exabeam™

RESEARCH REPORT

From Hype to Help: How AI is (Really) Transforming Cybersecurity in 2025

AI is No Longer a Future Concept in Cybersecurity

EXECUTIVE SUMMARY

AI is no longer a future concept in cybersecurity — it's here, embedded in day-to-day operations. But while adoption is rising, agreement on its effectiveness is not. The cybersecurity workforce is divided: executives are all-in on AI's potential, while analysts remain unconvinced it's delivering where it matters.

71% of executives say AI has significantly improved their team's productivity. Only 22% of analysts agree. This stark gap reflects more than just perception — it reveals a growing divide between strategic intent and operational reality. Analysts closest to the tools cite hallucinations, false positives, and added complexity. For them, AI isn't replacing manual work — it's reshaping it, often without reducing the burden.

This tension is also reshaping security teams. Over half of surveyed organizations have already restructured in response to AI adoption. Yet the change isn't about reducing headcount — it's about rethinking roles. New responsibilities are emerging around automation oversight, AI governance, and faster decision-making. Teams aren't shrinking; they're adapting.

The most tangible value AI offers for cybersecurity today is in threat detection, investigation, and response (TDIR) — where speed and signal clarity matter most. AI-driven tools are helping reduce the time it takes to identify and investigate threats, offloading repetitive analysis tasks and freeing up humans to act faster and more confidently.

Still, adoption and sentiment vary widely across regions. Organizations in India, the Midde East, Turkey and Africa (IMETA) report significantly higher productivity improvements than those in North America — suggesting that context, urgency, and infrastructure readiness all influence success. Meanwhile, trust in AI autonomy remains low — particularly among analysts. But trust isn't the headline. Effectiveness is. The priority today is clear: get to better outcomes, faster. AI should support human-led decisions, not replace them. When the tools reduce noise and improve speed without increasing risk, trust will follow.

This report underscores a central truth: AI's role in security is real, growing, and disruptive. But its success hinges on bridging the gap between leadership expectations and analyst realities. Organizations that ground their AI strategies in operational impact — not just high-level optimism — will be best positioned to lead the next phase of security evolution.

Contents

Key Findings

A security industry in transition

While AI adoption is widespread, its impact depends heavily on who you ask, where they work, and how closely they interact with the tools.

> “AI is streamlining security operations and reducing costs. The more we integrate AI into our SOC, the stronger our security posture becomes.”

SECURITY EXECUTIVE

> “It’s not that we don’t want to use AI — we just don’t trust it to work reliably without us watching it.”

SECURITY ANALYST

Bridging the AI Perception Gap: Executive Vision vs. Analyst Reality

Across the cybersecurity industry, enthusiasm for AI is high, but how that translates into real impact depends on who you ask.

71% of executives believe AI has significantly improved their team's productivity.

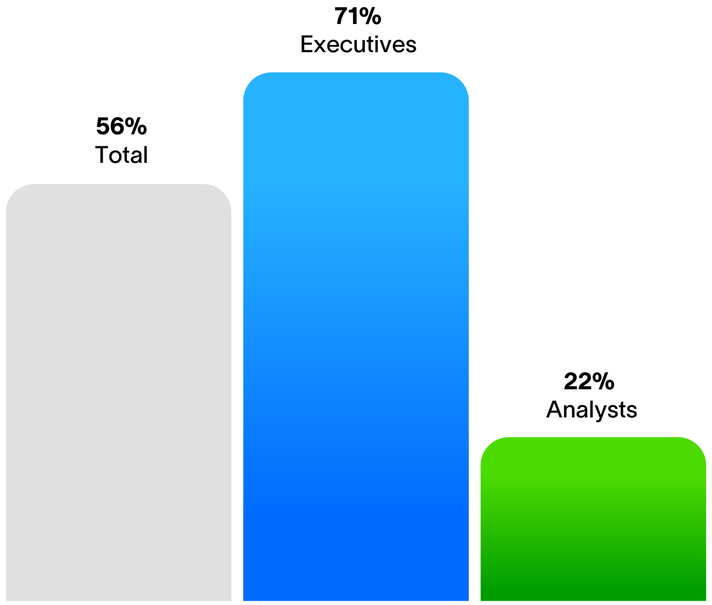
Only 22% of analysts say the same — those who use the tools daily are far more skeptical.

38% of executives are willing to let AI act independently in cyber defense.

Only 10% of analysts trust AI to act autonomously — highlighting a significant gap in trust, not just in effectiveness.

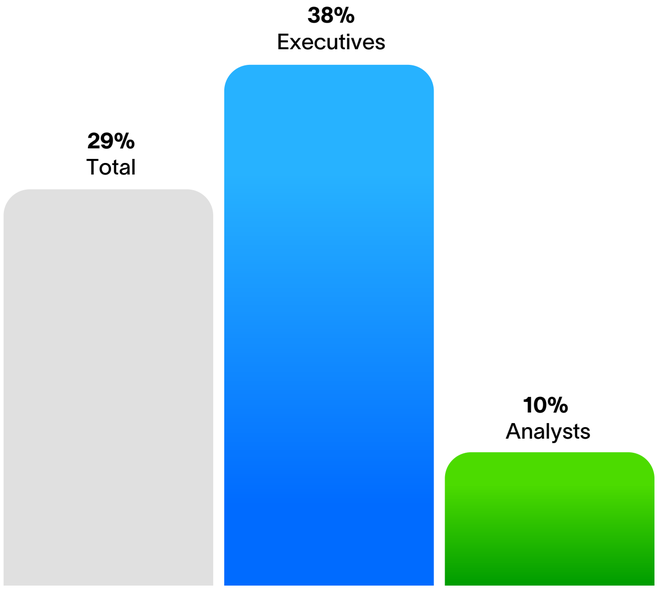
This stark contrast reveals that many organizations may be underestimating the challenges of AI implementation — particularly at the operational level.

Respondents Say AI Significantly Improved Security Team Productivity



% Respondents by role

Organizations Willing to Let AI Act Independently



% Respondents by role

... many organizations may be underestimating the challenges of AI implementation — particularly at the operational level.

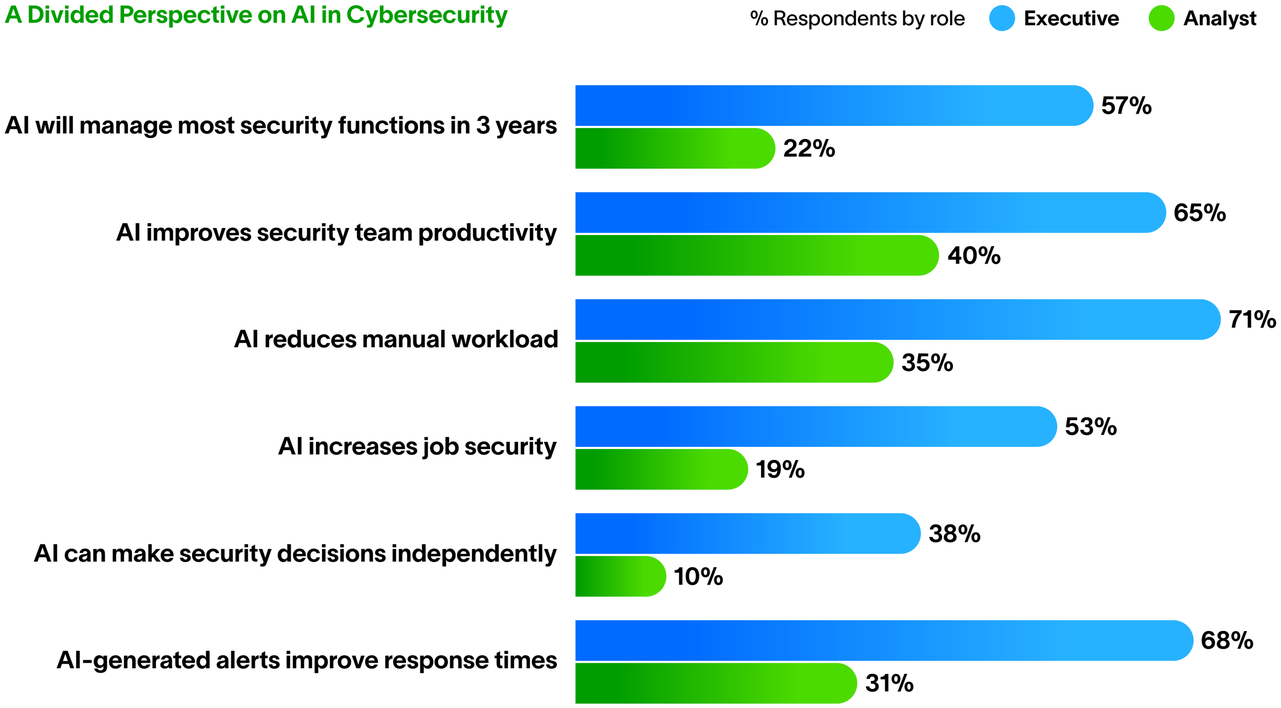
The Impact of AI

AI is widely seen as a transformational force in cybersecurity, yet security professionals at different levels of an organization perceive its impact very differently. While executives focus on AI's ability to cut costs, improve efficiency, and enhance security outcomes, analysts on the front lines highlight concerns about increased alert fatigue, false positives, and AI's need for human oversight.

Executives view AI as a long-term investment that optimizes operations and enhances security strategies, while analysts remain cautious, emphasizing real-world execution challenges.

This disconnect underscores the importance of aligning AI implementation strategies with operational realities, ensuring that security teams receive the proper training, tools, and support to fully leverage AI's potential.

A Divided Perspective on AI in Cybersecurity



Executives' Perspective

- AI reduces costs and increases efficiency
- AI will replace manual tasks in the SOC

Analysts' Perspective

- AI increases workload through false positives
- AI still requires human oversight

Where AI Delivers Today: Threat Detection, Investigation, and Response

AI enhances security teams' efficiency by automating repetitive tasks, streamlining workflows, and improving response times. Threat detection, investigation, and response (TDIR) stands out as AI's most effective application area: shortening time to insight, not making decisions for humans.

56% of security teams report that AI has improved their productivity.

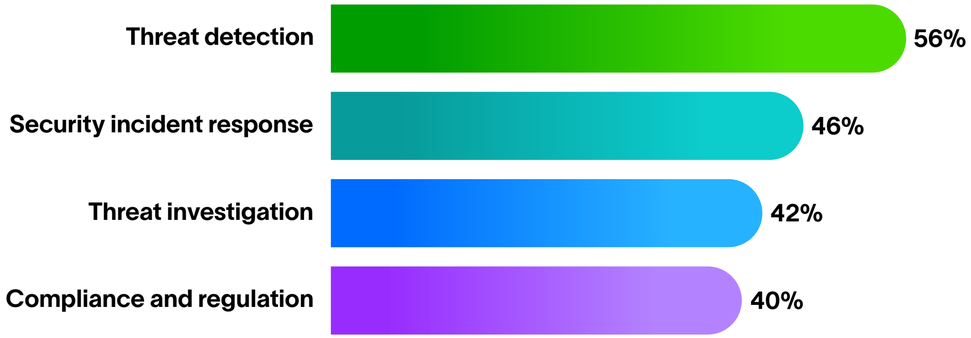
AI adoption is most potent in threat detection, incident response, and threat investigation.

56% of security professionals trust AI for threat detection.

AI-powered solutions are enhancing:

- Anomaly detection, by spotting behavioral deviations faster than human analysts.
- Incident response automation, by reducing the mean time to detect (MTTD).
- User behavior analytics, by helping identify insider threats.

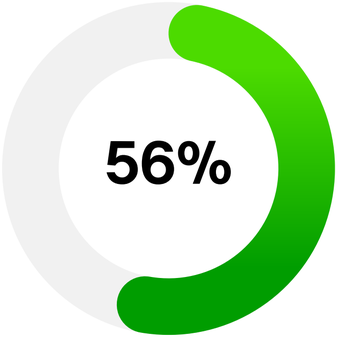
Security Functions Organizations are Currently Augmenting with AI



AI

56% of security teams report that **AI has improved their productivity.**

56% of security professionals **trust AI for threat detection.**



Security Teams Are Restructuring

41% of security leaders report that AI already delivers measurable cost savings, underscoring the financial incentives driving structural changes.

AI is reshaping security teams' composition, leading to workforce reductions and expansions in AI-specific roles.

More than half of the companies surveyed have adjusted their security team structures due to AI integration.

37% have reduced security staff, citing AI-driven automation as a key factor.

18% have expanded their teams, hiring for AI governance, automation, and data security roles.

How Organizations are Tracking the ROI of AI Cybersecurity Tools

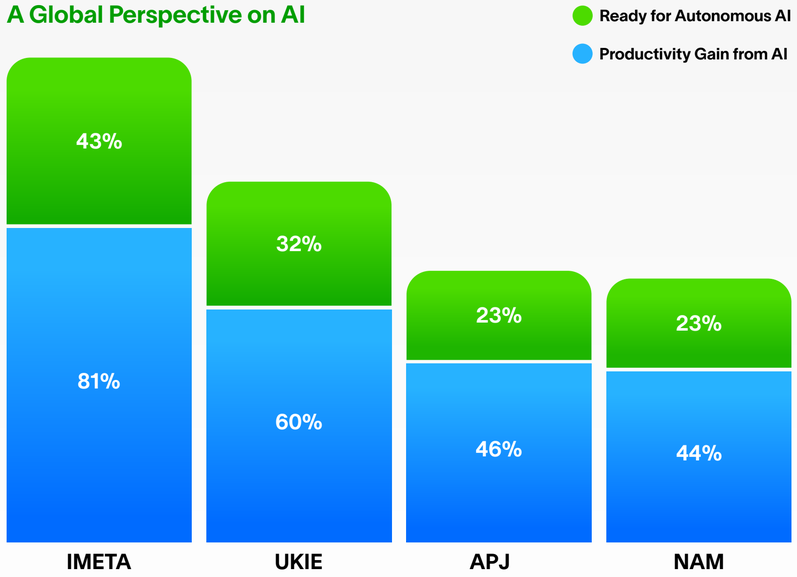
AI isn't just a tool — it's a catalyst for transformation. Security teams are evolving fast, with roles shifting toward automation, governance, and data integrity. To keep up with the pace and complexity of modern threats, teams must adopt agentic AI that can reason, act, and adapt on their behalf."

Gabrielle Hempel
Security Operations Strategist | Exabeam

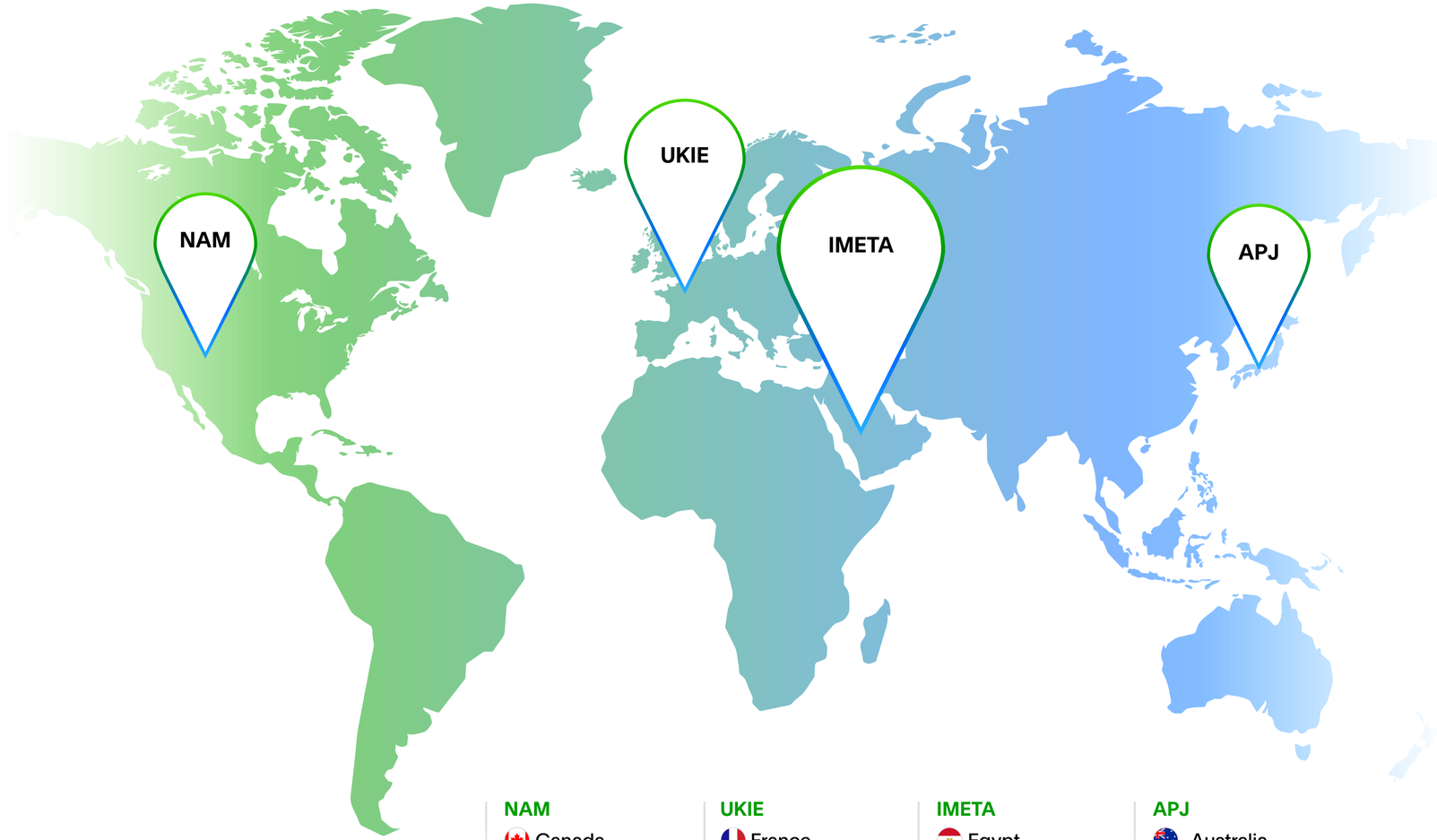
Adoption Isn’t Equal Across Regions

The report reveals stark regional disparities in AI’s impact on productivity. Organizations in IMETA are seeing the most significant gains in productivity, suggesting faster and more effective adoption of AI compared to regions like North America. This highlights how emerging markets may be leveraging AI as a strategic advantage.

A Global Perspective on AI



% Respondents by region



NAM
- Canada
- United States

UKIE
- France
- Germany
- Ireland
- Netherlands
- United Kingdom

IMETA
- Egypt
- India
- Saudi Arabia
- Turkey

APJ
- Australia
- Japan
- Singapore

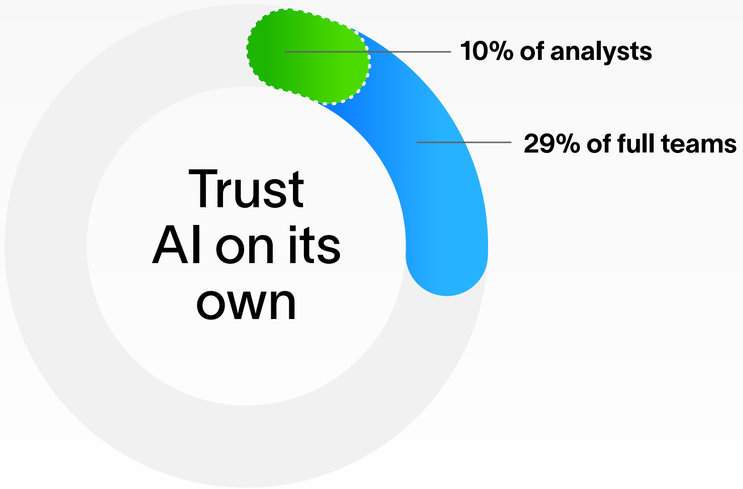
The Trust Paradox: It’s Not About Autonomy — Yet

AI is being adopted not to replace judgment, but to reduce overhead. As output improves, trust will follow. But it won’t lead.

Only 29% of teams fully trust AI on its own.

Among analysts, that number drops to 10%.

But autonomy isn’t the goal right now. Performance is.



> “Artificial intelligence should serve as a cognitive ally in cybersecurity — enhancing analyst capabilities while preserving the human element of trust, accountability, and strategic oversight.”

Steve Povolny
Senior Director, Security Research | Exabeam

EXPERT INSIGHT

How to Move Forward with AI

Steve Wilson Chief AI and Product Officer | Exabeam

"The data in this report makes one thing clear: there's a disconnect between the AI optimism held by CISOs and executives, and the operational frustration still felt by analysts. That's because much of the AI on the market today isn't moving the needle where it counts — it's reactive, superficial, and still demands too much handholding.

But that's starting to change. Agentic AI is no longer a future concept — it's here. This new wave of AI doesn't wait for commands. It's proactive, takes initiative, and drives investigations forward without needing constant input from an analyst.

Organizations that want to close the gap between vision and reality need to start adopting agentic AI now. It's the key to transforming overwhelmed teams into high-functioning, proactive security operations centers. By offloading the grunt work and surfacing insights at machine speed, agentic AI empowers analysts to focus on what's truly important — responding to the threats threats that matter most."

Conclusion

Bridging strategy and execution

As AI continues to reshape the cybersecurity landscape, organizations must reconcile leadership ambition with operational execution. Successful strategies will be defined by their ability to align AI capabilities with front-line needs, involve analysts in deployment decisions, and prioritize outcomes over hype.

Close the Gap, Realize the Value

AI rapidly transforms security teams, increases efficiency, and reshapes workforce structures. From streamlining workflows to reducing manual tasks, AI is unlocking new levels of efficiency across the cybersecurity function. It also redefines workforce dynamics, prompting organizations to restructure roles and invest in new skills.

However, the path to successful AI adoption is not without friction. A clear disconnect exists between leadership expectations and the practical concerns of frontline analysts. Bridging this divide is essential to harnessing AI's full potential.

To move forward confidently, organizations must implement the following measures:

- **Align AI capabilities with operational needs**
- **Involve front-line teams in tool selection and deployment**
- **Focus on performance, not promises**
- **Invest in skills, not just platforms**

The next phase of AI in cybersecurity won't be about speculation. It'll be measured by the time it saves, the complexity it reduces, and the outcomes it improves.

The future of AI should tangibly empower security teams to focus on the work that requires human intuition and creativity without introducing new risks.

METHODOLOGY

This report is based on research conducted by Sapio Research on behalf of Exabeam during February and March 2025. The survey represents a global audience of 1,000 cybersecurity professionals, including analysts, security team leads, and executive decision-makers across key sectors such as technology, financial services, manufacturing, healthcare, retail, and government. Respondents were required to either work directly in a cybersecurity function or be responsible for managing security teams.

The organizations represented varied in size, with a significant portion of participants coming from large enterprises with over 10,000 employees. To reflect the diversity of AI applications in use today and ensure that the data captured real world perceptions of AI's role in security operations across various contexts, the survey intentionally left the definition of "AI" open ended — allowing respondents to interpret it as machine learning, generative AI, agentic AI, or other AI-driven technologies relevant to their experience.

About Exabeam & Sapio Research

Exabeam and Sapio Research provide a comprehensive view of how AI is transforming the cybersecurity workforce — illuminating the opportunities, challenges, and strategic imperatives facing modern security teams.

exabeam™

Exabeam is a leader in intelligence and automation that powers security operations for the world's smartest companies. As a global cybersecurity innovator, Exabeam provides industry-proven, security-focused, and flexible solutions for faster, more accurate threat detection, investigation, and response (TDIR). Cutting-edge technology enhances security operations center performance, optimizing workflows and accelerating time to resolution. With consistent leadership in AI innovation and a proven track record in security information and event management (SIEM) and user behavior analytics, Exabeam empowers global security teams to combat cyberthreats, mitigate risk, and streamline operations.

SAPIO RESEARCH

This report was produced in partnership with Sapio Research, a global market research and insights agency known for its B2B and technology research expertise. Sapio designed and conducted the survey that underpins this report, gathering responses from cybersecurity professionals across industries and geographies. Their rigorous methodology and deep understanding of the security landscape ensured the findings reflect strategic leadership perspectives and the practical realities front-line security teams face.

Learn more about Exabeam at exabeam.com →