exabeam™

RESEARCH REPORT

From Adoption to Accountability: The New Economics of AI in Cybersecurity

EXECUTIVE SUMMARY

From Adoption to Accountability: The New Economics of AI in Cybersecurity

To understand how organizations are approaching cybersecurity investment in the age of AI, Exabeam partnered with Sapio Research to survey 750 IT decision-makers responsible for security across 12 countries. The research focused on 2026 budget planning, AI adoption strategies, investment justification challenges, and how organizations are measuring the value of their security programs.

The findings reveal that cybersecurity budgets are surging heading into 2026, with 95% of organizations increasing security spending and 74% reporting double-digit growth. Yet rather than building larger teams, organizations are channeling investments into AI-driven transformation that's fundamentally reshaping how security operations function, how resources are deployed, and how value is measured.

At the center of this shift lies a critical challenge: AI and automation are simultaneously the top driver of budget increases (44%) and the investments most at risk if budgets tighten (also 44%). Security leaders face mounting pressure to adopt AI quickly, yet many struggle to articulate its business value to boards and executive stakeholders. The result is an industry racing ahead on transformation while falling behind on measurement, communication, and strategic alignment.

This disconnect between innovation and justification isn't just an internal reporting challenge; it's a vulnerability that could undermine sustained investment. While 87% of security leaders express confidence in delivering business value, 30% cite lack of board understanding of the link between cybersecurity investment and business resilience as their biggest challenge in defending spend. Organizations are receiving mandates to invest in AI, but they lack the frameworks to measure and communicate its value effectively.

The organizations that succeed in 2026 and beyond will be those that not only deploy AI effectively but demonstrate convincingly and quantitatively that it's delivering the security outcomes and business value that justify the spend. This requires new approaches to measuring success, new narratives for communicating value, and strategic alignment between security operations and business leadership.

Contents

Key Findings

95% of organizations are increasing cybersecurity budgets in 2026, with 74% seeing double-digit growth

AI is the top budget driver (44%) but also the #1 target for cuts if budgets tighten (44%) and the hardest investment to justify (32%)

87% of security leaders are confident their investments deliver business value, yet 30% struggle with board understanding of the cybersecurity-business resilience link

92% say AI is already improving or will improve security operations by the end of 2026, with a focus on threat detection (38%), workforce productivity (38%), and automated response (35%)

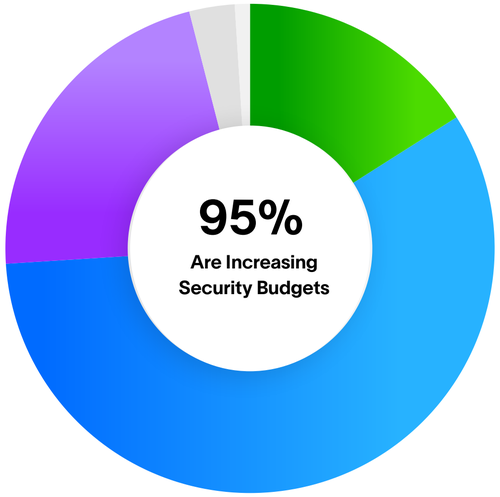
Regional variations are significant, Saudi Arabia shows the highest confidence in AI (75%) while Japan (27%) and Netherlands (27%) are more cautious

Unprecedented Budget Growth

The cybersecurity funding environment for 2026 represents a significant shift from recent years' budget constraint narratives. **With 95% of organizations increasing their security budgets and 74% seeing double-digit growth,** this expansion is being driven by technology capability investments rather than traditional headcount expansion.

AI and automation lead as the primary catalyst, reflecting both the technology's potential to transform security operations and executive-level mandates to modernize. However, this AI-driven budget growth introduces new challenges around value measurement and stakeholder communication that organizations are still learning to navigate.

Current Outlook for Cybersecurity Budgets in 2026



16%
Increasing by more than 20%

58%
Increasing by 10-20%

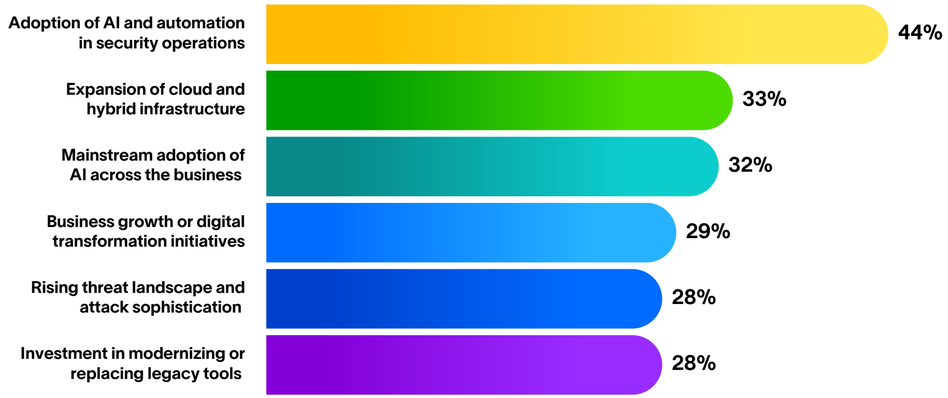
22%
Increasing by less than 10%

3%
Staying flat (±1%)

1%
Decreasing by less than 10%

(See appendix question A for complete data)

Primary Drivers of Budget Increases



(See appendix question B for complete data)

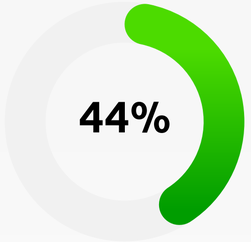
> **Security leaders are caught between executive pressure to modernize with AI and the reality that they don't yet have the frameworks to measure and communicate its value. Budget increases don't equal strategic clarity. Organizations are investing billions in AI transformation while using metrics designed for a pre-AI era. When boards start demanding accountability for these investments, and they will, security leaders who can't demonstrate clear business impact will see their budgets cut first. The window to develop real value measurement frameworks is closing fast."**

Steve Wilson
Chief AI and Product Officer
Exabeam

Security Leaders Struggle to Justify AI Spending

The research reveals a critical tension in how organizations approach AI investment. AI simultaneously holds three distinct positions in budget planning:

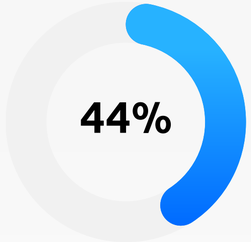
The #1 driver of budget increases



44% cite AI/automation as primary factor driving 2026 budget growth

(See appendix question B for complete data)

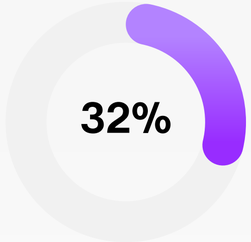
The #1 target for cuts if budgets were reduced



44% would cut AI platforms first if forced to reduce spending by 10%

(See appendix question C for complete data)

The #1 most challenging investment to justify

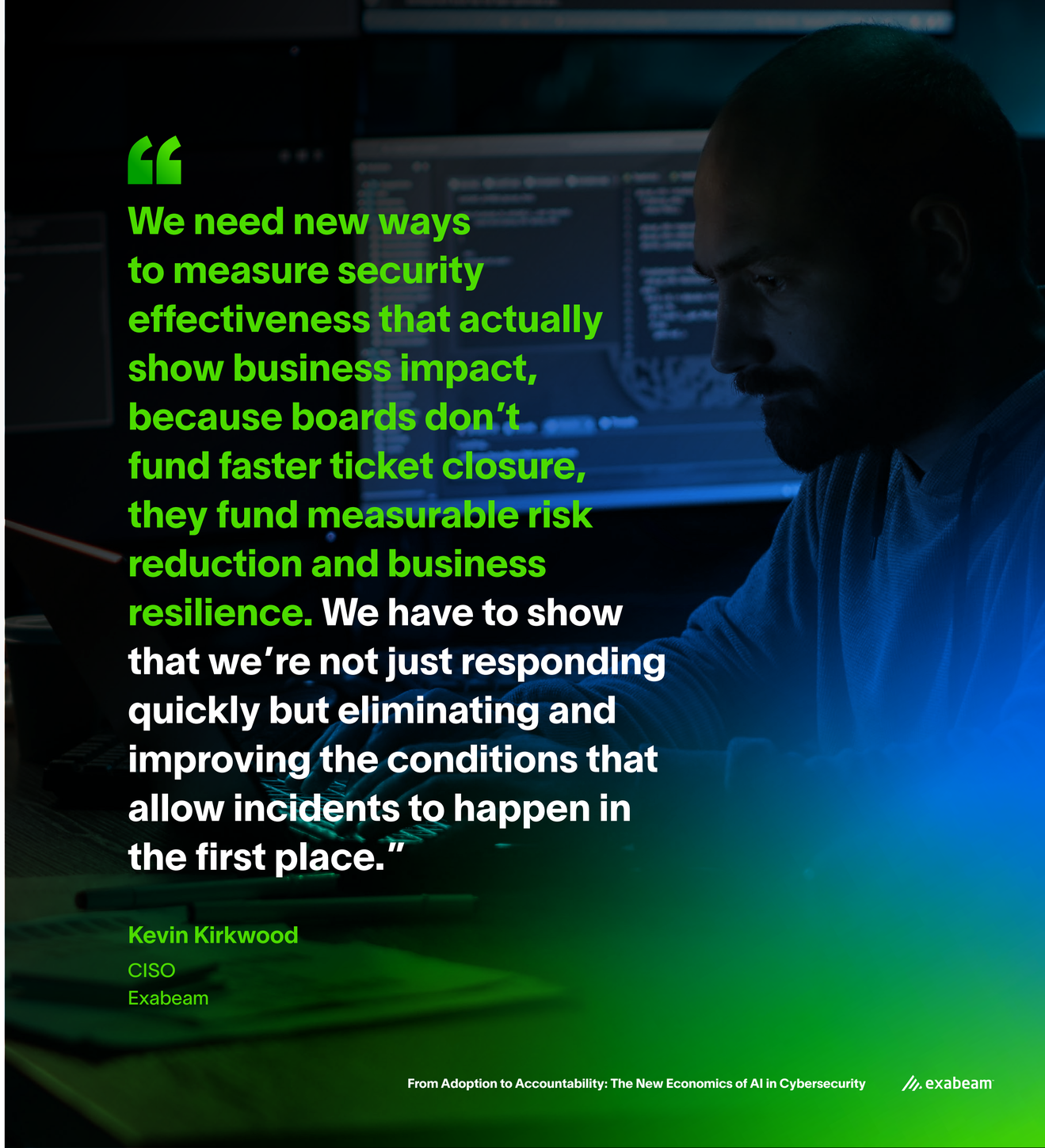


32% say AI is hardest to defend to stakeholders

(See appendix question D for complete data)

This alignment reveals that security leaders are getting budget allocations and mandates to invest in AI, but they lack confidence in their ability to demonstrate ROI to boards and executive stakeholders. They're investing based on competitive pressure and transformation mandates, not on proven frameworks for measuring and communicating value.

Security leaders aren't questioning AI's potential to transform operations. The challenge is quantifying that potential and translating it into business impact that boards and CFOs can evaluate. Without clear frameworks for measuring and communicating AI value in business terms, organizations risk investing in technology they can't defend when budgets come under scrutiny.



> **"We need new ways to measure security effectiveness that actually show business impact, because boards don't fund faster ticket closure, they fund measurable risk reduction and business resilience. We have to show that we're not just responding quickly but eliminating and improving the conditions that allow incidents to happen in the first place."**

Kevin Kirkwood
CISO
Exabeam

EXPERT INSIGHTS

What CISOs Are Actually Saying

CISO | Tech

One of the main reasons [for our budget increase] is it's the shift of some of the costs and the spending to AI-based tools, they save money and so that's been one of the main reasons. [...] The reality is that AI is the future for everything and it's like the Internet or mobile phones, or other things that you cannot be left behind. It's a belief from a business standpoint that AI is a critical baseline for business in the future."

CISO | Insurance

AI is at the peak of inflated expectations, and most organisations are getting a bunch of wild guesses in terms of the accuracy from AI ... it doesn't surprise me that a lot of folks are having a hard time justifying, because you can't gauge how fast you move forward, you're just allowing folks to tinker with a new shiny toy if it's not based and built on the right foundation."

CISO | Tech

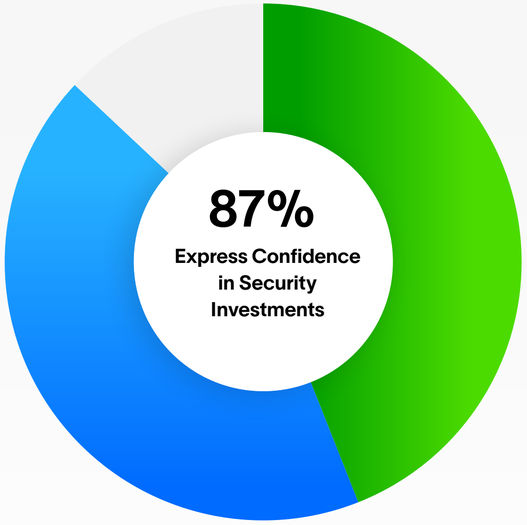
I think there's no question at all about whether we needed to use AI, adopting AI for cybersecurity or other things without question. [...] It's more of a question of when is the right time. Because it's not just replace everything and change everything, some things need to have more ROI analysis, some things need to be tested first before actually saying that. It's a massive change."

The Value Demonstration Challenge

While 87% of security leaders express confidence, **44% extremely confident** and **43% confident**, that their investments are delivering business value, the mechanisms they use and the barriers they face to demonstrate this value reveal significant gaps in how security value is communicated to business stakeholders.

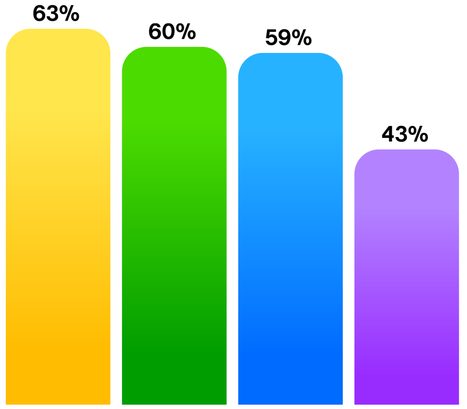
The Disconnect is Clear

Security leaders believe they're using quantified ROI and outcome metrics, but boards and executives still don't understand the connection between security investments and business risk. **The problem isn't a lack of metrics. Security teams are relying on traditional security measurements that don't translate** into the business impact language boards need to evaluate investment decisions and understand how security protects and enables business objectives.



(See appendix question E for complete data)

How Security Leaders Measure Value



63%
Quantified ROI (financial impact, risk reduction models)

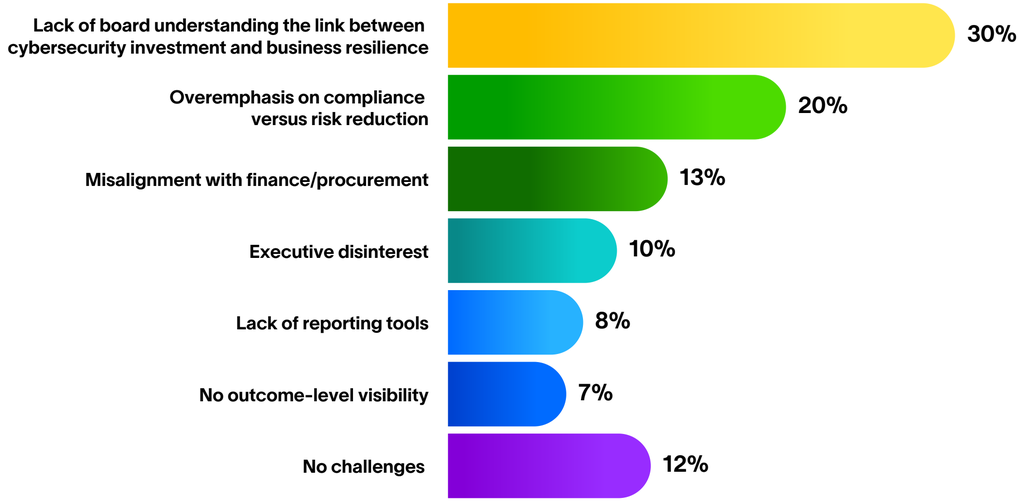
60%
Operational metrics (alert closure rate, patch coverage)

59%
Outcome metrics (mean time to detect/respond)

43%
Narrative metrics (security posture, anecdotal wins)

(See appendix question F for complete data)

Biggest Challenges in Defending Security Spend



(See appendix question G for complete data)

EXPERT INSIGHTS

Reframing Security Metrics for the Boardroom

"Traditional metrics like mean time to resolution become problematic in AI-assisted environments where time windows can vary from 2 hours to 7 months depending on the nature of the incident. **Organizations need new frameworks for measuring security effectiveness that account for AI's impact on operations.** The most effective approaches focus on outcome-based metrics that tie directly to business resilience: prevented breaches, reduced business disruption, and faster recovery from incidents. These are metrics executives understand because they translate security performance into business impact."

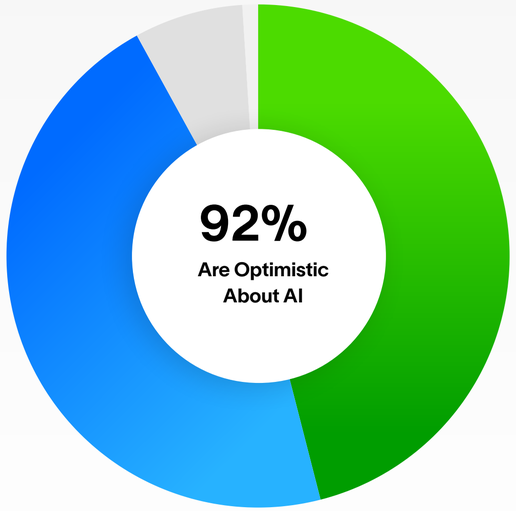
Steve Povolny
VP of AI Strategy and Security Research
Exabeam

"Faster response times and polished dashboards may signal operational maturity, but they don't necessarily reflect reduced enterprise risk. **In the era of AI insiders, systems can be compromised yet remain online because the economic cost of disruption feels too high.** The metric shift must move from restoration speed to measurable reductions in recurrence likelihood, decision drift, and autonomous privilege creep. When you quantify structural risk compression instead of incident closure, you align security investment with business durability."

Steve Moore
Chief Security Strategist
Exabeam

Organizations See AI Improving Core Security Functions

Nine out of ten security leaders (92%) say AI is either already improving their security operations or will improve them by the end of 2026. This optimism is split evenly with **46% stating AI is already improving speed and accuracy** and **46% expecting improvements next year.**

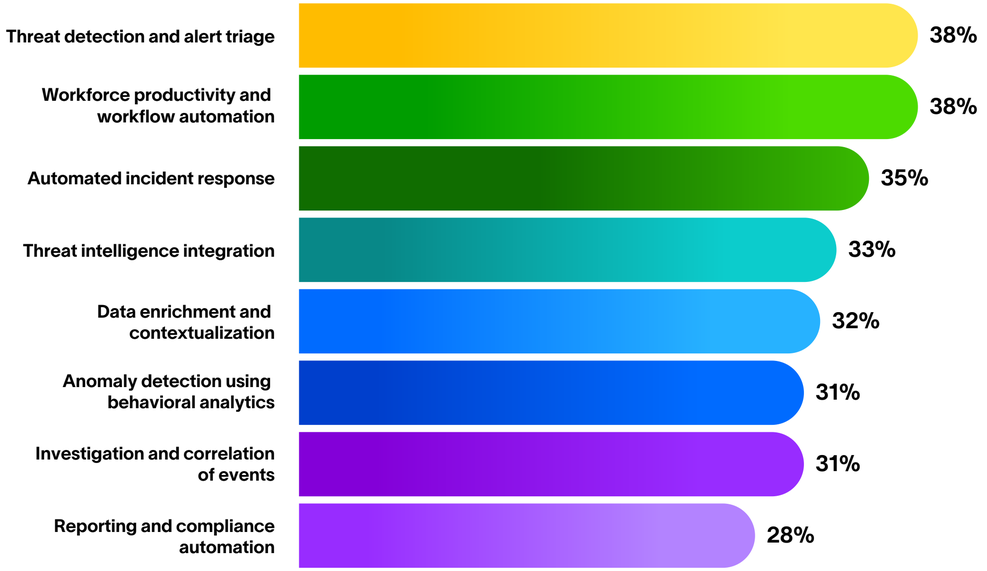


Areas Where AI Will Have Greatest Impact

These priorities reveal that organizations are using AI to address core operational bottlenecks, including the high-volume, repetitive tasks that have historically overwhelmed security teams. The focus on threat detection, alert triage, and automated response directly addresses the alert fatigue and talent shortage challenges that have plagued the industry.

The emphasis on threat detection (38%), workforce productivity (38%), and incident response (35%) indicates that organizations view AI as both a capability enhancement and a force multiplier for existing teams. Rather than wholesale replacement, the focus is on augmentation: using AI to handle repetitive analysis so human analysts can focus on complex investigation and strategic response.

Areas Security Leaders Expect AI to Have the Greatest Impact by 2026



(See appendix question I for complete data)

> **The greatest value of AI in security operations lies not in replacing human analysts, but in reallocating effort away from manual triage toward higher-value analytical work. In this model, AI supports risk prioritization, enrichment, correlation, and contextual decision-making, enabling analysts to focus on complex investigations and informed response decisions."**

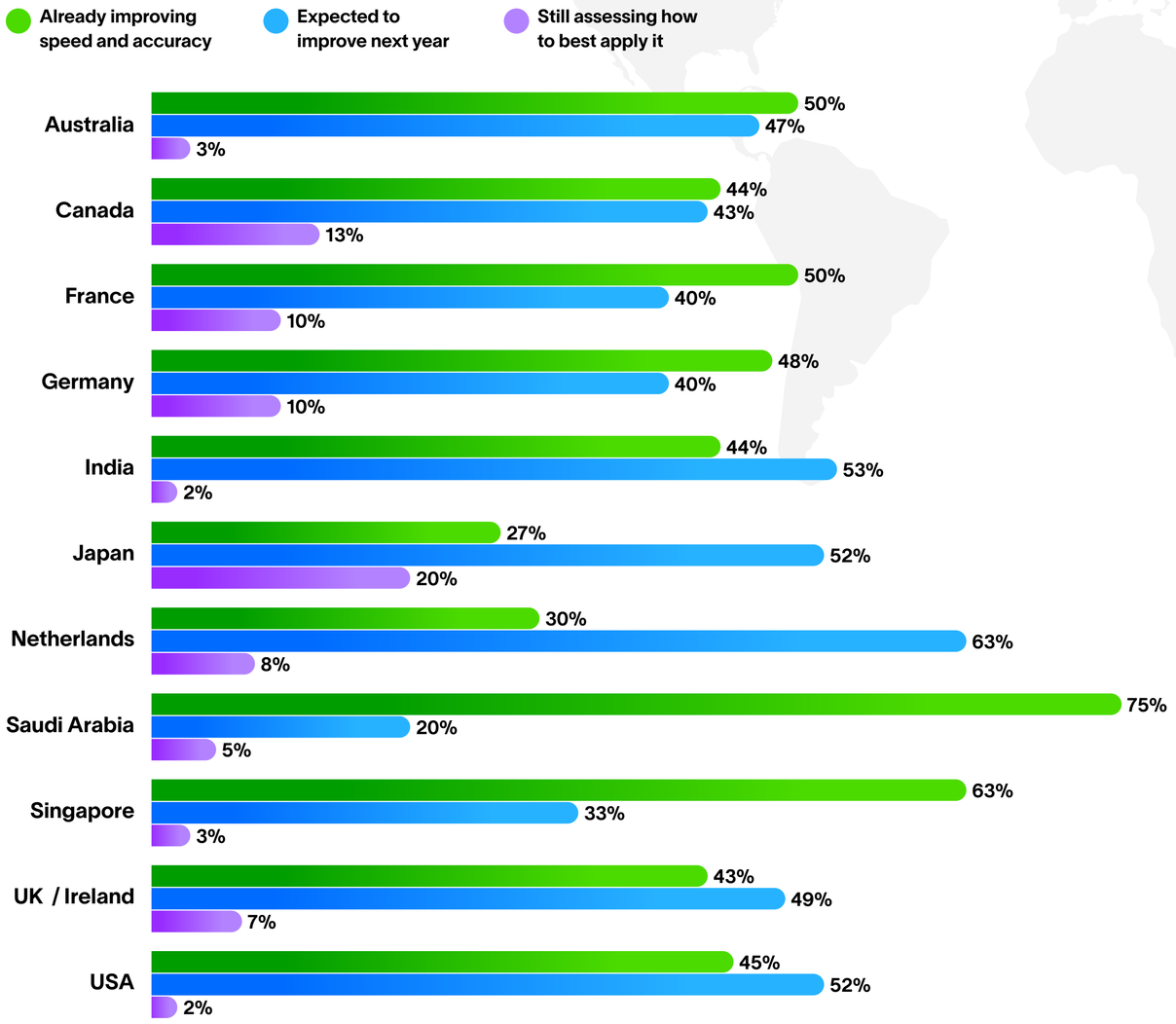
Findlay Whitelaw
Security Researcher and Strategist | Exabeam

Regional Variations in AI Confidence

Saudi Arabia reports the highest rate of organizations saying AI is already improving security operations (75%), reflecting a greater willingness to deploy AI-driven automation and replace traditional security roles. This aggressive adoption aligns with the region's broader digital transformation initiatives and national technology investment priorities.

In contrast, other countries show more measured adoption. The Netherlands (30%) and Japan (27%) report the lowest current impact rates, suggesting a more conservative approach that emphasizes careful evaluation and workforce preservation before scaling AI deployment.

View of AI's Role in Improving Security Operations In 2026



(See appendix question H for complete data)

Conclusion

The cybersecurity industry is experiencing a rare moment of budget abundance, with 95% of organizations increasing spending and 74% seeing double-digit growth. This expansion is being driven primarily by AI and automation investments that are fundamentally reshaping how security operations are structured, staffed, and measured.

CONCLUSION

The Justification Gap Is the Next Security Challenge

The central challenge is clear: security leaders are caught between innovation mandates and a justification gap. They're investing heavily in AI transformation — with AI as the top budget driver at 44% — while simultaneously struggling to articulate its business value to boards and CFOs. The fact that AI is also the most challenging investment to justify (32%) and the first thing that would be cut if budgets tighten (44%) reveals an industry adopting technology faster than it can prove its worth.

This isn't a sustainable dynamic. Budget abundance creates expectation, and organizations that can't demonstrate clear value from AI investments risk seeing those budgets retracted when economic conditions shift or when boards demand accountability for transformation spending.

The organizations that will thrive in this environment are those that recognize deployment is only half the challenge. Success requires developing new frameworks for measuring AI impact and new approaches for communicating that value to business stakeholders. This requires:

- Outcomes-based metrics that tie security performance directly to business resilience: prevented breaches, reduced business disruption, faster recovery from incidents.
- Executive-ready communication that translates technical security improvements into business impact language that boards and CFOs understand.
- Strategic alignment between security operations and business leadership on what success looks like and how it will be measured.
- Workforce development that prepares teams for AI-augmented operations while maintaining critical human expertise.

The industry's trajectory is clear: AI will fundamentally reshape security operations. The question is whether organizations can develop the value measurement and communication capabilities to sustain these investments through the scrutiny that inevitably follows periods of rapid spending growth.

Success in 2026 and beyond will belong to organizations that not only implement AI effectively, but can also demonstrate, convincingly and quantitatively, that it delivers security outcomes and business value commensurate with its cost.

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.

METHODOLOGY

This report is based on research conducted by Sapio Research on behalf of Exabeam in December 2025. The survey captured insights from 750 IT decision-makers responsible for security in organizations with 500+ employees. Respondents represented 12 countries across Europe (UK, Ireland, France, Germany, Netherlands), North America (USA, Canada), and Asia-Pacific and Middle East regions (India, Saudi Arabia, Singapore, Japan, Australia), spanning key sectors including technology, financial services, manufacturing, healthcare, retail, telecommunications, and government.

Learn more about Exabeam at exabeam.com →

Appendix

Appendix | Page 1

Question A: What is your organization's current outlook for cybersecurity budget in 2026? (Select one)

		Regions			Countries										
	All Respondents	APAC	EMEA	North America	Australia	Canada	France	Germany	India	Japan	Netherlands	Saudi Arabia	Singapore	UK / Ireland	USA
Increasing by more than 20%	16%	21%	16%	13%	33%	9%	20%	3%	27%	13%	8%	31%	13%	13%	14%
Increasing by 10% – 20%	58%	52%	52%	67%	63%	59%	55%	45%	62%	37%	55%	48%	53%	55%	70%
Increasing by less than 10%	22%	24%	25%	18%	3%	31%	25%	35%	11%	40%	33%	15%	30%	25%	14%
Staying flat (±1%)	3%	3%	6%	1%	-	1%	-	15%	-	7%	3%	5%	3%	6%	1%
Decreasing by less than 10%	1%	1%	1%	-	-	-	-	-	-	2%	3%	-	-	1%	-

Question B: What are the primary factors driving the change in your organization's 2026 cybersecurity budget? (Select up to three)

		Regions			Countries										
	All Respondents	APAC	EMEA	North America	Australia	Canada	France	Germany	India	Japan	Netherlands	Saudi Arabia	Singapore	UK / Ireland	USA
Adoption of AI and automation in security operations	44%	51%	45%	39%	43%	39%	53%	52%	69%	36%	26%	39%	-	51%	38%
Expansion of cloud and hybrid infrastructure	33%	33%	34%	32%	47%	32%	28%	48%	29%	32%	28%	32%	-	36%	32%
Mainstream adoption of AI across the business	32%	35%	31%	30%	17%	26%	28%	36%	33%	43%	36%	32%	-	29%	32%
Business growth or digital transformation initiatives	29%	34%	22%	34%	47%	27%	13%	12%	33%	29%	13%	26%	-	30%	36%
Rising threat landscape and attack sophistication	28%	31%	26%	29%	30%	27%	45%	39%	29%	34%	18%	11%	-	28%	30%
Investment in modernizing or replacing legacy tools	28%	19%	29%	30%	20%	36%	30%	27%	27%	11%	44%	32%	-	22%	28%
Executive prioritization of cyber resilience	24%	22%	25%	24%	27%	23%	18%	30%	20%	23%	28%	29%	-	21%	24%
Compliance with new or evolving regulations	23%	22%	25%	21%	27%	20%	15%	21%	11%	27%	18%	29%	-	30%	22%
Talent acquisition and workforce development needs	23%	19%	24%	23%	20%	24%	23%	21%	29%	13%	21%	35%	-	20%	23%
Cost reduction and operational efficiency pressures	16%	19%	13%	18%	17%	24%	13%	6%	13%	23%	15%	16%	-	14%	16%

Appendix | Page 2

Question C: If your cybersecurity budget were to be reduced by 10% in 2026, which technology areas would be the first at risk of cuts? (Select up to three)

		Regions			Countries										
	All Respondents	APAC	EMEA	North America	Australia	Canada	France	Germany	India	Japan	Netherlands	Saudi Arabia	Singapore	UK / Ireland	USA
AI and automation platforms	44%	44%	42%	46%	43%	44%	38%	43%	58%	40%	43%	42%	33%	43%	47%
Third-party security tools and integrations	39%	38%	38%	39%	47%	45%	38%	43%	29%	30%	33%	34%	60%	42%	37%
Cloud security technologies	37%	44%	31%	39%	33%	39%	30%	30%	62%	43%	28%	37%	27%	30%	39%
Threat detection and response tools	32%	24%	36%	32%	30%	23%	33%	28%	24%	25%	28%	46%	17%	39%	35%
Data protection and encryption solutions	31%	35%	25%	34%	33%	31%	20%	18%	38%	28%	23%	29%	47%	28%	35%
Perimeter security solutions (e.g., firewalls, VPNs)	30%	28%	30%	32%	43%	29%	35%	23%	16%	27%	23%	40%	33%	28%	32%
Identity and access management (IAM) tools	30%	33%	26%	33%	30%	28%	30%	30%	36%	30%	25%	25%	37%	25%	34%

Question D: What is the most challenging cybersecurity investment to justify within your 2026 budget? (Select one)

		Regions			Countries										
	All Respondents	APAC	EMEA	North America	Australia	Canada	France	Germany	India	Japan	Netherlands	Saudi Arabia	Singapore	UK / Ireland	USA
AI and automation technologies	32%	31%	25%	39%	43%	28%	20%	25%	36%	22%	30%	22%	30%	28%	43%
Cloud or hybrid infrastructure security	12%	8%	12%	14%	13%	13%	15%	10%	9%	7%	10%	12%	7%	11%	14%
Threat detection, investigation, and response (TDIR)	11%	14%	12%	9%	10%	15%	8%	13%	18%	17%	15%	9%	7%	15%	8%
Business continuity and cyber resilience	9%	10%	8%	9%	3%	9%	5%	10%	7%	7%	3%	12%	27%	7%	8%
Risk-based prioritization and threat modeling	7%	11%	7%	6%	3%	11%	10%	-	16%	13%	8%	11%	7%	5%	5%
Analyst headcount or training	7%	5%	11%	5%	3%	7%	13%	8%	-	10%	13%	12%	7%	9%	5%
Identity and access management (IAM)	6%	7%	7%	6%	13%	7%	8%	5%	11%	3%	8%	5%	-	8%	6%
Third-party or supply chain risk management	6%	7%	5%	6%	7%	5%	8%	3%	2%	8%	5%	9%	10%	3%	6%
SIEM modernization	3%	3%	6%	2%	-	1%	3%	10%	2%	5%	3%	6%	3%	6%	2%
We haven't encountered significant justification challenges	6%	4%	8%	4%	3%	4%	13%	18%	-	8%	8%	2%	3%	8%	4%

Appendix | Page 3

Question E: How confident are you that your cybersecurity investments are delivering business value? (Select one)

		Regions			Countries										
	All Respondents	APAC	EMEA	North America	Australia	Canada	France	Germany	India	Japan	Netherlands	Saudi Arabia	Singapore	UK / Ireland	USA
Extremely confident	44%	49%	46%	40%	53%	36%	28%	33%	58%	43%	35%	75%	43%	43%	42%
Confident	43%	44%	48%	38%	47%	56%	60%	65%	38%	47%	58%	20%	43%	50%	32%
Somewhat confident	13%	7%	6%	22%	-	8%	13%	-	4%	8%	8%	5%	13%	7%	26%
Not at all confident	0%	1%	-	-	-	-	-	3%	-	2%	-	-	-	-	-

Question F: When asked to demonstrate the value of your security program to leadership or the board, what type of evidence do you rely on? (Select all that apply)

		Regions			Countries										
	All Respondents	APAC	EMEA	North America	Australia	Canada	France	Germany	India	Japan	Netherlands	Saudi Arabia	Singapore	UK / Ireland	USA
Quantified ROI (e.g., financial impact, risk reduction models)	63%	63%	56%	70%	60%	68%	45%	55%	76%	55%	50%	65%	63%	58%	71%
Operational metrics (e.g., alert closure rate, patch coverage)	60%	62%	56%	62%	70%	65%	60%	45%	64%	58%	40%	60%	57%	62%	61%
Outcome metrics (e.g., mean time to detect/respond)	59%	58%	59%	60%	70%	59%	65%	58%	47%	63%	58%	58%	50%	58%	60%
Narrative metrics (e.g., general security posture, anecdotal wins)	43%	51%	37%	45%	60%	32%	33%	33%	51%	48%	35%	34%	47%	43%	49%
We do not have a formal value validation process	2%	2%	2%	1%	3%	3%	-	10%	-	3%	3%	-	3%	-	-

Question G: What's your biggest challenge defending cybersecurity spend to executive stakeholders? (Select one)

		Regions			Countries										
	All Respondents	APAC	EMEA	North America	Australia	Canada	France	Germany	India	Japan	Netherlands	Saudi Arabia	Singapore	UK / Ireland	USA
Lack of board understanding the link between cybersecurity investment and business resilience	30%	27%	21%	39%	40%	29%	18%	18%	33%	13%	20%	20%	33%	26%	42%
Overemphasis on compliance versus risk reduction	20%	24%	20%	19%	20%	20%	28%	15%	22%	23%	20%	23%	30%	18%	18%
Misalignment with finance/procurement	13%	18%	13%	10%	13%	12%	15%	18%	16%	23%	10%	11%	17%	13%	10%
Executive disinterest	10%	6%	13%	10%	-	3%	13%	15%	7%	10%	15%	11%	3%	12%	12%
Lack of reporting tools	8%	6%	10%	6%	-	12%	5%	3%	11%	7%	8%	20%	3%	10%	4%
No outcome-level visibility	7%	10%	8%	3%	10%	4%	5%	15%	7%	13%	13%	6%	10%	7%	3%
No challenges	12%	8%	14%	12%	17%	20%	18%	18%	4%	10%	15%	9%	3%	14%	10%

Appendix

Question H: What best describes your view of AI's role in improving your security operations in 2026? (Select one)

		Regions			Countries										
	All Respondents	APAC	EMEA	North America	Australia	Canada	France	Germany	India	Japan	Netherlands	Saudi Arabia	Singapore	UK / Ireland	USA
Already improving speed and accuracy	46%	42%	50%	45%	50%	44%	50%	48%	44%	27%	30%	75%	63%	43%	45%
Expected to improve next year	46%	48%	42%	50%	47%	43%	40%	40%	53%	52%	63%	20%	33%	49%	52%
Still assessing how to best apply it	7%	9%	7%	5%	3%	13%	10%	10%	2%	20%	8%	5%	3%	7%	2%
We don't expect major improvements	1%	1%	1%	-	-	-	-	3%	-	2%	-	-	-	1%	-

Question I: In which areas of security operations do you expect AI to have the greatest impact by 2026? (Select up to three)

		Regions			Countries										
	All Respondents	APAC	EMEA	North America	Australia	Canada	France	Germany	India	Japan	Netherlands	Saudi Arabia	Singapore	UK / Ireland	USA
Threat detection and alert triage	38%	33%	38%	41%	50%	41%	40%	28%	36%	22%	33%	35%	37%	46%	41%
Workforce productivity and workflow automation	38%	44%	34%	38%	60%	41%	38%	38%	47%	32%	23%	35%	50%	35%	37%
Automated incident response	35%	34%	36%	35%	20%	37%	38%	28%	36%	48%	30%	35%	17%	43%	34%
Threat intelligence integration	33%	36%	30%	35%	30%	39%	30%	25%	40%	40%	33%	31%	30%	30%	34%
Data enrichment and contextualization	32%	33%	31%	32%	30%	32%	25%	20%	44%	23%	33%	38%	40%	31%	32%
Anomaly detection using behavioral analytics	31%	36%	28%	32%	40%	28%	28%	28%	20%	40%	18%	26%	47%	33%	33%
Investigation and correlation of events	31%	33%	28%	32%	43%	29%	20%	38%	38%	25%	20%	34%	30%	27%	33%
Reporting and compliance automation	28%	23%	31%	27%	13%	20%	35%	40%	24%	27%	28%	37%	23%	23%	29%