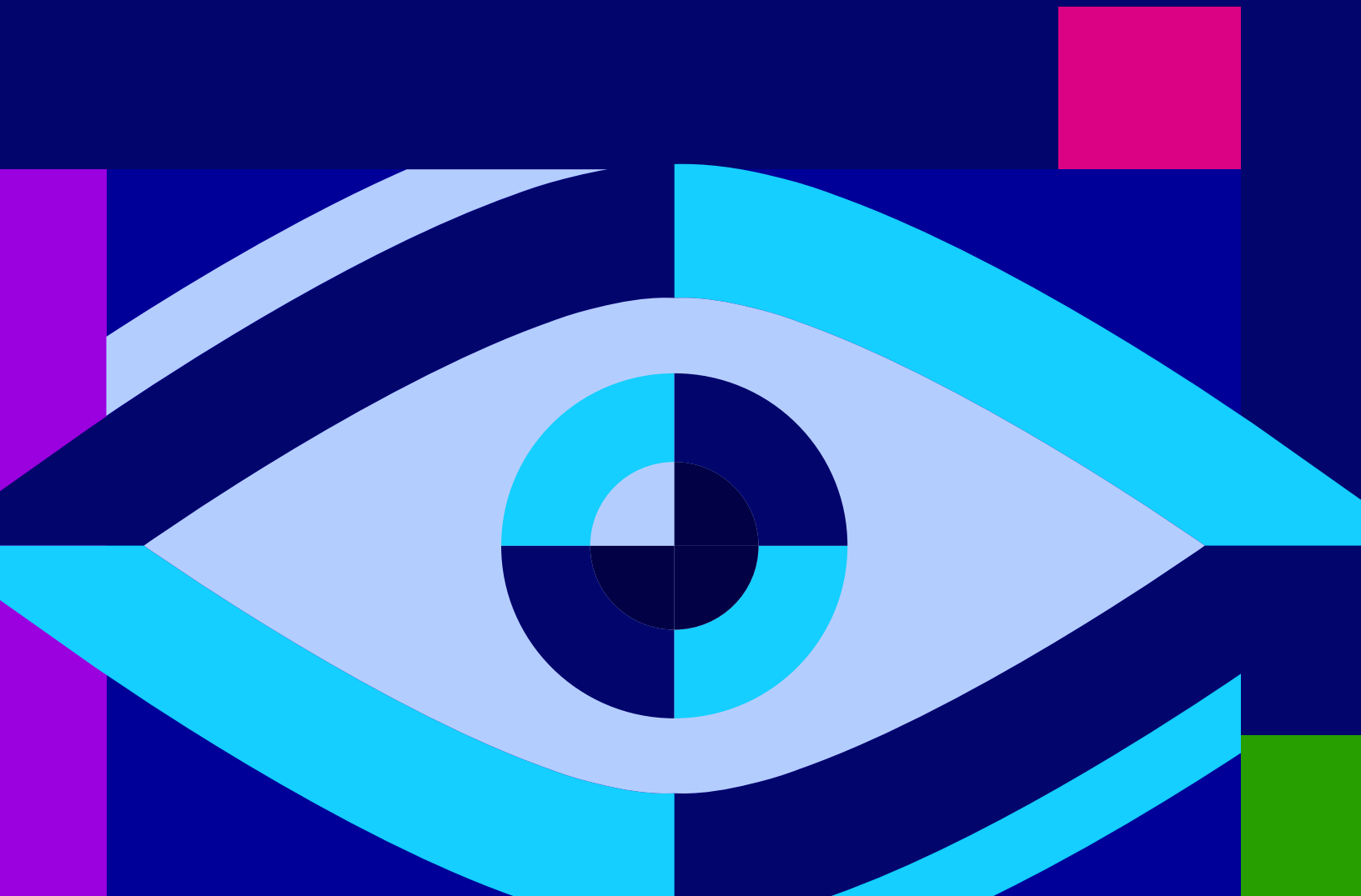
sumo logic

Research conducted and verified by UserEvidence

RESEARCH CONTENT 2026

2026 Security operations insights

Two-thirds of security leaders lack security tooling designed for modern application environments



What's inside

Introduction

Security is only becoming more complicated for enterprise organizations. Application environments are changing rapidly as DevOps teams dial up velocity and data volumes scale. Hype around AI has created a rush to develop and adopt AI tools while broadening the attack surface and forcing defenders to reconsider the viability of their solutions.

At the same time, attackers are escalating their tactics: stealing credentials at scale, disrupting operations through advanced ransomware, and exploiting gaps across supply chains. These types of breaches affect millions of users, illustrating how quickly an exposure can spread across cloud ecosystems.

In response, many security leaders are investing in more security and cloud operations tools. Yet these sprawling security tech stacks often create additional problems. Many don't communicate with one another, creating more work and less reliable coverage. As security teams become leaner, they have less capacity to connect the dots between siloed tools.

To understand how enterprise organizations are navigating these challenges, Sumo Logic partnered with UserEvidence to survey 506 security leaders. The data reveals overwhelm and frustration as well as a clear need for security and cloud operations tools that simplify, consolidate, and create a source of truth security leaders can trust.

Key takeaways

90%

Ninety percent of security leaders say AI/ML is extremely or very valuable in reducing alert fatigue and improving detection accuracy. Yet their most common AI use cases focus on basic tasks like threat detection. AI adoption isn't as widespread through advanced security workflows as marketing narratives often suggest.

37%

Most enterprise organizations are experiencing rapid change in their application environments. Yet only **37% strongly agree** that their security tooling is designed for these environments.

51%

Enterprises are largely divided on satisfaction with and confidence in their security stack. **Only 51% say their current SIEM is very effective at reducing mean time to detect and respond to threats.** And just 52% are very confident their current SIEM can scale to meet future security and cloud operations needs.

42%

Most organizations need tooling that supports a lean security team structure, **but only 42% say their current security stack does this very well.** Eighty-seven percent agree that unified security and monitoring tooling would improve team efficiency.

93%

Ninety-three percent of enterprise organizations use at least three security operations tools, and 45% use six or more. It's no surprise that over half (55%) of respondents report having too many point solutions in their security stack.

80%

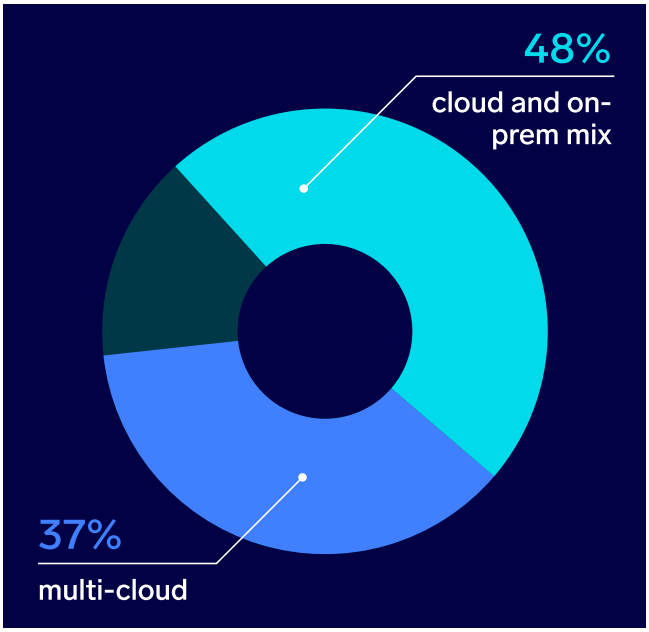
Eighty percent of enterprise organizations say security and DevOps use shared observability tools, but only 45% say the two teams are very aligned on tooling and workflows. One hundred percent say a unified platform for logs, metrics, and traces would be valuable for their security and DevOps teams.

The current state of security and cloud operations tooling

As enterprise organizations navigate digital transformation, many have adopted more mature cloud strategies and encountered rapidly changing application environments. Both hybrid and multi-cloud strategies give SOC managers more complicated environments to protect. As a result, they require the right tooling and sufficient resources to maintain security.

The current state of cloud operations tooling

Hybrid and multi-cloud strategies are the most common approaches among surveyed security leaders. Nearly half (48%) have adopted a cloud and on-premises mix, while 37% have a multi-cloud strategy. Those with a single cloud provider or a fully on-premises setup are in the minority.



The benefits of hybrid and multi-cloud strategies are numerous. They offer greater flexibility, preventing organizations from having to rely on a single provider for all workloads. In addition, both strategies create fewer vendor lock-in issues and make scaling simpler, which helps control costs.

In fact, cloud adoption is by far the most significant factor causing organizations to rethink and update their security and cloud operations tooling. Three-quarters (75%) of surveyed security leaders say cloud adoption is driving the need to modernize these tools.

75%

of leaders say cloud adoption drives modernization for security and cloud operations tooling

Yet it certainly isn't the sole driver of this decision. As development velocity increases and applications require more sophisticated features and integrations, respondents say factors like application complexity (56%) and DevOps acceleration (51%) prompt their organizations to update tooling.

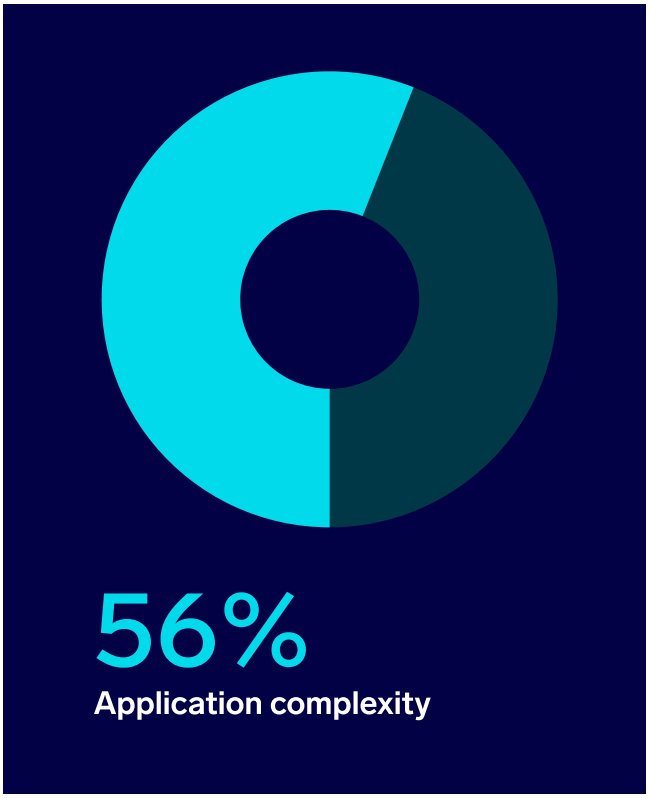
At the same time, adhering to governance standards and framework controls also drives the need for modern security and cloud operations tooling. Fifty-four percent of respondents say compliance requirements are a key factor in this decision.

However, cost and talent stand out as relatively minor factors. Only about a third of respondents cite either cost pressures (35%) or talent and resource constraints (35%) as drivers of the need for more modern tooling.

Most organizations are experiencing rapid change in microservices, containers, and other elements of their application environments. But the speed of change varies. Half (50%) of respondents say the speed of change is somewhat rapid, while a third (34%) say it's very rapid.

As application environments continue to change and cybersecurity threats continue to evolve, security leaders are likely to encounter new risks and challenges. The solution? Security and cloud operations tooling designed for modern application environments.

Other key considerations for modernizing tooling:



54%

Governance standards and compliance

51%

DevOps acceleration

35%

Cost pressures

35%

Talent and resource constraint

The current state of security tooling

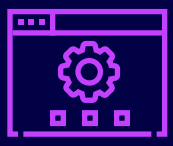
Most surveyed security leaders say their current security tooling is sufficient in today's environment. Altogether, 87% agree that their security tooling is designed for modern application environments.

Yet this statement isn't the vote of confidence it might seem at first glance. Only 37% of surveyed security leaders strongly agree with this statement—indicating that nearly two-thirds have at least some reservations about how their security tooling operates in today's application environments.

In some cases, these reservations may be tied to organizations' current cloud strategies. Most (88%) surveyed security leaders say that cloud-native platforms simplify their security operations, potentially because they expect their cloud providers to offer built-in security. But if they also need to secure on-premises platforms, their security operations may be unnecessarily complex.

This aligns with findings in the Sumo Logic 2025 Security Operations Insights report, which reveals that 90% of security operations leaders say supporting data sources from multi-cloud and hybrid-cloud environments is very or extremely important for their SIEM.

In other cases, however, these reservations may stem from shortcomings in organizations' current SIEM solutions. Just 37% of respondents say they have a cloud-native SIEM that offers scalability, unified telemetry, and built-in AI features with advanced analytics.



37%

of security leaders strongly agree that their security tooling is designed for modern application environments

37%

of security leaders have a cloud-native SIEM with built-in AI features, unified telemetry, and scalability

Instead, a hybrid SIEM solution is the most common setup among surveyed security leaders. Nearly half (46%) rely on a hybrid solution, combining on-premises capabilities with cloud-based analysis to monitor, detect, and respond to threats across environments.

Satisfaction with and confidence in existing security stacks

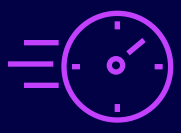
When asked to rate satisfaction with and confidence in their organizations' current SIEM solutions, some enterprise security leaders express misgivings. Most teams need tooling that enables them to do more with less, but their current solutions don't always check this box.

Efficacy of SIEM, log management, and security analytics tooling

Overall, 92% of organizations say their current SIEM is effective at reducing mean time to detect and respond to threats. Yet only half (51%) say it's very effective. The remaining half (49%) say it's only partially effective—or worse, not effective at all.

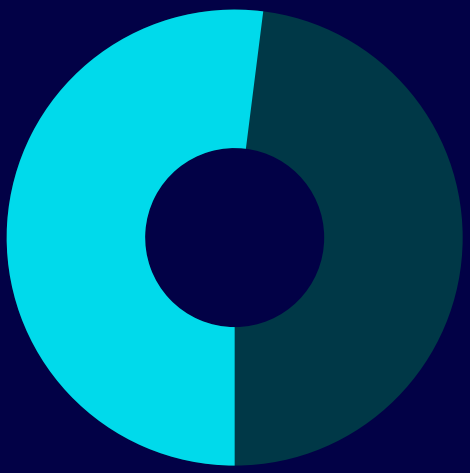
This nearly even split suggests that many organizations' SIEM platforms have substantial room for improvement. The 41% who say their solution is only somewhat effective have clear friction points that prevent them from declaring it to be very effective.

Organizations are similarly divided in terms of confidence in their SIEM's ability to scale. While 92% have confidence in their current SIEM, just over half (52%) of surveyed security leaders say they're very confident that their current SIEM can scale to meet future security and cloud operations needs.



51%

of security leaders say their current SIEM is very effective at reducing mean time to detect and respond to threats



52%

of security leaders are confident their SIEM can scale to meet future security and cloud operations needs

Just under half (48%) of respondents report a lower level of conviction. 40% are only somewhat confident that their SIEM can scale. To maintain a secure environment while scaling to analyze larger data volumes, organizations may have to consider an alternative SIEM solution that inspires confidence.

Survey respondents report similar success rates with their current log management and security analytics vendors. Just over half (52%) say they're very satisfied with these vendors, while 39% percent are only somewhat satisfied.

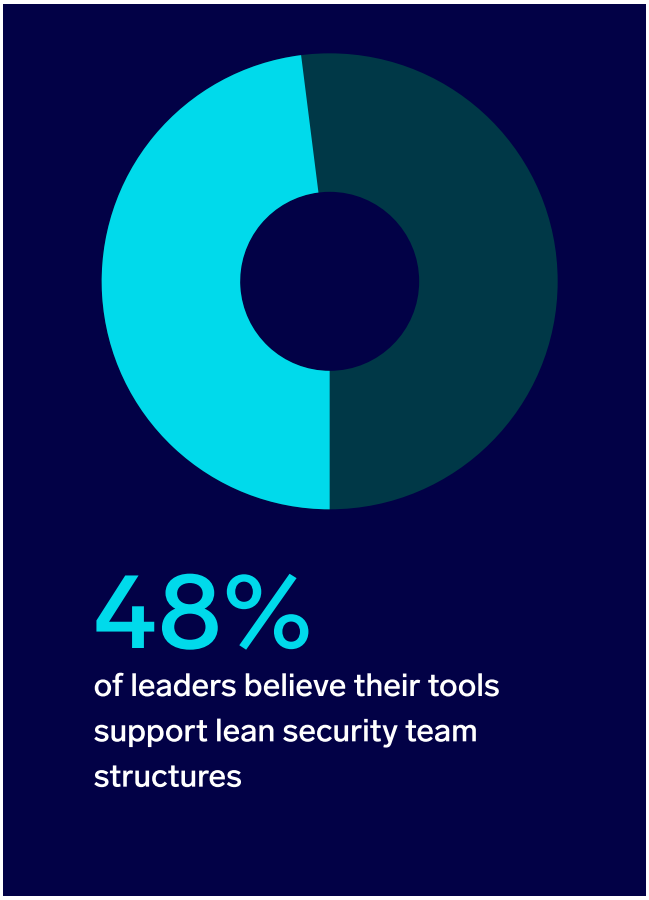
Those who are very satisfied with their current log management and security analytics vendors are more likely to highly rate their security solutions' capabilities. Over half (56%) of this segment strongly agrees that their security tooling is designed for modern application environments (versus 37% overall).

This indicates that those who have strong security log management and analytics tools are more likely to see their security tooling as ready for modern environments—including those with hybrid and multi-cloud strategies and rapidly scaling workloads.

Suitability for lean security teams

Security teams are becoming increasingly lean. Two-thirds of organizations report staffing shortages due to a combination of layoffs and budget cuts, the ISC2 **2024 Cybersecurity Workforce Study** reveals.

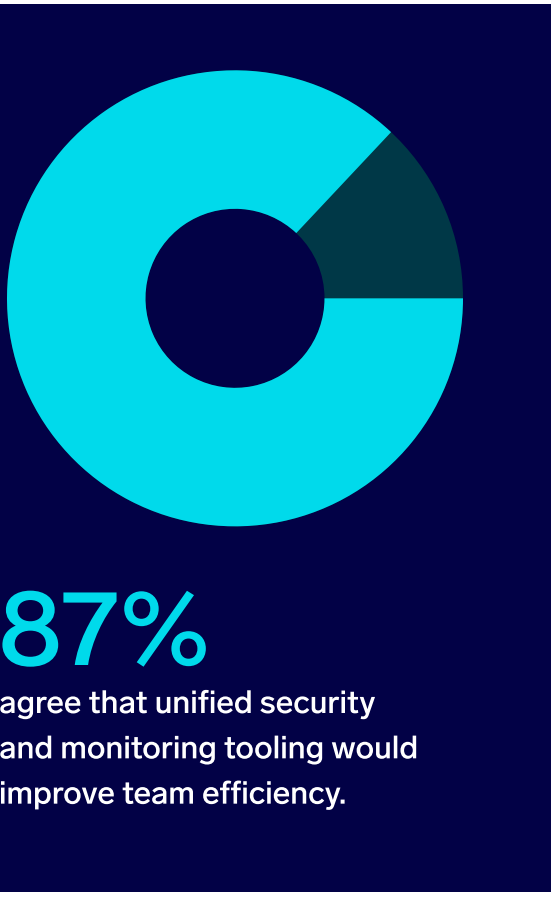
As a result, organizations need tooling that allows small teams to do more with less. But when asked how well their current tooling supports a lean security team structure, less than half (48%) of surveyed security leaders say "very well." Most (41%) of the remaining respondents say their tooling supports a lean structure only somewhat well.



> **Sumo Logic centralizes logs from all systems, giving security teams unified visibility. It enables real-time threat detection with automated alerts to speed incident response. Prebuilt compliance content streamlines audits and regulatory reporting. Advanced search and dashboards improve investigation and root cause analysis. Its cloud-native scalability supports modern, hybrid, and multi-cloud security operations.**
>
> **SecOps Manager,** Game Development Software Company

A unified platform that streamlines automation, AI/ML features, and scalability is increasingly essential for lean security teams. As the right skill sets continue to prove elusive, organizations must look beyond talent alone to meet security requirements.

Most respondents (87%) agree that unified security and monitoring tooling would improve team efficiency, with 42% expressing strong agreement with this statement.



> **Sumo Logic is instrumental in our security operations, proactively identifying potential threats through its Cloud SIEM Insights. Its capabilities have transformed our approach to security, allowing us to be more efficient and impactful with such a small team.**
>
> **Jessica Herold** Flock Safety

Considerations for SIEM platforms and cybersecurity tools

Most enterprise security leaders prioritize AI/ML features and real-time visibility in SIEM platforms and cybersecurity tools. However, most evaluate vendors in their security stacks relatively infrequently, likely due to vendor lock-in. As a result, they may miss opportunities to access these advanced capabilities.

Automation and AI usage

When it comes to threat detection and response, automation is table stakes for security leaders. 70% of respondents say they've fully or mostly automated their threat detection and response process, with 25% reporting it's fully automated. Those who rely on a mostly or fully manual process are in the extreme minority.

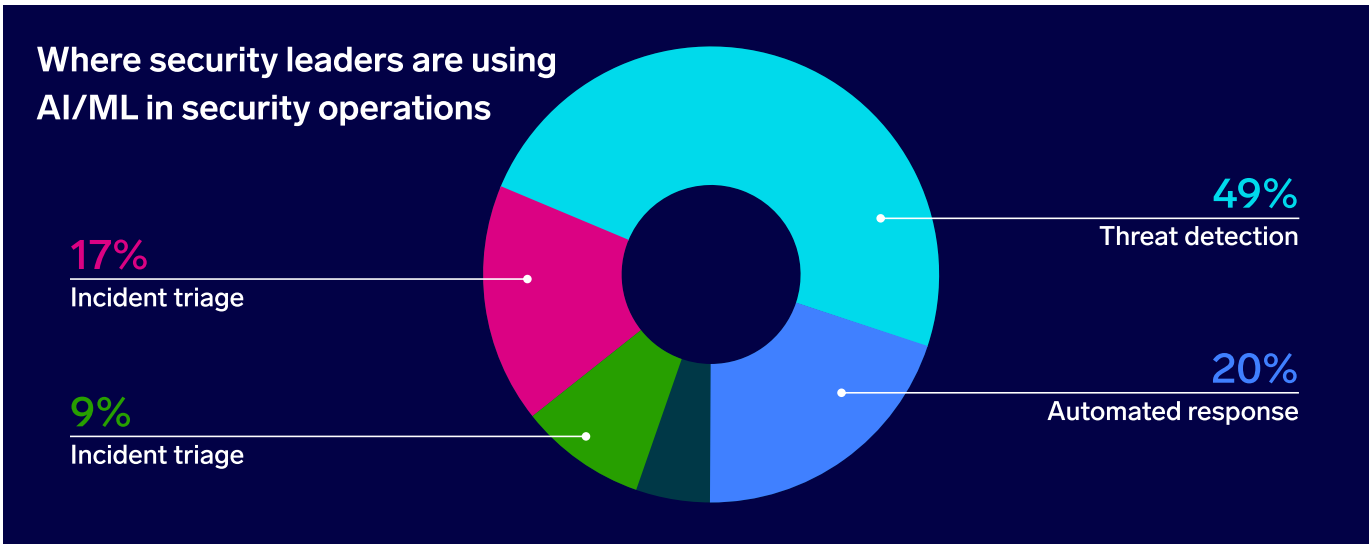
However, AI adoption isn't as widespread. While 96% of surveyed security leaders say they've adopted AI, their use cases are relatively basic.

This contradicts the marketing narratives that suggest most security leaders have widely adopted AI throughout their security and cloud operations workflows.

96%

of security leaders have adopted AI to some extent

Nearly half (49%) of respondents use AI/ML for threat detection. Other AI/ML use cases include automated response (20%) and anomaly detection (17%). Incident triage (9%) is the least commonly cited use case for AI/ML.



Of those who use AI/ML, the majority are optimistic about the value this technology creates—even though their current use cases are relatively limited. 90% of these respondents say AI/ML is extremely or very valuable in reducing alert fatigue and improving detection accuracy. Half (49%) say it's extremely valuable.

This aligns with findings in the Sumo Logic 2025 Security Operations Insights report, which reveals 90% of respondents say AI is extremely or very important in their decision to purchase a new security solution. As security teams become leaner, time-saving technology like AI becomes increasingly important.

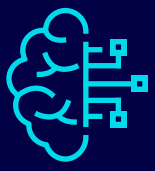
Real-time capabilities

When it comes to essential features for security tooling, AI and automation are only the beginning. The data suggests that it's hard to overstate the importance of real-time threat detection, analytics, and visibility.

When evaluating modern SIEM platforms, most organizations prioritize both real-time analytics and AI/ML features. Ninety-six percent of surveyed security leaders use AI/ML in their security operations, and 61% say AI/ML capabilities are a top priority in a SIEM platform.

90%

of security leaders say AI/ML is valuable in reducing alert fatigue and improving detection accuracy



61%

of security leaders prioritize AI/ML capabilities in a SIEM platform

With [Sumo Logic's] powerful query functions coupled with intuitive AI integration and Mobot (the Dojo AI at your side), nothing is impossible—plus the ability to automate the reduction of noise within the platform to allow for more streamlined insights where and when you need it.

Brandon Hewgill, Head of Information Security

PATRIANNA

Other important factors include real-time analytics (63%), cloud-native design (58%), and scalability (55%). Budget is also a major factor when considering a new SIEM platform. Over half (58%) of respondents say cost efficiency is a key factor in this decision-making process.

Real-time threat detection minimizes the time cyberattacks have to do damage, making this capability crucial for most security leaders. Eighty-nine percent of respondents agree that real-time threat detection is a top priority for their team, with half (51%) strongly agreeing with this statement.

In addition, 93% of surveyed security leaders say it's extremely or very important to have real-time visibility across the organization's entire environment—including cloud, applications, and infrastructure. More than half (54%) say this is extremely important.

89%

of security leaders rank real-time threat detection as their top priority

93%

of security leaders say it's extremely or very important to have real-time visibility across the organization's entire environment

> **Sumo Logic plays a critical role in our incident detection and investigation by providing timely alerts and linking relevant log data to each incident. This helps us respond faster and minimize customer impact. The platform's flexibility allows us to scale and adapt as our monitoring needs evolve.**
>
> VP Platform
>
> boku

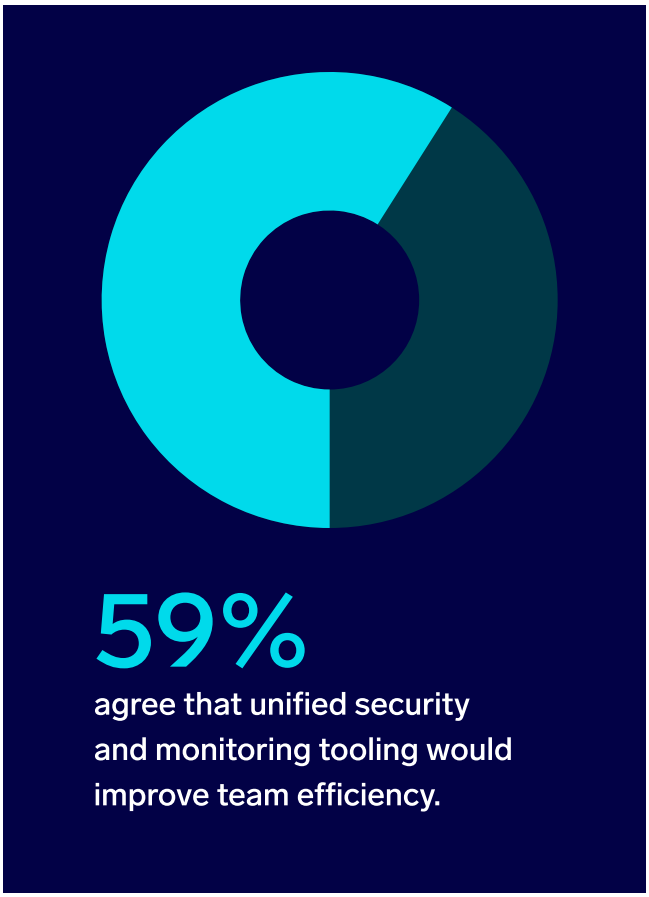
Security vendor review frequency

For many organizations, adopting new cybersecurity tooling with AI/ML and real-time capabilities may be easier said than done. Most organizations review and consolidate their security stacks relatively infrequently.

Only 41% of respondents report consolidating or evaluating vendors in their security stack quarterly. The majority (59%) review security vendors twice per year at most, while a quarter (26%) do so annually.

Those who say they're very satisfied with their current vendor for log management and security analytics are more likely to consolidate or evaluate vendors in their security stack more often. Over half (54%) of this segment does so quarterly, suggesting that more frequent evaluations may lead to more robust cybersecurity capabilities.

However, financial incentives to buy multiple products from a single vendor may affect these patterns. The belief that their solutions may work better together may drive some of this reluctance to review security vendors more frequently.



The case for a unified SOC platform powered by telemetry

While SIEM platforms are typically designed for threat detection, investigation, and response (TDIR), enterprise security leaders often expect these solutions to do more. When their SIEMs don't deliver, they often resort to investing in additional software. This tends to lead to sprawling tech stacks, disconnected tools, and strained budgets.

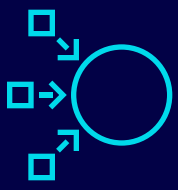
SIEM capabilities and limitations

When it comes to SIEM features, threat detection isn't the most common capability cited by surveyed security leaders. More than three-quarters (78%) report using their SIEM for cloud security monitoring, while 72% use its threat detection capabilities.

In addition, 70% of respondents use their SIEM for security orchestration, automation, and response (SOAR), while 62% use it for log management. On average, respondents report using 4.1 SIEM capabilities. Over a third (35%) report using five or more capabilities.

To leverage these capabilities, most organizations rely on their SIEM to ingest multiple data sources. The most common among survey respondents include identity and access logs (71%), cloud audit logs (69%), application logs (66%), and infrastructure logs (64%).

On average, respondents report ingesting 4.14 data sources into their SIEM. Over a third (36%) say they use their SIEM to ingest five or more data sources.



36%

of security leaders say their SIEM ingests five or more data sources

Organizations that have only one or two sources may opt to evaluate the data in native platforms rather than investing in a SIEM. But the more complex your stack becomes and the more data sources you need to monitor, the more you need a solution that can ingest data from a wide range of sources.

> **We needed appropriate SaaS visibility and logging, and Sumo Logic was one of the few solutions offering a great Terraform provider and hosted collector. Sumo Logic's innovative approach suits our structure well and has proven useful for us.**
>
> **Sajeeb Lohani,**
> Global Technical Information Security Officer
> bugcrowd

Inflated security tech stacks

When they need multiple tools to ingest various data sources or monitor different parts of the stack, security leaders often end up purchasing additional tools to bridge the gap. In fact, 93% of respondents have at least three tools in their security operations stack. Nearly half (45%) use six or more security operations tools, and 10% use more than ten.

Organization size has some effect on tool usage, with larger companies more likely to use more tools. While 40% of organizations with 500 to 999 employees use six or more tools, 51% or those with 10,000 or more employees use six or more tools.

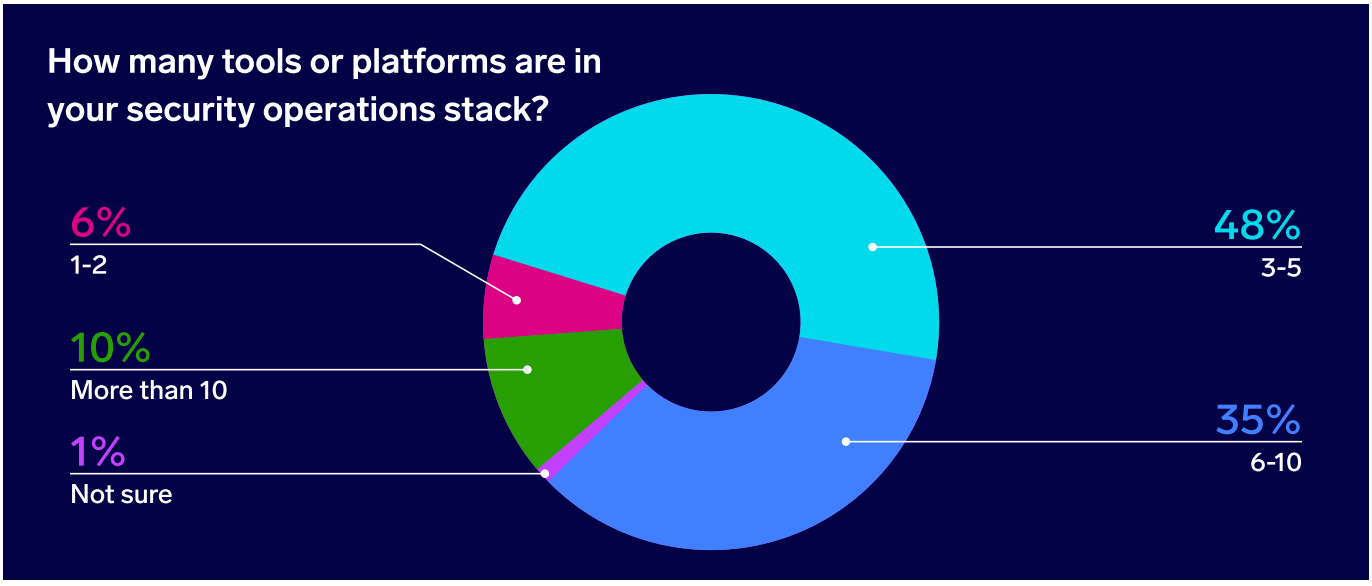
In many cases, these tools don't talk to each other. More than half (55%) of respondents agree or strongly agree that they struggle with too many point solutions in their security stack. Siloed tools can quickly create more noise than signal, leading to alert fatigue.

When asked about their biggest pain points with their current security operations tooling, 40% of respondents say they're juggling too many siloed tools. When tools don't share data, they make it difficult to assess threats across the environment or see the full attack chain. This creates security gaps that attackers can easily exploit, slowing incident response.

However, the most common problem among surveyed security leaders is budget. Nearly two-thirds (63%) say high operational cost is their biggest pain point. This suggests that investing in too many tools is creating both operational issues and budget constraints.

63%

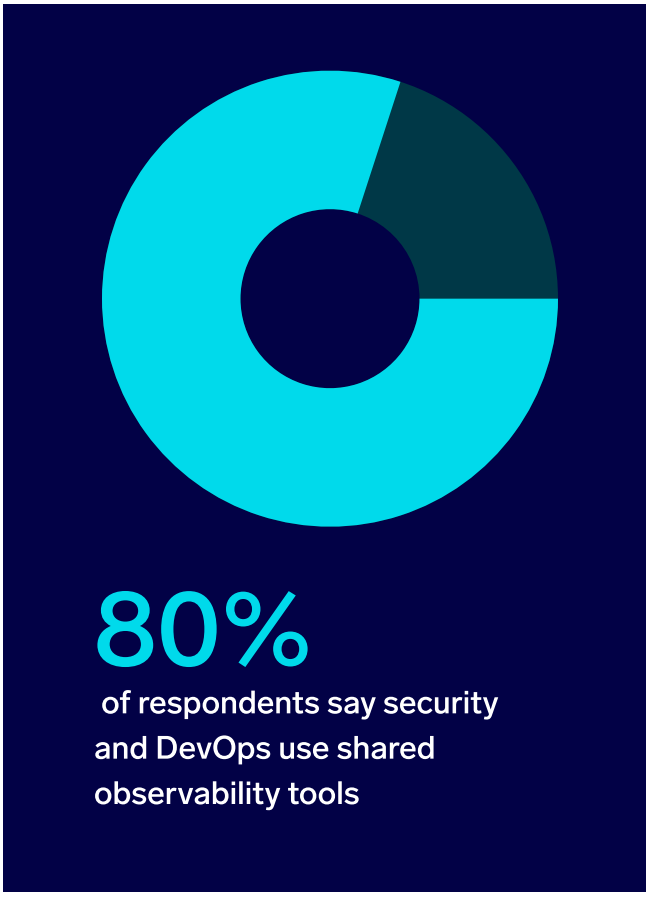
of security leaders say operational cost is their biggest pain point



Unified security and cloud operations to resolve misalignment

Misalignment across security and DevOps teams likely exacerbates these issues—and fragmented ownership of cloud operations tooling doesn't help either. There's no clear standard for ownership among respondents. While 37% say IT owns this tooling, 16% report security owns it and 15% say DevOps owns it.

While most (80%) respondents say security and DevOps use shared observability tools, less than half (45%) say the two teams are very aligned on tooling and workflows. A similar percentage (43%) say the two teams are only somewhat aligned.



The data suggests a connection between aligned security and DevOps teams and success with security and cloud operations tooling. Of the teams that say they're very aligned:

84%

are very satisfied with their current vendor for log management and security analytics (versus 52% overall)

82%

say their SIEM is very effective at reducing mean time to detect and respond to threats (versus 51% overall)

81%

are very confident their current SIEM can scale to meet future needs (versus 52% overall)

62%

strongly agree that their security tooling is designed for modern application environments (versus 37% overall)

Given the widespread team alignment and software ownership issues, it's no surprise that virtually all respondents say a unified security and cloud operations platform would be beneficial. All (100%) surveyed security leaders say a unified platform for logs, metrics, and traces would be valuable for their security and DevOps teams. Just over half (51%) say a unified platform would be extremely valuable, and 40% say it would be very valuable.

100%

of security leaders say a unified platform for logs, metrics, and traces would be valuable for security and DevOps teams

As we continuously change our business and add new services for our customers, website updates, and different integrations to produce sales, with the power of Sumo Logic within our toolbox, we're confident that we can ingest, report, and search logs. We can also build reporting from any of those third parties, whether they're currently supported or not by Sumo Logic, because we can throw anything at it and normalize the data.

John Sacchetti, Director of Cybersecurity and Networking

DXL

Conclusion

Enterprise security leaders are understandably overwhelmed. As application environments evolve and cyberattacks become more sophisticated, security teams are becoming leaner, expected to do more with less. As AI continues to complicate the threat landscape, it adds yet another technology that needs to be monitored, secured, and used in security.

Only 37% of security leaders strongly agree that their security tooling is designed for these rapidly changing environments. Ninety-three percent are already using three or more security operations tools, and over half (55%) already have too many point solutions in their security stack.

The solution isn't a larger security tech stack with more siloed tools. Instead, it's a unified platform that acts as a single source of truth for DevSecOps, providing real-time insights and visibility across the entire environment.

For over 15 years, Sumo Logic has provided that single source of truth. Designed for cloud-native and hybrid environments, Sumo Logic handles unstructured logs, combines security and log analytics data, and scales easily.

As an integrated Intelligent Security Operations Platform powered by exabyte-scale log analytics and cloud-native architecture, Sumo Logic aligns security and DevOps, creating a collaboration between security and observability.

See Sumo Logic Cloud SIEM in action.

Learn more →

Methodology and demographics

To create this report, Sumo Logic commissioned UserEvidence to conduct an independent market survey of 506 security leaders and practitioners in October 2025. The research sample was vendor-neutral and didn't target Sumo Logic or UserEvidence customers, although they weren't excluded from participating.

Most survey respondents (81%) were security leaders at the manager or director level, primarily information security managers or security managers (31%) were directors of IT security manager risk (21%). The remaining 19% were security practitioners.

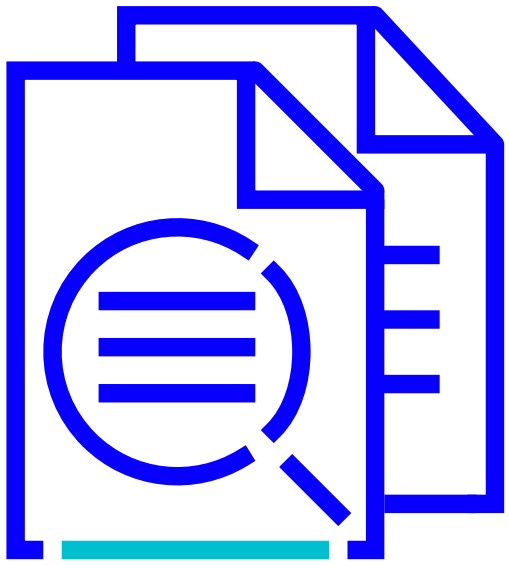
All survey respondents represented organizations with at least 500 employees. The largest segments were from organizations with 500 to 999 employees (40%) and organizations with 1,000 to 4,999 employees (31%).

Most survey respondents (72%) worked for organizations in the IT industry. The rest were from organizations in the manufacturing (7%), financial services (7%), healthcare (4%), and other industries.

About UserEvidence

UserEvidence is a software company and independent research partner that helps B2B technology companies produce original research content from practitioners in their industry. All research completed by UserEvidence is verified and authentic according to their research principles:

Identity verification, significance and representation, quality and independence, and transparency. All UserEvidence research is based on real user feedback without interference, bias, or spin from our clients.



UserEvidence research principles

1 Identity verification

In every study we conduct, UserEvidence independently verifies that a participant in our research study is a real user of a vendor (in the case of Customer Evidence) or an industry practitioner (in the case of Research Content). We use a variety of human and algorithmic verification mechanisms, including corporate email domain verification (i.e., so a vendor can't just create 17 Gmail addresses that all give positive reviews), and pattern-based bot and AI deflection.

2 Significance and representation

UserEvidence believes trust is built by showing an honest and complete representation of the success (or lack thereof) of users. We pursue statistical significance in our research, and substantiate our findings with a large and representative set of user responses to create more confidence in our analysis. We aim to canvas a diverse swatch of users across industries, seniorities, personas—to provide the whole picture of usage, and allow buyers to find relevant data from other users in their segment, not just a handful of vendor-curated happy customers.

3 Quality and independence

UserEvidence is committed to producing quality and independent research at all times. This starts at the beginning of the research process with survey and questionnaire design to drive accurate and substantive responses. We aim to reduce bias in our study design, and use large sample sizes of respondents where possible. While UserEvidence is compensated by the vendor for conducting the research, trust is our business and our priority, and we do not allow vendors to change, influence, or misrepresent the results (even if they are unfavorable) at any time.

4 Transparency

We believe research should not be done in a black box. For transparency, all UserEvidence research includes the statistical N (number of respondents), and buyers can explore the underlying blinded (de-identified) raw data and responses associated with any statistic, chart, or study. UserEvidence provides clear citation guidelines for clients when leveraging research that includes guidelines on sharing research methodology and sample size.

About Sumo Logic

Sumo Logic, Inc. helps make the digital world secure, fast, and reliable by unifying critical security and operational data through its Intelligent Operations Platform. Built to address the increasing complexity of modern cybersecurity and cloud operations challenges, we empower digital teams to move from reaction to readiness—combining agentic AI-powered SIEM and log analytics into a single platform to detect, investigate, and resolve modern challenges. Customers around the world rely on Sumo Logic for trusted insights to protect against security threats, ensure reliability, and gain powerful insights into their digital environments. For more information, visit www.sumologic.com.