and ensure strong future outcomes. These strategies help reduce costs while preserving agility, visibility, and security maturity.

Introduction

Security data management has been a persistent but evolving problem in cybersecurity for a couple of decades. Initially, the problem was primarily limited availability of security telemetry. As that problem began to be solved, centralization and analysis became the focus. Now, there is so much potentially useful security telemetry available, and so many analytic tools and applications across an increasingly complex storage landscape, that finding cost-effective ways to bring it all together has become a primary concern.

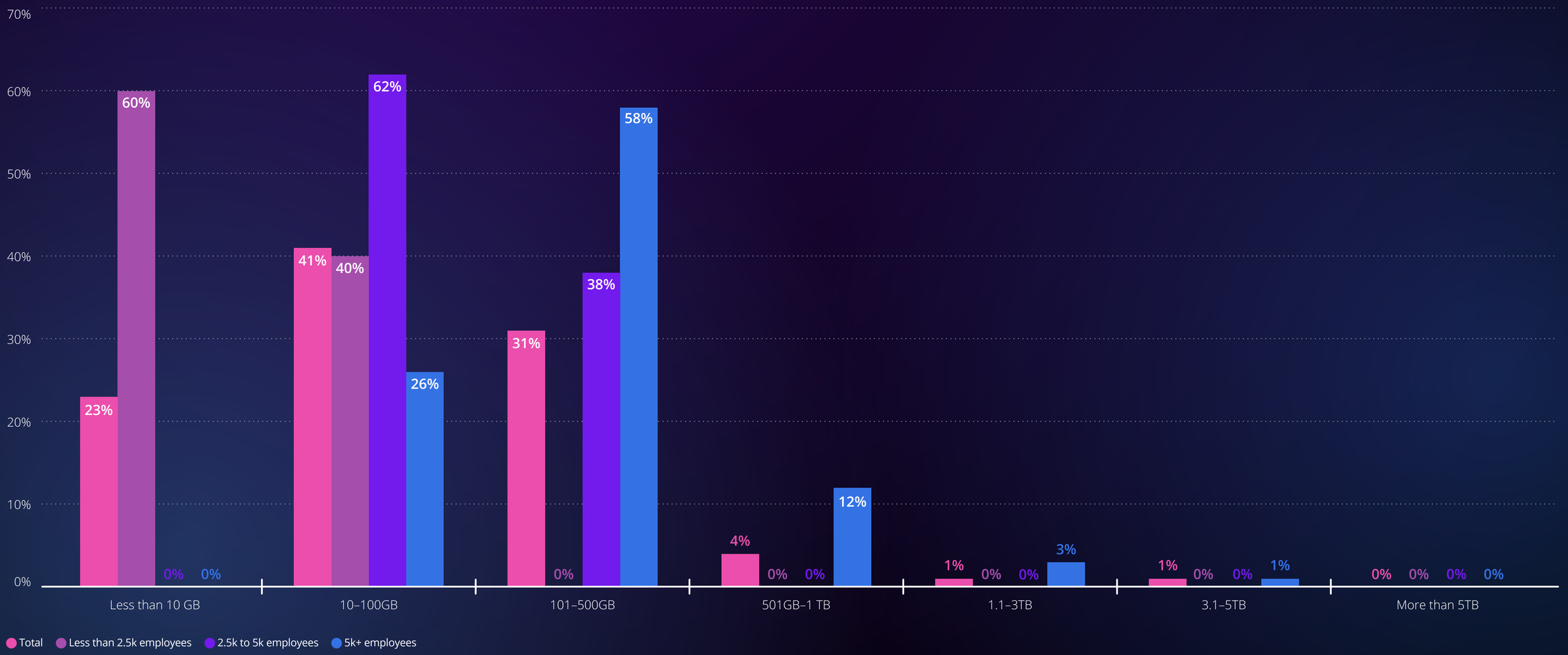
Organizations today are struggling with managing too much low-value data, in too many places, while at the same time worrying that visibility gaps mean they might be missing some high-value data. The primary inhibitor today, and the primary inhibitor expected over the next several years, is the cost of managing all this security data. However, organizations see a way forward, based on a strategy of optimizing security data management practices and leveraging automation technologies, which increasingly involve the use of GenAI.

Omdia fielded a survey to 462 cybersecurity decision-makers to understand how organizations are using security data and the drivers and inhibitors of more strategic security data use. Respondents represented organizations in North America, South America, EMEA, and APAC, with at least 500 employees. Respondents held manager-level and above positions, with decision-making capability for SecOps strategy or purchase decisions at their organization. For full information on the respondents' demographics, please see the appendix.

Current State: Data volume grows exponentially

So, how much security data does a typical organization ingest today? Well, not surprisingly, that depends on several factors, most notably the size of the organization. However, most organizations (78%) ingest at least 10GB of security telemetry data every day. Large enterprises can ingest much more. Among the organizations with more than 5,000 employees surveyed, 4% ingest 1TB or more of security telemetry daily.

Figure 1: Average security telemetry ingested daily (by company size)

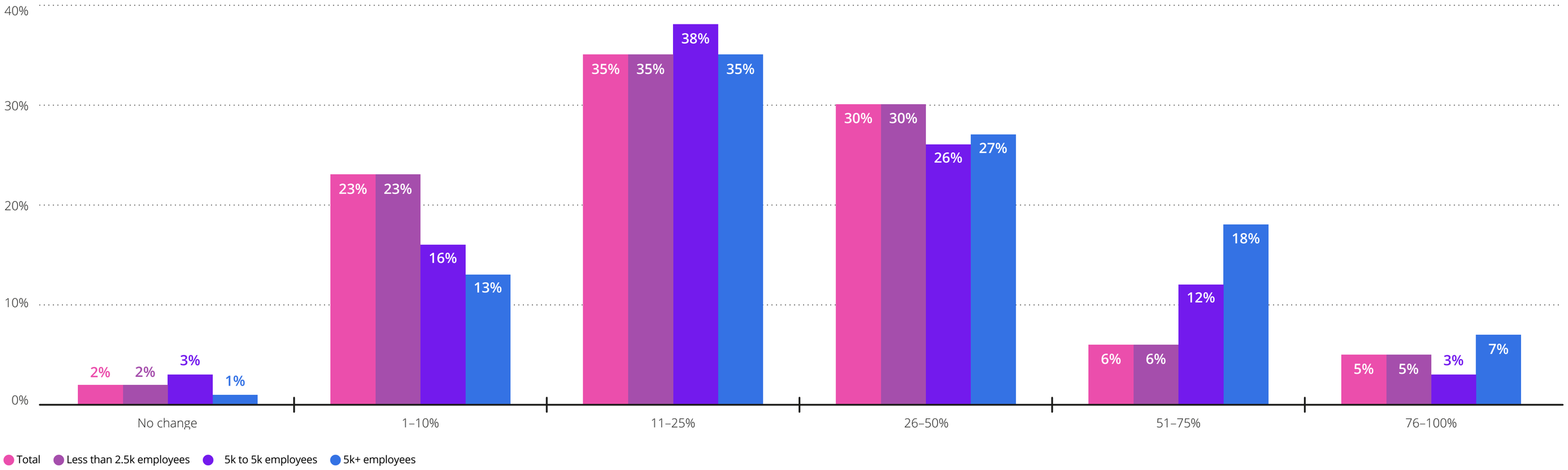


SOURCE: OMDIA

Regardless of company size, the amount of security data collected year-over-year continues to grow (see Figure 2). More than ten percent (10.8%) of organizations saw a year-over-year increase of more than 50%. For organizations with over 5,000 employees, 25% reported more than 50% growth in the amount of security data ingested.

Adding to this complexity is the fact that storage locations are also increasing. On average, organizations are storing data across seven different locations. Not only is there too much data to keep track of, but it is also now spread across an ever-broadening landscape.

Figure 2: Average growth in security data volume (year/year) by company size



SOURCE: OMDIA, **NOTES:** N=462 SECOPS DECISION MAKERS

Sources of growth

Among all organizations surveyed, 98% report data growth in the past year. The sources of data that were flagged most often as impactful to this growth are listed in Table 1.

Overall, cloud workloads are flagged by most organizations as a contributor to security data growth. Cloud logs were cited by an even higher (72%) percentage of respondents in APAC. EDRs, whose telemetry does not always have the best reputation with respect to its signal-to-noise ratio, were flagged by 44.8% of respondents. Larger companies more often cite IoT/OT security data and EDR telemetry as contributing to data growth than smaller companies.

An additional complexity in data growth is that approximately half of respondents supported federated search across disparate data sources. On average, seven data sources were supported, but not surprisingly, large enterprises were much more likely to support a greater number of data sources (see Figure 3).

Table 1: What data sources contribute the most to your security data growth?

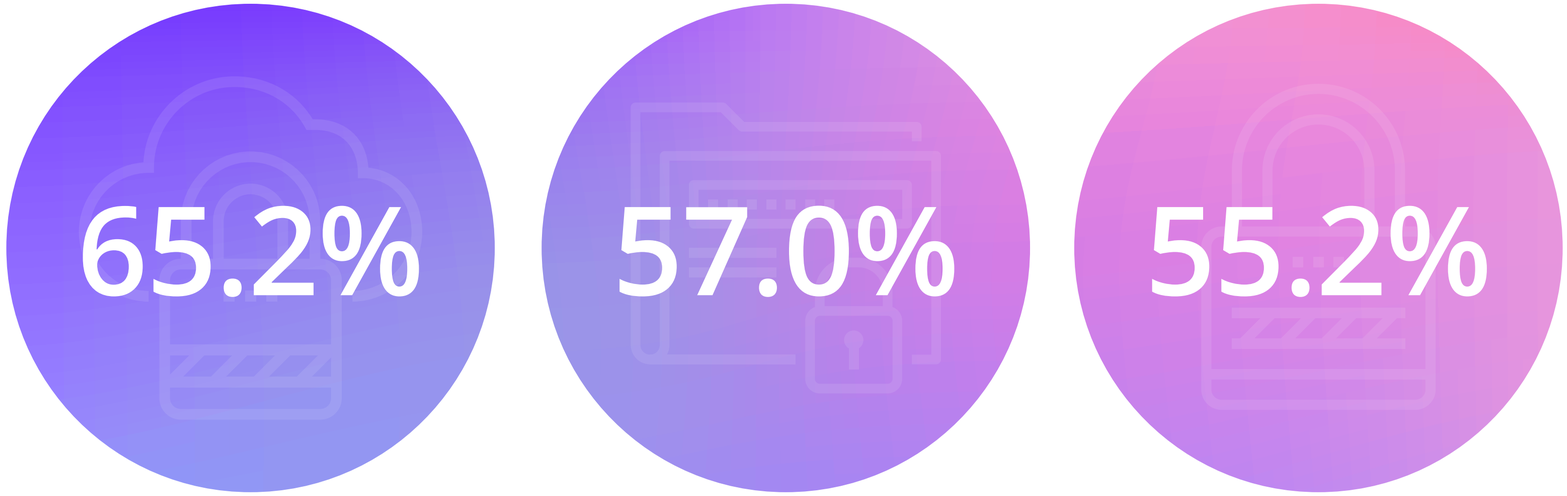
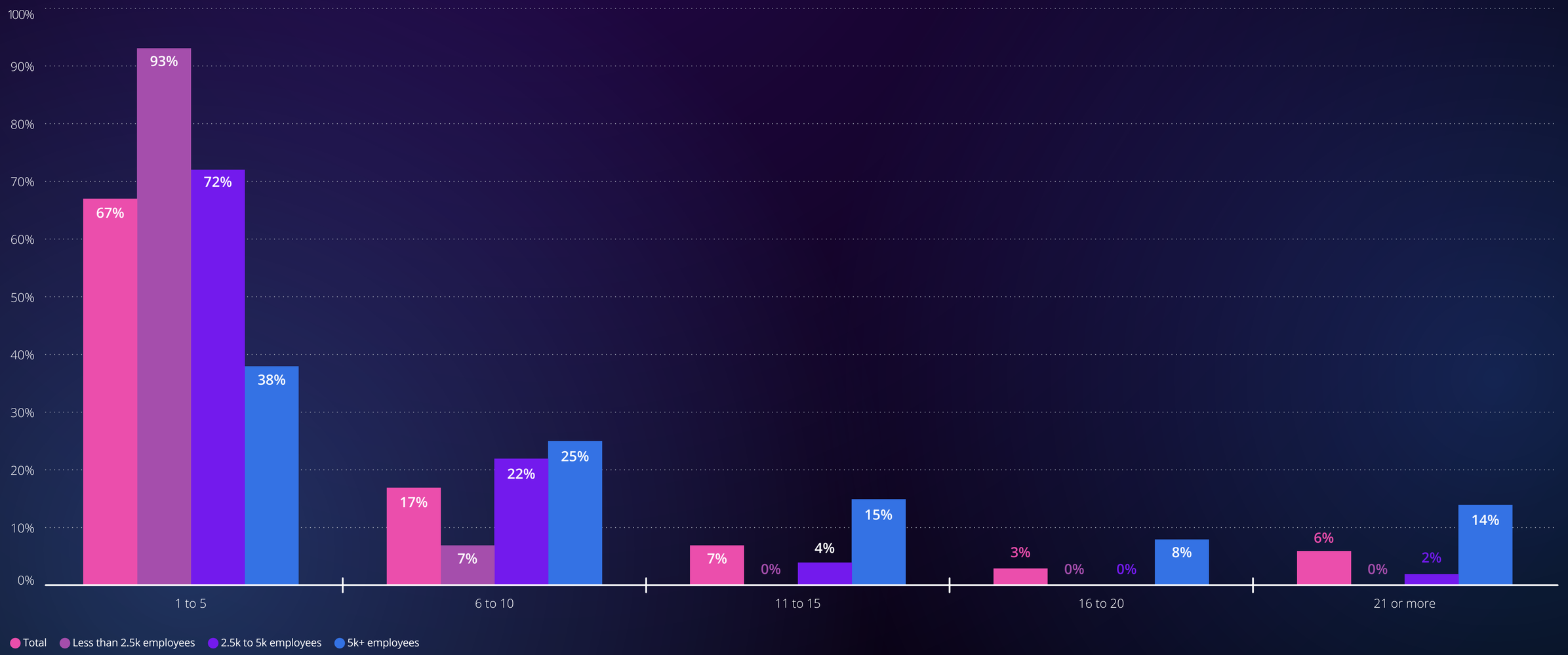


Figure 3: Average number of data sources supported, by company size



SOURCE: OMDIA, **NOTES:** N=462 SECOPS DECISION MAKERS

There is broad reliance on public cloud infrastructure to store security telemetry data across regions and by company size (see Table 2). Large enterprises are more likely to use private cloud (55%) than organizations with fewer than 2,500 employees (35%). Surprisingly, large enterprises are also more likely to use managed security services provider (MSSP) storage than organizations under 2,500 employees (35% to 25%).

Organizations are increasingly seeking solutions to preserve the flexibility of cloud storage while maintaining stringent security standards. This balance is especially critical as teams look to scale analytics capabilities without locking themselves into rigid or high-cost models. Cloud continues to be the forerunner, but the most security-mature verticals are still more hesitant to move data to the cloud—48% of BFSI organizations still store their data on-prem.

Table 2: Where does your organization store security data?

Public cloud (e.g., AWS, Azure)	55.6%
Hybrid cloud environment	50.4%
Private cloud	44.8%
Security information and event management (SIEM) system	41.6%
On-premises data centers	39.8%
Managed security service provider (MSSP) environment	30.3%
Data lake	12.6%

Organizations struggle to find meaningful value from massive data sets

Security teams are in an increasingly precarious position. As we have seen, the amount of data continues to grow, and as we will see, so do the costs associated with collecting, processing, and analyzing security data. Cost has become the number one concern when determining which security data to ingest (see Table 3). Without a strategic approach to security data management, that constraint can run at cross purposes to the other most important data evaluation criteria: value to the SOC team and meeting compliance and regulatory requirements.

Organizations in North America are more concerned with costs than other geographies (60% compared to 55% overall). North American respondents also tend to be more concerned about the accessibility of data (64% to 54%) and the volume of data (54% to 46%) provided by a given data source.

Cost concerns are so prevalent that most organizations (61.5%) now have a formal security telemetry data storage strategy in place that relies on purpose-specific tools and processes. (This number is approximately 70% among organizations based in APAC [70.5%] and South America [69.3%].) Another 30% of organizations overall have an information strategy that uses ad-hoc tools and informal processes.

Table 3: What factors do you evaluate when determining which security data to ingest?

55.2%	Cost of data storage and processing
55.2%	Value to the SOC team, especially for threat detection and response (TDIR)
55.2%	Compliance and regulatory requirements

SOURCE: OMDIA

ABUNDANCE WITHOUT UTILITY

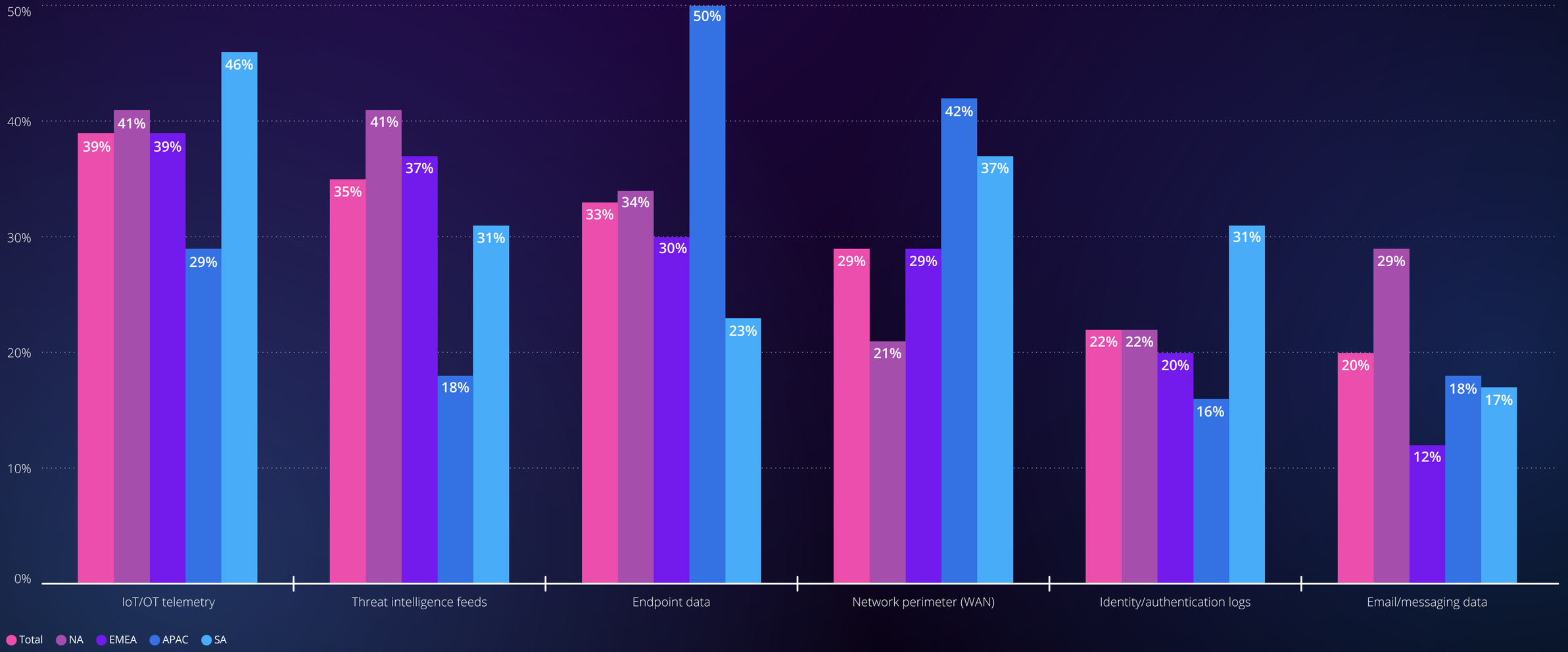
Challenges around cost are driven primarily by both the overall growth in security data available and a sort of "fear of missing out" that the right data will not be ingested and stored. In fact, despite the widely held concerns around cost and data overload, organizations still widely believe that they have visibility gaps that need to be addressed.

Overall, only 42% of organizations report having full visibility into their digital infrastructure. While almost no organizations with more than 2,500 employees reported having "significant" data blind spots, 50% reported some gaps. Disturbingly, a third (33.5%) of organizations with fewer than 2,500 employees reported significant blind spots.

Among all organizations, gaps in IoT/OT telemetry, threat intelligence feeds, and endpoint data are top concerns. There is, however, significant variation by region in what is not being collected (see Figure 4).

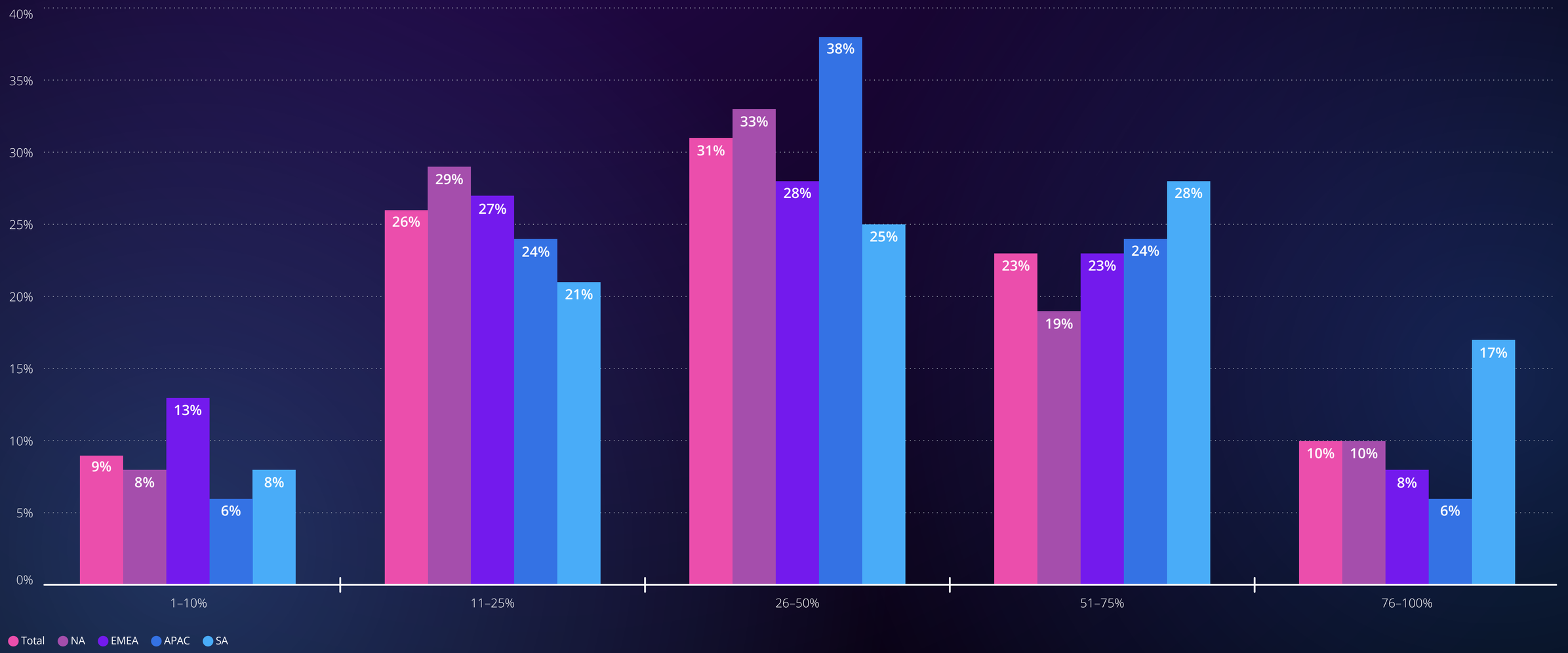
An additional concern is that overall, 67% of organizations report that less than half of the security data they collect is useful for TDIR. As seen in Figure 5, however, there are significant differences in response to this question by region.

Figure 4: Data not gathered/not fully gathered, by region



SOURCE: OMDIA, **NOTES:** N=462 SECOPS DECISION MAKERS

Figure 5: Percentage of security data collected that is useful for threat detection and response, by region



SOURCE: OMDIA, **NOTES:** N=462 SECOPS DECISION MAKERS

COST CHALLENGES EXPECTED TO PERSIST

Perhaps the most daunting aspect of the challenges facing TDIR teams is the fact that they appear to be getting worse, not better. The top three challenges noted by organizations today are:

- **Rapid growth in the volume of data**
- **Balancing the need for comprehensive data with information overload**
- **Unpredictable costs**

These challenges were relatively consistent across geographies, but APAC stood out for several challenges. APAC-based organizations were more likely to be challenged by data volumes (49% compared to 41% of all respondents), balancing security needs with the cost of a solution (49% to 36%), managing redundant/unnecessary data (53% to 32%), and managing data residing in disparate locations (40% to 31%).

When asked to predict the biggest concerns related to security data management several years from now, rising financial costs remain the biggest concern (see Table 4). In fact, cost is expected to be a major concern by an even larger percentage of organizations (28.6% to 30.1%). Among all organizations, concerns about rising costs outpace all other concerns by at least ten percentage points, and the only other concern that is not expected to be (somewhat) alleviated over this timeframe is growth in IoT/OT data.

Table 4: What is your biggest concern with security data management today and in 2–3 years from now?

RESPONSES	TODAY	2–3 YEARS FROM NOW
Rising financial costs	**28.6%**	**30.1%**
AI's role in security operations	19.9%	19.3%
Growth of IoT/OT security data	18.4%	18.8%
Ensuring continued data availability	16.9%	16.2%
Complexity of federated data management	16.0%	15.2%

SOURCE: OMDIA

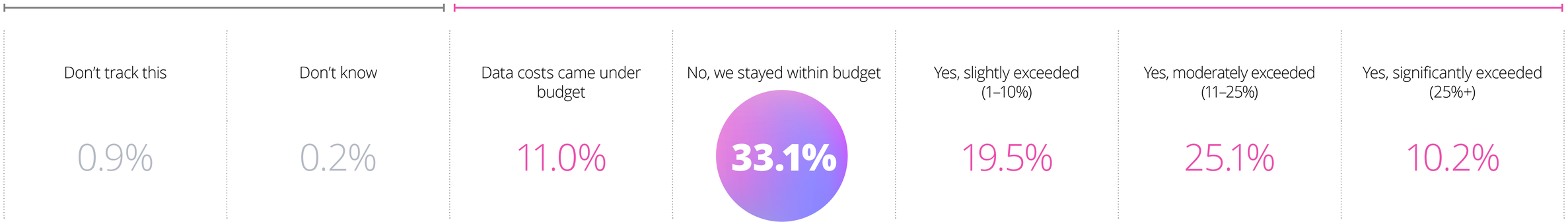
Organizations deploy a host of techniques to increase the value of security data, including filtering and prioritizing high-value data sources (62%) and implementing deduplication and optimization strategies (45%). More than half of organizations (53.7%) use a tiered storage strategy for security data to help manage costs.

Where does all this complexity leave organizations with respect to analysis of security data? Less than four percent of organizations report that they can support real-time (i.e., instant) analysis in response to a breach, and less than ten percent (8.9%) can perform near-real time (i.e., within minutes) analysis.

Table 5: Thinking back to your organization's last major security incident, how quickly was your team able to access and analyze all the stored security data needed to determine what happened?

RESPONSES	ALL RESPONDENTS
Instantly	**3.9%**
Within minutes	**8.9%**
Within hours	**40.9%**
Within a day	**35.3%**
Multiple days or longer	**10.0%**
Don't know	**1.1%**

Table 6: Have your actual data costs exceeded your forecasts in the past year?



SOURCE: OMDIA

TRADEOFFS AND UNCERTAINTY

As noted, security teams are left balancing serious cost concerns with the need for more (and better) data for both security and compliance requirements. Not surprisingly, this is a difficult balance. More than half (54.8%) of organizations reported that security data costs exceeded forecasts last year. 10% of organizations report that they significantly (i.e., more than 25%) exceeded forecasts.

Interestingly, larger organizations (5,000 employees or more) were more likely to stay within budget (42%) compared to all respondents (33%) but were also slightly more likely (13% compared to 10% overall) to significantly exceed budget (i.e., 25% or more).

The inability to accurately budget the costs of security data management can leave security teams with limited recourse if they exceed budget. The most common options for addressing budget overruns are making additional funding requests (50%) and sharing the overrun across multiple departments (39%). As bad as these choices are, the third most "popular" response (38%) is reducing data ingestion to cut costs—all of which are ultimately ineffective for data management.

GETTING IN FRONT OF THE PROBLEM

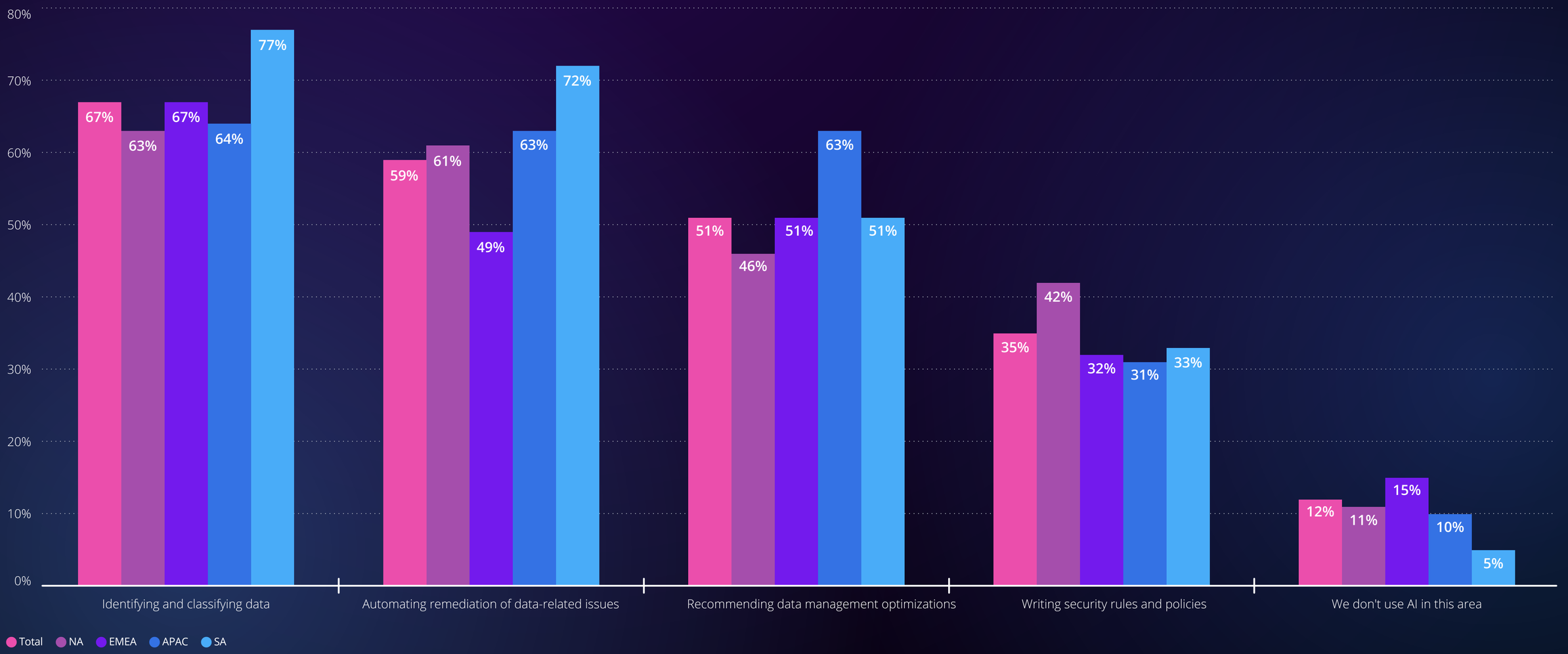
Understandably, organizations are quite literally trying to get in front of the problem. When asked to rate the most important factors in the data ingestion process, data onboarding was rated critical by 49% of organizations, followed closely by data pipeline management (44%).

Organizations across the board report some level of investment in data pipeline management. Overall, 23% of organizations have significantly increased (15% or more) spending on security pipeline management year-over-year, and 50% reported moderately (less than 15%) increased year-over-year spend.

The next era of security data management will be powered by AI

There is a strong conviction that the future of security data management is AI-powered. The embrace of AI tools to enhance security data management has been broad and swift. Currently, 88% of organizations are using AI for some aspects of security data management (see Figure 6).

Figure 6: Where organizations use AI for security data management



SOURCE: OMDIA

Table 7: Which features/functionalities are most important in a security data management solution?

FEATURES	
AI-powered insights and automation	47.4%
High-quality data onboarding	45.7%
Advanced search and analytics (e.g., federated, high-speed capabilities)	42.9%

Table 8: What benefits would you experience from an optimized security data management practice?

BENEFITS	
Increased flexibility in data access and usage	53.5%
Better overall security posture	53.5%
Reduced costs/improved cost efficiency	49.4%

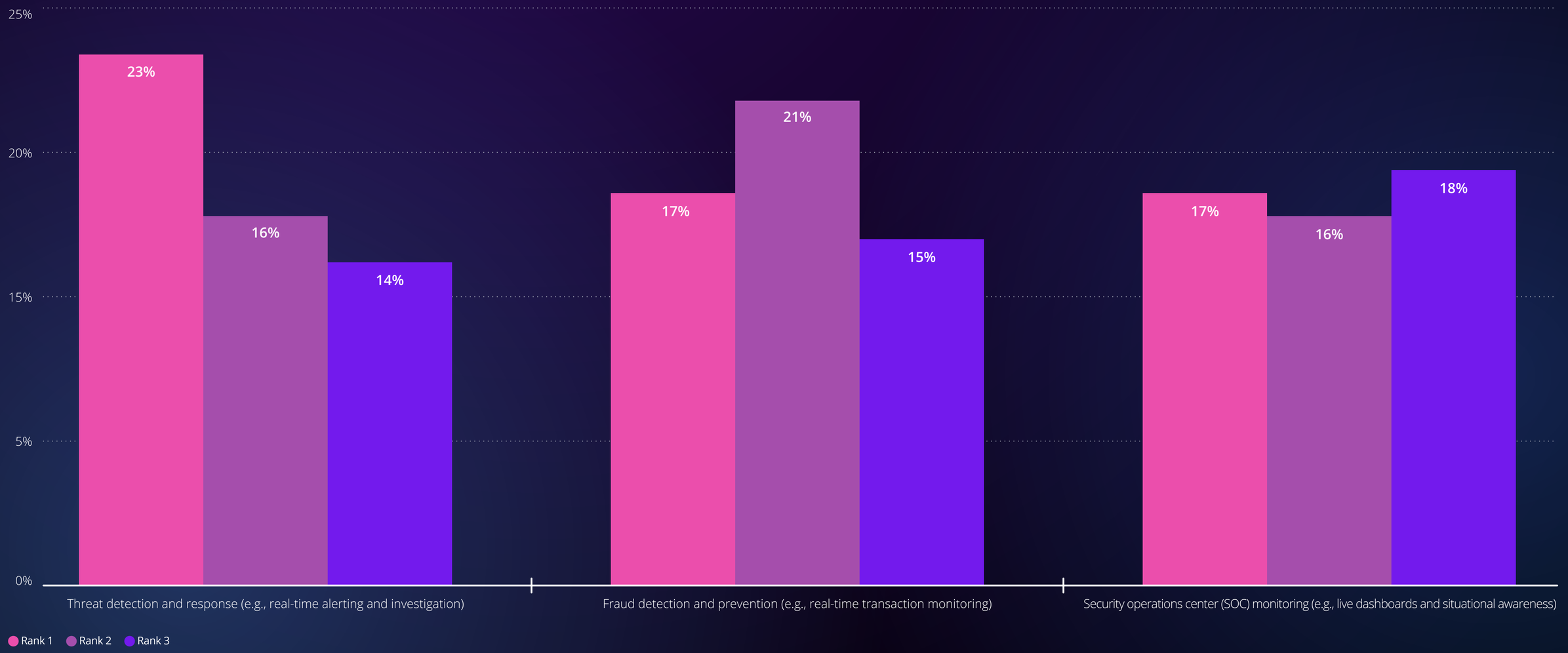
In fact, AI-enabled automation is now viewed as the most requested component of security data management solutions (see Table 7).

What are the expected benefits of enabling these features and optimizing security data management best practices? When asked about expected benefits, the top three responses (see Table 8) address greater flexibility in data usage, better security outcomes, and lower costs.

Organizations want to be more innovative in how they use security data, and they believe that doing so strategically will improve both their security posture and cost structure. What is clear from the data is that organizations want the right data delivered to the right user at the right time. Increasingly, that requires an open, flexible, and federated architecture that can deliver security data in real time.

The desire to broadly analyze security data in real time is driven by several important use cases. When asked where they would find the most value from real-time security data processing, organizations had a clear focus on TDIR, fraud detection and prevention, and SOC monitoring (see Figure 7).

Figure 7: Use cases in which real time data processing provides the most benefit



SOURCE: OMDIA

Conclusion

Security telemetry data will only continue to grow at an unprecedented rate, meaning now is the time for organizations to separate signal from noise. While the need for strong TDIR has historically contrasted with concerns around cost, complexity, and visibility, we are beginning to see a path forward that allows organizations to effectively balance security practitioners' need for the right data at the right time, with the fiscal realities of cloud storage.

The future of security data management hinges on architecture that is open, flexible, and real-time, which will enable organizations to get the right data to the right teams and tools, as fast as needed. Strategic data onboarding, tiered storage, and AI-powered automation are no longer nice-to-haves—they are critical to maximizing the value of every bit of data ingested.

Ultimately, organizations must balance this innovation with cost-efficiency, meaning watching spend closely, prioritizing high-value data, and ensuring their data infrastructure can adapt quickly to emerging use cases. The organizations best positioned for success will be those that can flexibly ingest and analyze security data at scale, in real time, and at an accessible cost.

Recommendations

Based on the data findings from this survey, Omdia has four key recommendations for organizations looking to improve their security data management practice:

Adopt a tiered data storage strategy: Implementing a multi-tiered approach can help manage growing security data volumes, performance, and cost. Frequently accessed or high-value data should remain in fast-access storage, while archival or low-priority data can be offloaded to cold storage. Further, regularly assessing which of these data sources are delivering high-security value versus those that are contributing excess cost can help continuously manage costs.

Prioritize real-time monitoring capabilities: Invest in infrastructure and processes that support real-time detection and response. Organizations should assess where they need immediate visibility (usually at critical systems or endpoints) and build pipelines that support streaming data analytics and minimal latency alerting. For endpoints specifically, this consistent collection can greatly reduce blind spots.

Capitalize on AI and automation for alert management: The volume of security alerts can be overwhelming, especially as data volume increases. This can be a prime use case for AI (such as behavior analytics, prioritization, and automated triage) and can help reduce analyst fatigue and increase the likelihood of catching true positives faster.

Utilize a federated data access model: Enable querying of data across disparate systems without centralizing all telemetry in a single repository. A federated approach supports cost management, reduces data duplication, and offers flexibility for hybrid and multi-cloud environments. Further complementing this approach with a low-cost, easily searchable storage solution like a data lake will provide further scalable retention without sacrificing accessibility or performance.

Appendix

Methodology

In April 2025, Omdia conducted an online survey of 462 SecOps decision makers regarding their priorities, challenges, and needs in security data management. Survey participants included respondents in manager-level positions and higher, across global geographies. Surveys were fielded using a double-blind methodology to ensure anonymity.

GEOGRAPHY	
EMEA (UK, Germany, France)	34%
North America (US, Canada)	33%
APAC (India, Japan, China, Singapore)	17%
South America (Brazil, Mexico)	16%

COMPANY SIZE (EMPLOYEES)	
500 – 999 employees	16%
1,000 – 2,499 employees	22%
2,500 – 4,999 employees	26%
5,000 – 9,999 employees	23%
10,000+ employees	13%

RESPONDENT ROLE	
IT	82%
Cybersecurity	18%

RESPONDENT LEVEL	
C-level Executive	10%
Vice President	14%
Director	46%
Manager	30%

INDUSTRY (TOP 5)	
Technology services/consulting	17%
Software/SaaS	17%
Manufacturing, construction, materials	14%
Banking, financial services, insurance	12%
Retail/eCommerce	11%

About

Splunk

Cisco (NASDAQ: CSCO) is the worldwide leader in technology that powers the Internet. Cisco inspires new possibilities by reimagining your applications, securing your data, transforming your infrastructure, and empowering your teams for a global and inclusive future. Discover more at www.cisco.com.

Splunk, now part of Cisco, helps organizations worldwide turn data into doing. Splunk's unified security and observability platform delivers real-time insights across diverse environments, enabling organizations to build resilience, accelerate innovation, and drive business outcomes. As part of Cisco's portfolio, Splunk expands its mission to power a more secure, connected, and inclusive future. .

Learn more at www.splunk.com

Omdia

Omdia is a global technology research powerhouse, established following the merger of the research division of Informa TechTarget (Ovum, Heavy Reading, and Tractica) and the acquired IHS Markit technology research portfolio*.

We combine the expertise of more than 400 analysts across the entire technology spectrum, covering 150 markets. We publish over 3,000 research reports annually, reaching more than 14,000 subscribers, and cover thousands of technology, media, and telecommunications companies.

Our exhaustive intelligence and deep technology expertise enable us to uncover actionable insights that help our customers connect the dots in today's constantly evolving technology environment and empower them to improve their businesses – today and tomorrow.

*The majority of IHS Markit technology research products and solutions were acquired by Informa in August 2019 and are now part of Omdia.

The Omdia team of 400+ analysts and consultants are located across the globe

Americas

Argentina
Brazil
Canada
United States

Asia-Pacific

Australia
China
India
Japan
Malaysia
Singapore
South Korea
Taiwan

Europe, Middle East, Africa

Denmark
France
Germany
Italy
Kenya
Netherlands
South Africa
Spain
Sweden
United Arab Emirates
United Kingdom

Omdia

E insights@omdia.com
E consulting@omdia.com
W omdia.com

OmdiaHQ
Omdia

Citation Policy

Request external citation and usage of Omdia research and data via citations@omdia.com