Cybersecurity
INSIDERS

## 2023 REPORT

# Artificial Intelligence in Cybersecurity

ARISTA ENEA zscaler™

# Executive Summary

Fueled by the remarkably human-like capabilities of ChatGPT and other generative AI tools released over the past year, AI has catapulted into the spotlight across nearly all industries, including cybersecurity. But does this heightened visibility mean AI is poised to transform cybersecurity, or is AI to some extent just the star of the latest technology hype cycle? To help answer this question, Cybersecurity Insiders surveyed its 600,000-member information security community to find out what CISOs and their frontline cybersecurity teams think about AI's current and potential impact on their profession, and to discover the current AI maturity level of organizations based on team knowledge, AI strategy development, adoption of AI-enhanced tools, and current and planned budgets.

A foundational insight is that cybersecurity professionals believe the transformative power of AI is very real. An overwhelming 92% expect AI to have a major (61%) or moderate (31%) impact on the industry over the next several years, and most have ambitious plans to close what the survey reveals are significant gaps in their AI maturity level. Other key findings, grouped under the themes of fears, hopes, and plans include the following:

## FEARS

- **Phishing & social engineering** top the list of attacks AI will likely make more dangerous
- **Rogue AI** is a serious concern for a majority (77%) of cybersecurity professionals
- **Offensive AI** will develop faster than defensive AI according to most (62%)

## HOPES

- **Better threat detection & vulnerability assessments** are the most desired AI benefits
- **Intrusion detection & prevention** (48%) is the domain expected to benefit most from AI
- **Cost savings** is ranked as the number one KPI used to measure AI success (41%)

## PLANS

- **Adoption** is at ground zero or only in the earliest implementation stages for 61%
- **Anomaly detection & network monitoring** lead deployed AI/ML-enhanced functions
- **Budget** increases are expected by 68%, with 41% viewing AI as a high or top priority

For a panel discussion about the needs and concerns raised in this survey, we invite you to watch our on-demand webinar "Get Ready for the AI Revolution – Fears, Hopes and Plans for AI in Cybersecurity: Surprising Results from New Survey".

Many thanks to Enea, Arista Networks, and Zscaler for supporting this important research, with special gratitude to Enea for their invaluable contribution to this report.

Thank you,

Holger Schulze

**Holger Schulze**
CEO and Founder
Cybersecurity Insiders

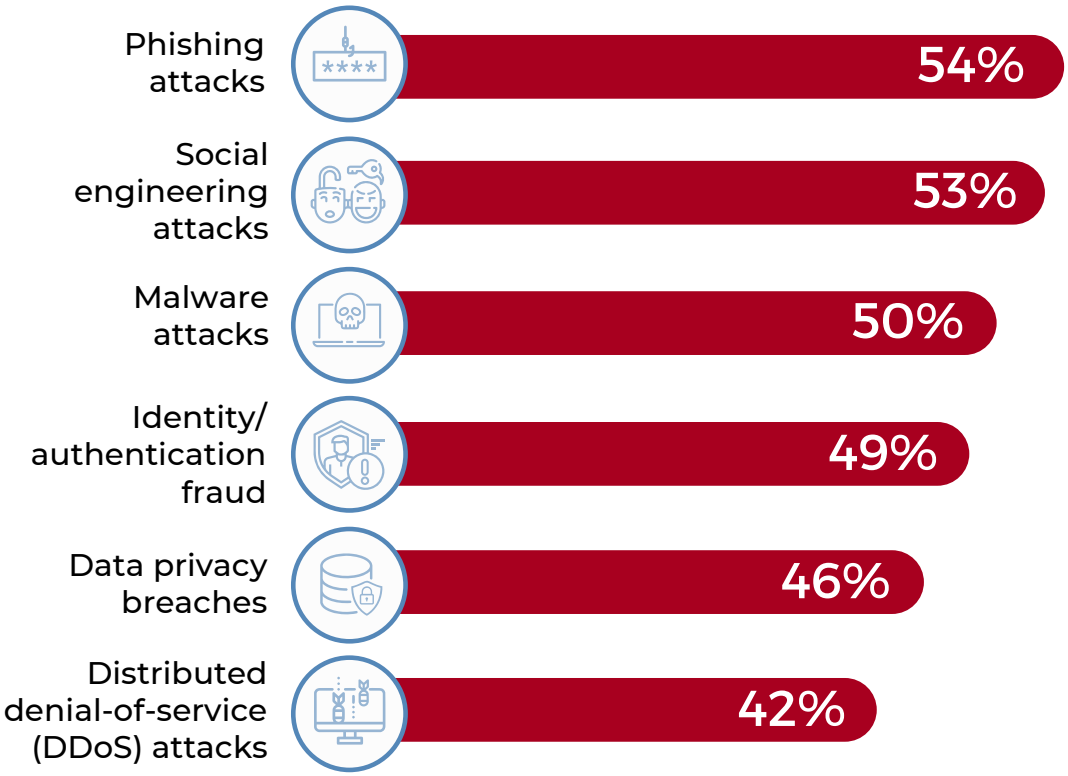
Cybersecurity INSIDERS

| FEARS |

# More Dangerous Cyber Attacks

Many organizations are concerned AI will be used to make current types of attacks more dangerous in the near future, with phishing attacks (54%) topping the list. This is followed closely by social engineering attacks (53%) and malware attacks (50%). These threat vectors typically rely on human error or manipulation, so it is logical to assume they will be more effective through AI, which can be used to generate very human-like text and produce highly deceptive images, videos, and sounds.

**In your opinion, which types of attacks will become more dangerous in the near future because of AI input?**




Also cited: Ransomware attacks (39%), Advanced persistent threats (APTs) (38%), Supply chain exploits (31%)

In characterizing how AI will make such attacks more dangerous, respondents stated they believe AI will make cyber attacks:

- Significantly more sophisticated (71%)
- Faster and more scalable (63%)
- More difficult to detect (66%)
- More unpredictable (56%)

Reports of AI-enhanced attacks emerging to date indicate that respondents are quite accurate in their assessments of what types of attacks are most likely to be made more effective by AI, and why they will be more difficult to combat.[1]

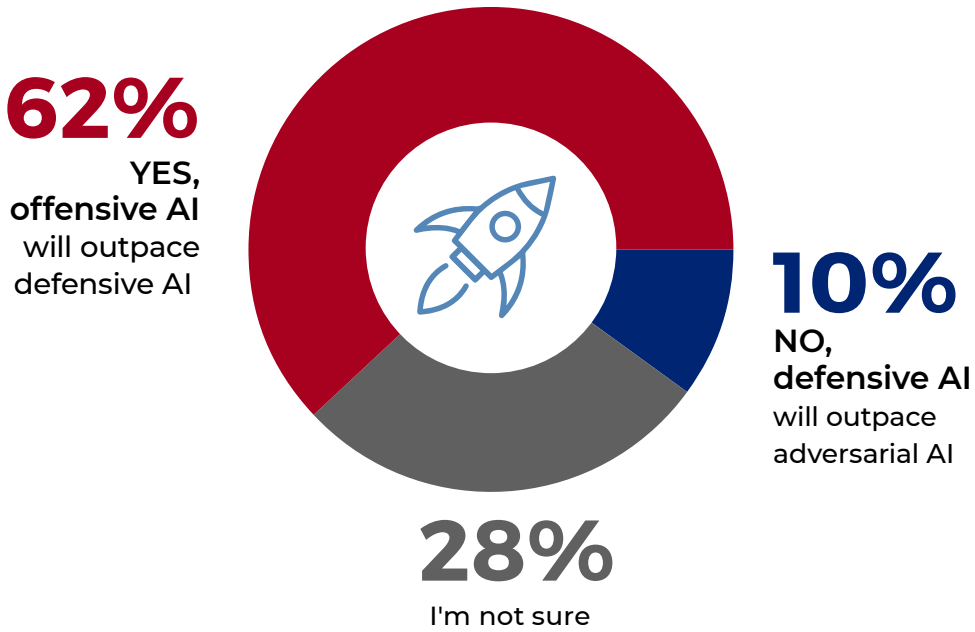
*1. See, for example, the December 2022 report "The security threat of AI-enabled cyberattacks" from the Finnish Transport and Communications Agency Traficom at https://bitly.ws/VGLu*

# Offensive AI Stronger Than Defensive AI

The tremendous power of AI can be deployed by both adversaries and defenders, and which side will have the advantage is a critically important question. A significant majority of respondents (62%) is quite pessimistic and believes that the development of AI by adversaries will outpace defensive AI capabilities. Only 10% hold an optimistic view that defensive AI will keep up with increasingly sophisticated threats, and 28% are unsure.

While, at least for now, defensive AI is proving itself to be highly effective,[2] there are several actions an organization can take to reduce pessimism and build confidence. These include prioritizing investment in advanced defensive AI capabilities to narrow the perceived gap, focusing on tools that exploit defensive advantages (such as comprehensive knowledge of an organization's IT environment), employing Zero Trust network architectures that limit lateral movement and hence can help contain damage in case of a breach, and establishing KPIs that can demonstrate progress as defensive capabilities are developed.

**Do you believe that the development of offensive AI/ML will outpace the development of defensive AI/ML that protects against attacks?**




*2. For example, see IBM Security Cost of a Data Breach Report, Section 2, at https://www.ibm.com/reports/data-breach*

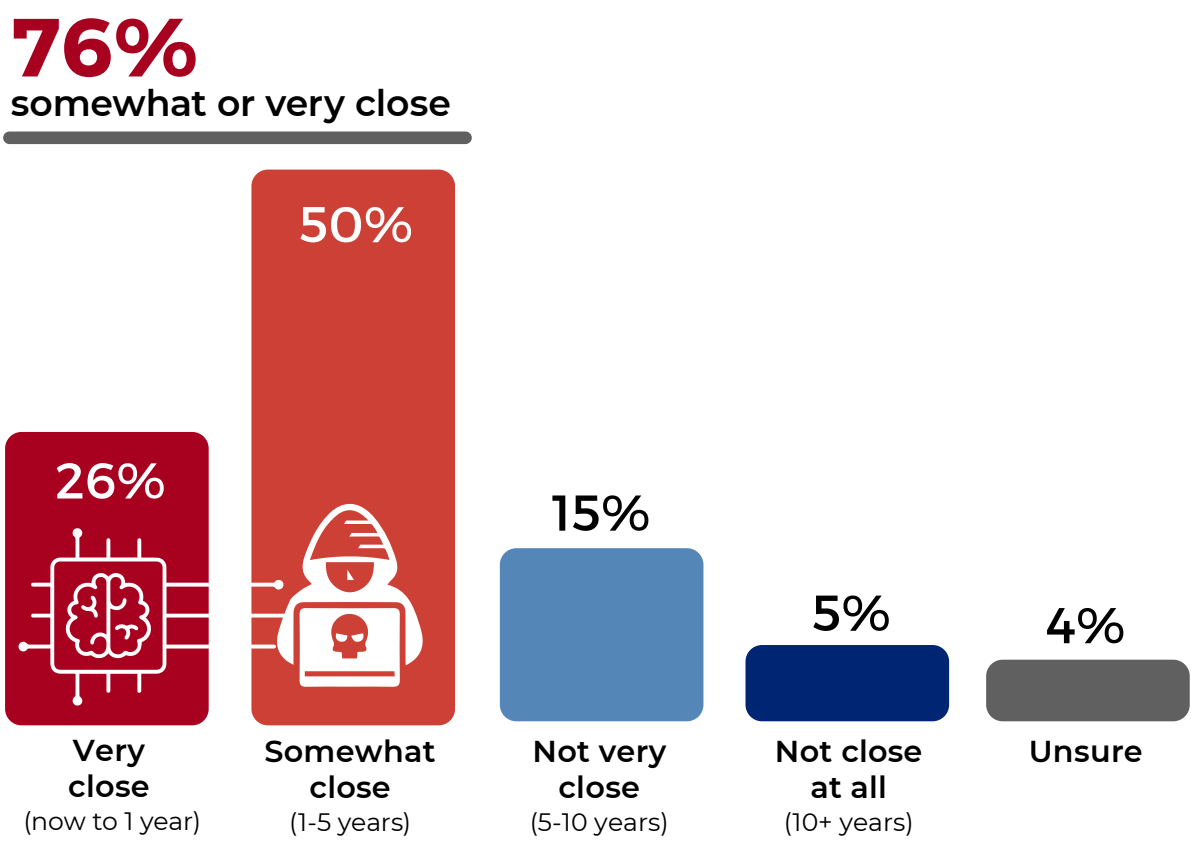
| FEARS |

# Quasi-Unstoppable Malicious AI

A vast majority (76%) of respondents think the world is somewhat close (50%) to encountering malicious AI that can bypass most known cybersecurity measures, or (alarmingly) has already arrived at such a situation or will within the next year (26%). Nonetheless, in a follow-up question, respondents feel very confident (19%) or somewhat confident (50%) in their organization's ability to defend against AI/ML powered attacks at present.

Based on these findings, it is important for CISOs to remind themselves and their teams that even if they believe such a grave threat is imminent, there is nothing to be gained by waiting for these AI threats to fully materialize; proactivity is the key to risk reduction and damage mitigation. Investments in AI-assisted real-time threat detection, advanced analytics, constant cybersecurity upskilling, and the use of advanced breach containment and recovery strategies and tools can provide a robust, multilayered defense against emerging AI-enabled cyber threats that will no doubt continue to evolve. Continuous education and training in particular can be effective in building defensive capabilities. In fact, when asked what steps they feel an organization should take to prepare for sophisticated or overwhelming AI attacks, the number one response was "Increasing cybersecurity training and awareness for employees."

**How close do you think the world is to malicious/adversarial AI that can evade most known cybersecurity defenses?**

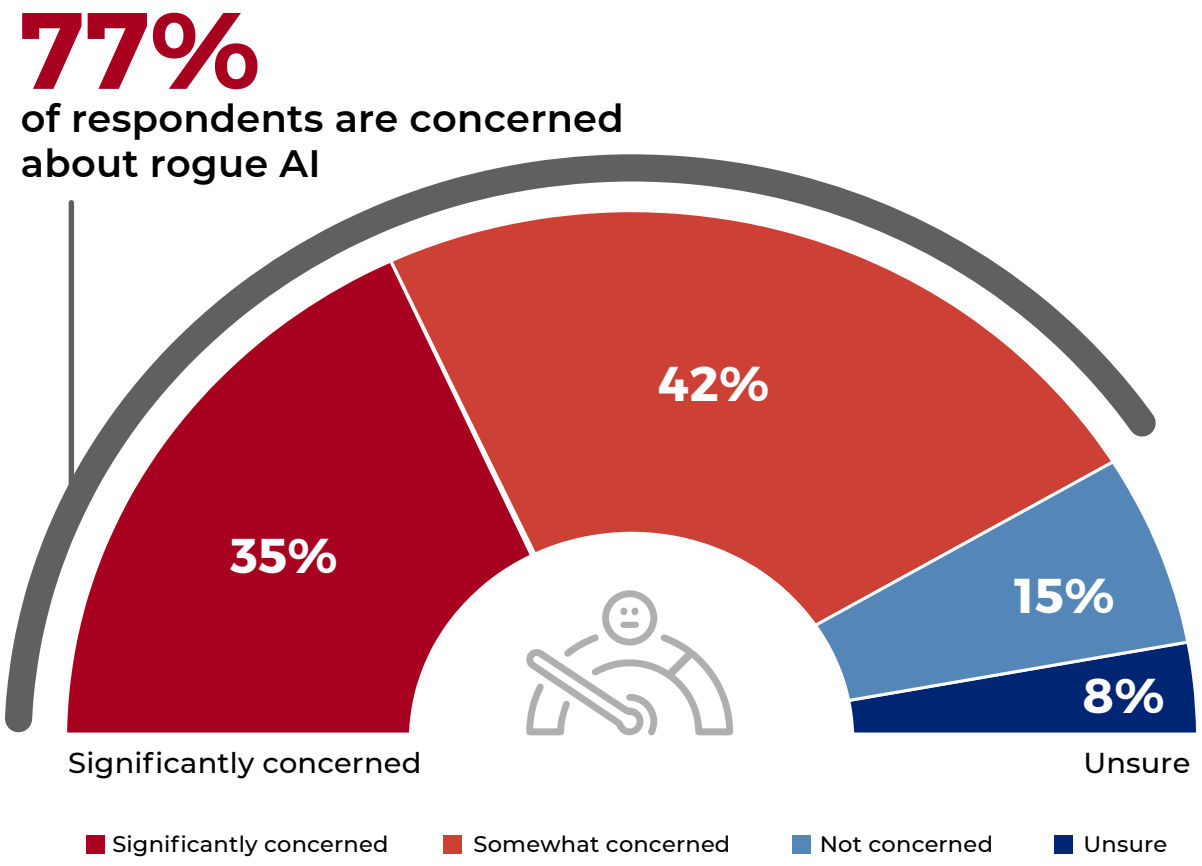


# Concern About Rogue AI

Once confined to the realm of science fiction, fears about rogue AI have become a real-world concern. What exactly is “rogue AI”? Two key elements are embedded in the survey question: it is an AI system that acts with autonomy and behaves dangerously. It can be further described as operating outside of - or contrary to - its intended purpose, scope, and/or programming, and its potential to cause harm may be due to deliberate actions and behaviors, or simply due to unpredictable behavior. In any case, rogue AI is without a doubt a serious concern among cybersecurity professionals, with 77% reporting they are either “significantly” or “somewhat” concerned about it. Only 15% claim they are not concerned.

Given this high level of concern, organizations would benefit from a strong governance framework for AI ethics and operational risk management, including a rigorous monitoring system that can provide an early warning of any rogue behaviors. It is also advisable to discuss rogue AI detection capabilities with cybersecurity solution vendors or in-house development teams.

**Are you concerned about rogue AI (an application that becomes fully autonomous and behaves dangerously)?**



# Anticipated Benefits Of AI In Cybersecurity

The most significant perceived benefits of AI in security operations fall under the three general categories below, with the specific benefits of improved threat detection, improved vulnerability assessment, and accelerated response nearly tied for first place.

**1) Improved Threat Detection (58%)**

**2) Enhanced Attack Surface Management**

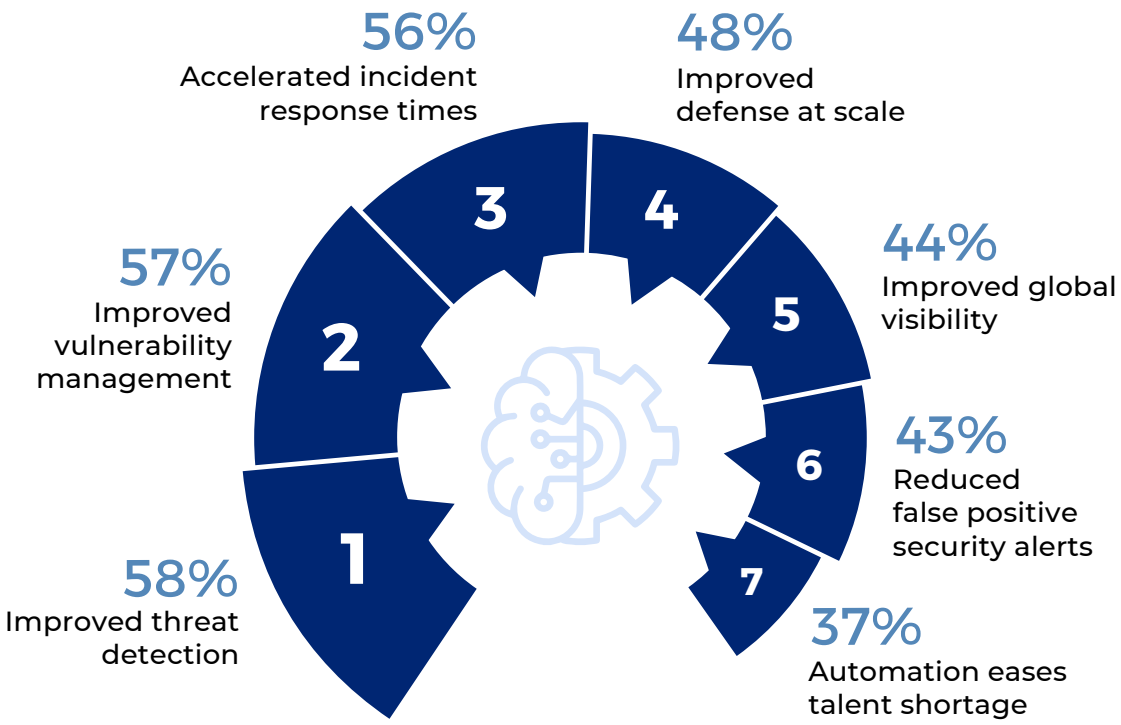
- Improved vulnerability assessment and predictive analysis (57%)
- Improved global visibility into the network and IT infrastructure (44%)

**3) Greater SecOps Efficiency (i.e., AIOps for Cybersecurity)**

- Accelerated incident response times (56%)
- Improved scalability in defending against attacks (48%)
- Reduced false positive security alerts (43%)
- Alleviation of cybersecurity talent shortages through automation (37%)

In response to this question, only 5% selected “Other”, indicating a consensus that the seven options presented represent the most commonly anticipated benefits, or perhaps those that are most familiar or mature. In any case, solution providers would do well to address these specific expectations in their product roadmaps and communications, and should work to boost awareness of innovative benefits which are not yet widely known, such as AI-powered Zero Trust micro-segmentation, AI-enhanced quality of experience, AI-based sandboxing verdicts, AI-based knowledge graphs of network environments, and much more.

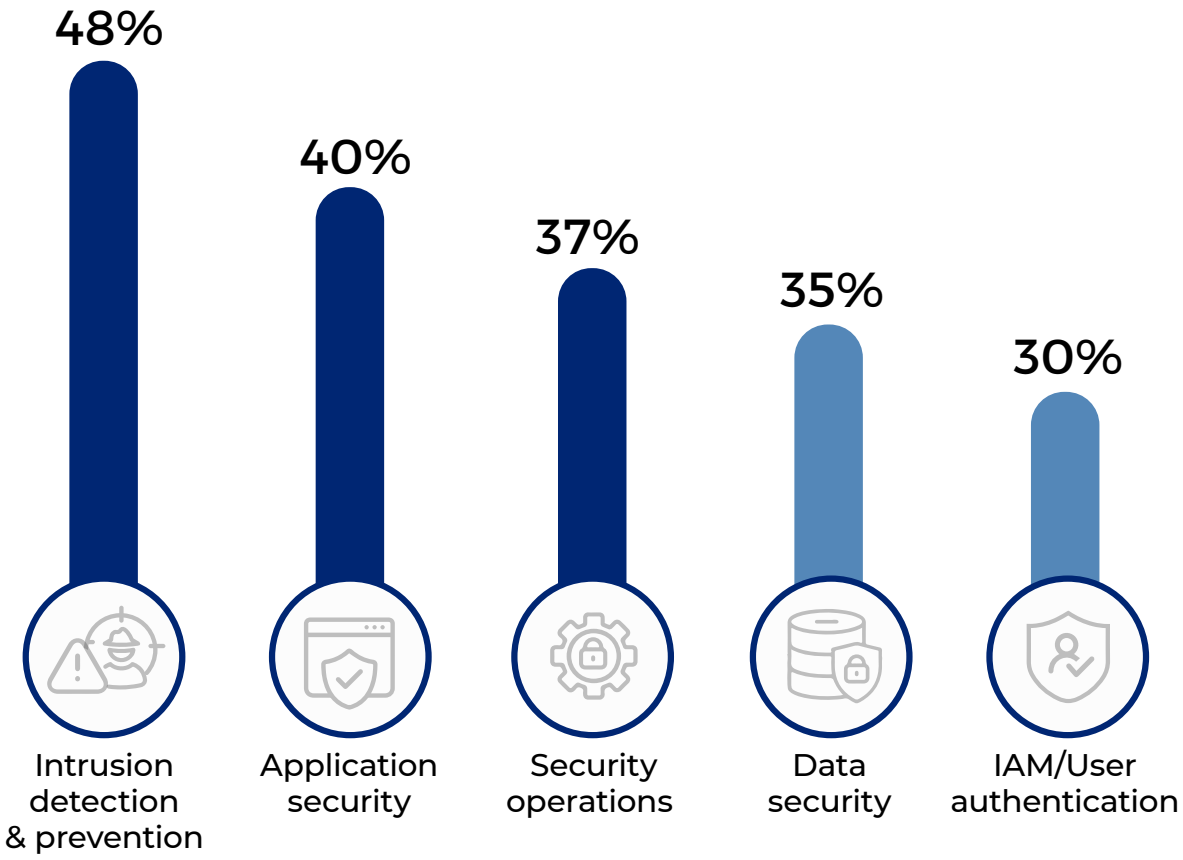
**What do you see as the most significant benefits of incorporating AI into your cybersecurity operations?**



# Cybersecurity Domains Made Stronger By AI

Respondents were also asked which cybersecurity domains they expect to benefit most from AI. The standout domains are intrusion detection and prevention (48%), followed by application security (40%) and security operations (37%). Interestingly, despite the increasing importance of cloud technologies, cloud workload protection was only selected by 21% of respondents (despite the extremely high ratio of breaches in 2023 that involved data stored in the cloud—public, private, or multiple environments[3]).

**Which cybersecurity domains do you think will benefit most from AI?**




Also cited: Firewalls/UTMS 25%, Cloud workload protection 21%, Forensics 15%, Equipment/device vulnerability management/patching 12%, Other 1%

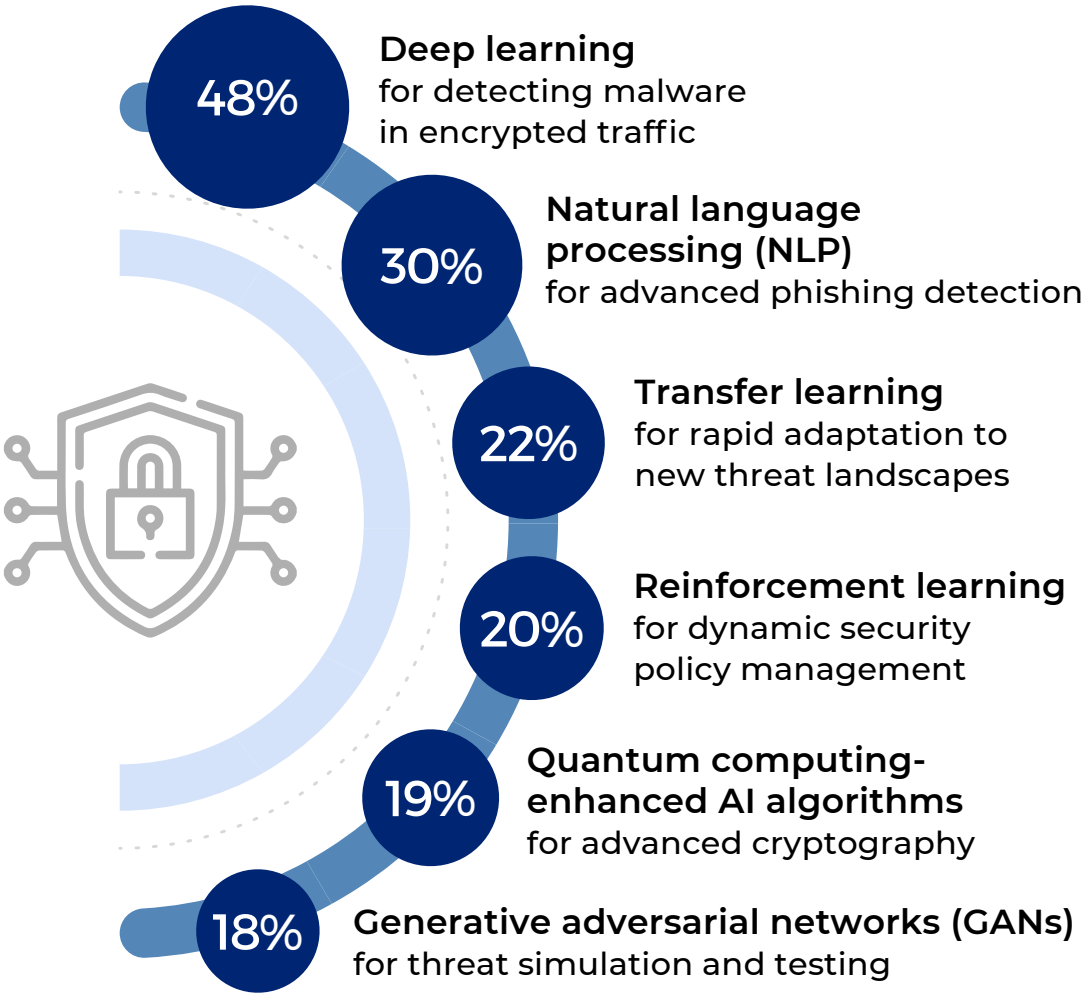
*3. Ibid, IBM Security Cost of a Data Breach Report 2023*

# Most Promising AI/ML Technologies

We asked which AI and ML technologies hold the most promise for enhancing cybersecurity defenses. The most noteworthy finding is the strong focus on deep learning for detecting malware in encrypted traffic, chosen by 48% of respondents. Natural language processing (NLP) for advanced phishing detection also ranks high at 30%, followed by transfer learning for rapid adaptation to new threat landscapes at 22%.

If solution vendors have current or planned R&D initiatives in these domains, sharing knowledge about these activities would be a good way to build confidence in the ability to meet future challenges arising from offensive use of AI.

**In your opinion, which emerging AI and ML techniques hold the most promise for enhancing cybersecurity defenses?**




Also cited: Explainable AI (XAI) to improve transparency and trust in AI-driven security solutions 17%, Unsure 16%, Federated learning for secure, Privacy-preserving data sharing 14%, Other 4%

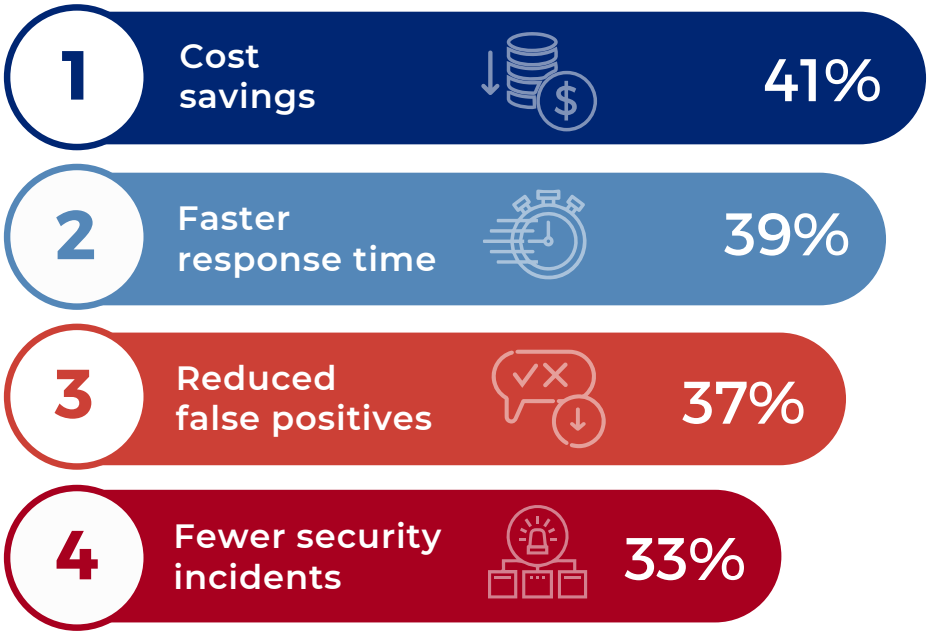
# Success Metrics For AI In Cybersecurity

Establishing clear key performance indicators (KPIs) is a must for assessing the effectiveness of technology plans and ensuring alignment with business objectives. It is no different for AI. When asked about AI KPIs used by their organizations, cost savings (41%) was, interestingly, listed as the number one KPI amongst respondents, even though it did not even make the list of the top anticipated benefits of AI integration. This may represent a dichotomy in C-suite versus rank-and-file priorities, or it may be due, at least in part, to the fact that 'cost savings' was not explicitly named as a possible response in the preceding benefits question.

Regardless, security professionals should be aware that using AI-enhanced security tools and automation has in fact been shown to reduce the cost of a breach by nearly 40%.[4] A prudent policy would be to attend carefully to the ways in which technical performance improvements can be quantified financially, and vendors should take care to integrate ROI analyses into their value proposition.

Another interesting finding is that 22% of organizations utilize a quality of experience KPI for AI, which is often overlooked in AI discussions, even though, as demonstrated by select vendors, AI has tremendous potential for QoE improvement.

**How does your organization measure the success or effectiveness of AI in your cybersecurity strategy?**




Also cited: Not measuring at this time 24%, User/client satisfaction 22%, Unsure 18%

*4. Ibid, IBM Security Cost of a Data Breach Report 2023*

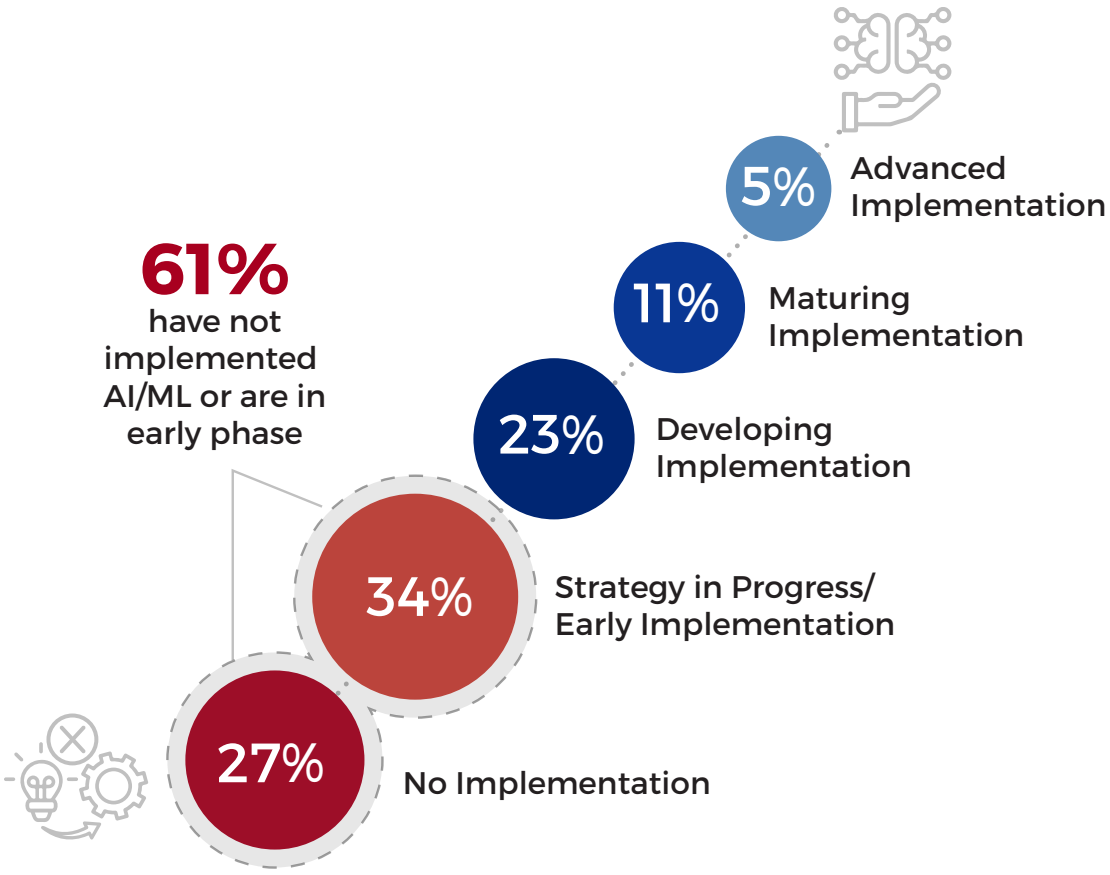
# Current Maturity Level For AI

In line with findings from other studies that touch on AI, a notably high number of organizations - nearly two-thirds (61%) - do not yet have a formal AI strategy in place; they either have not begun (27%) or have only just begun (34%) to integrate AI technologies into their cybersecurity defenses. Only a small fraction (16%) defines their implementation as mature or advanced, with established AI strategies and AI technologies well integrated into their cybersecurity defenses.

On a positive note, in another question, nearly a third (32%) report having a dedicated resource or team responsible for AI governance in cybersecurity. Also encouraging is the fact that most have ambitious plans to rapidly close their implementation gaps, as is evident in succeeding questions. Executing on those plans can deliver a high ROI in terms of significantly reduced time to breach detection and containment, and breach cost.[5]

While it is critical to have a well-defined AI strategy and AI governance policies, for those who do not yet have a strategy in place, quick wins can be achieved by focusing initially on high-impact AI enhancements in areas like threat detection, incident response, and observability, thereby building internal support for developing and funding a formal plan.

**How would you describe your organization's adoption of AI and ML in cybersecurity?**



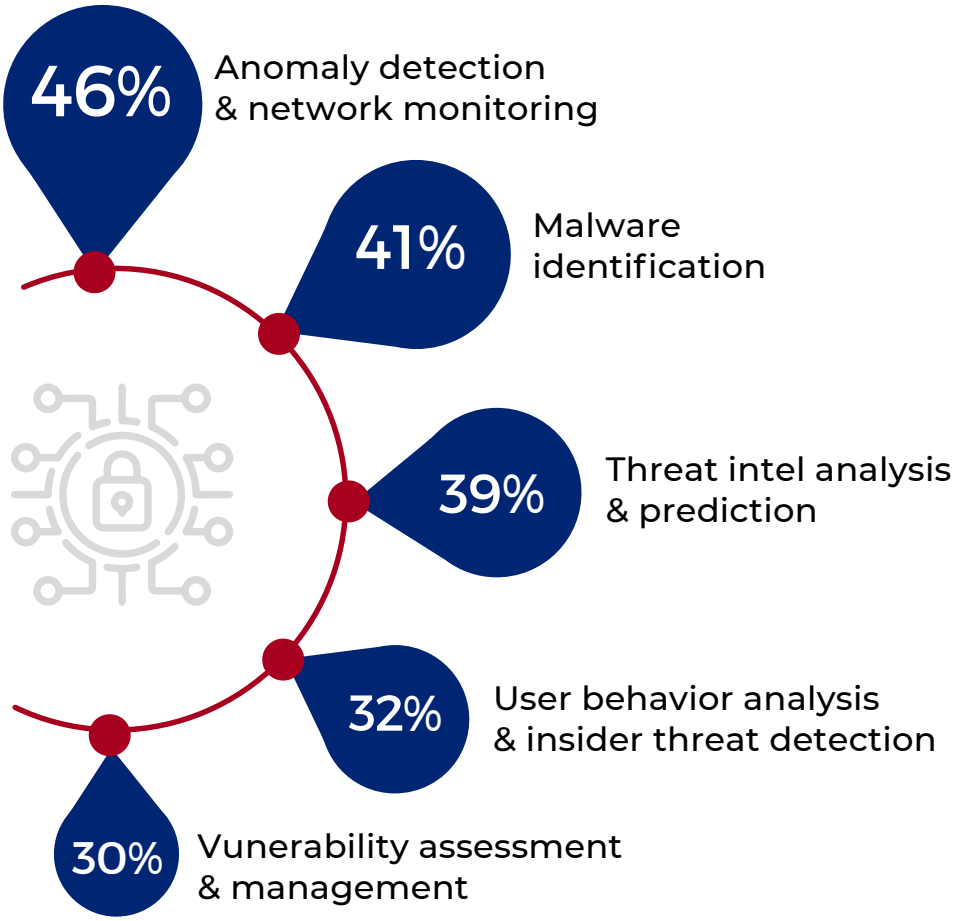

*5. Ibid, IBM Security Cost of a Data Breach Report 2023*

# Current Uses Of AI

The specific cybersecurity functions currently being enhanced by AI and ML provide a snapshot of where the technology is already finding utility.

The leading AI applications in cybersecurity today are in anomaly detection and network monitoring (46%), followed by malware identification (41%), threat intelligence (39%), user behavior analysis and insider threat detection (32%), and vulnerability assessment and management (30%). It's noteworthy that user support systems (24%) and automated incident response (23%) are lower on the list, despite the significant potential of such tools to help alleviate the critical shortage of human cybersecurity talent (see the 'Workforce Impact and Training Needs' section at the end of this report).

**What cybersecurity functions in your organization are currently enhanced by AI and ML?**



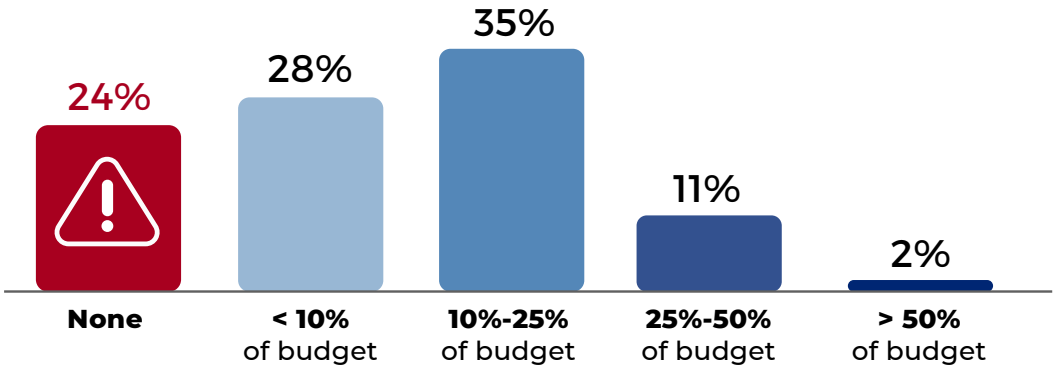

Also cited: User support systems (chatbots, virtual assistants, knowledge bases, etc.) (24%), Automated incident response and remediation (23%), Security posture management (17%), Adversarial AI research and development (7%)

# Current & Planned Budget For AI

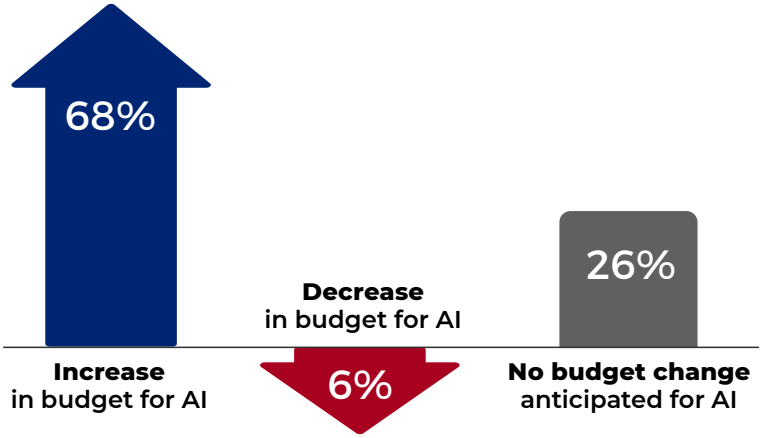
In line with the large percentage (27%) who have not yet begun their AI journey, 24% report no current allocation in their cybersecurity budget for AI-enhanced technologies, and another 28% allocate less than 10%. This finding is disconcerting, though it doesn't necessarily reflect a complete absence of AI capabilities at these organizations, as virtually all new and upgraded cybersecurity vendor solutions today integrate some AI capabilities, even though end users may not be aware of these capabilities. Importantly, however, an overwhelming 68% expect their AI security budgets to increase over the next two years.

Organizations planning a budget increase will get the highest ROI for their investment if they ensure they have a coherent strategy in place for how these additional resources will be used, how they align with business priorities, and how ROI will be measured. For the third of respondents (32%) who anticipate either no change or a decrease in budget allocation, unless they are among the respondents already investing heavily in AI, it's worth revisiting these decisions in light of AI's rapidly growing influence in cybersecurity.

**What portion of your cybersecurity budget is currently allocated to AI-enhanced technologies?**




**What changes to this allocation do you anticipate in the next two years?**

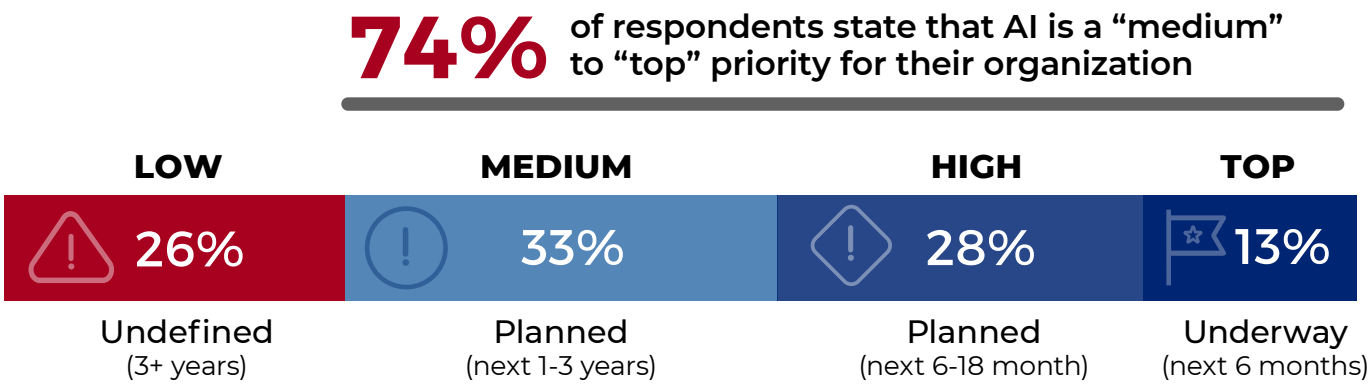


# Importance of AI Implementation

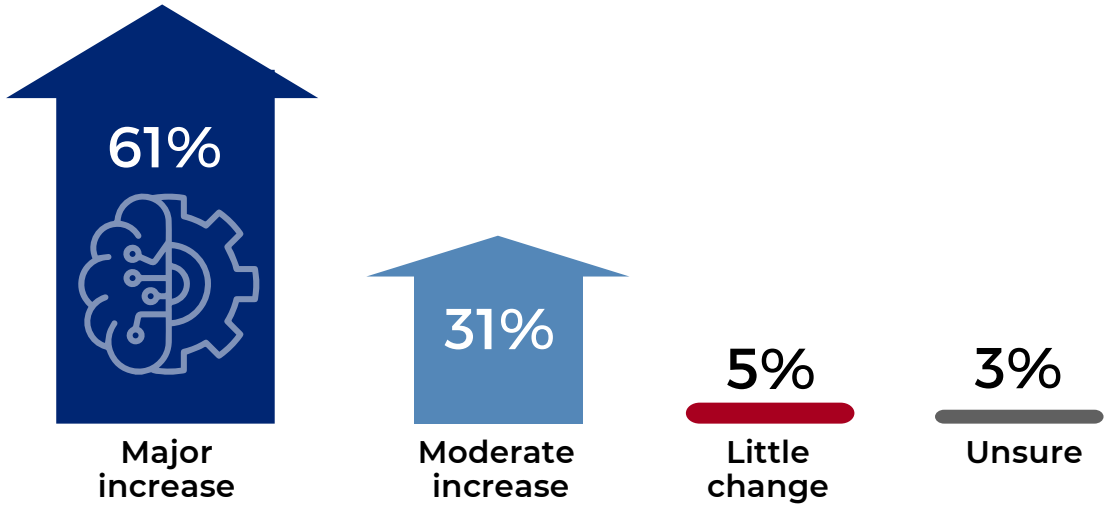
While expectations of increased AI budgets are an implicit sign of AI's growing importance in cybersecurity, other responses drive this point home in a very explicit way. Significantly, three-quarters of respondents (74%) state that AI is a "medium" to "top" priority for their organization. The percentage who consider it a top priority (13%) aligns with the percentage who are already dedicating more than 25% of their cybersecurity budget to AI investments (13%).

Of concern is the high number (26%) who consider AI a low priority, along with the 24% who report no dedicated AI budget. This suggests a troubling lack of urgency regarding a threat landscape that is already being reshaped by AI. However, for many of these organizations, it may just be an honest reflection of where they are today, even though they may expect change is coming. There is some evidence for the latter view in the fact that an overwhelming 92% anticipate a moderate to major increase in the impact of AI on cybersecurity, with 61% of those selecting "major increase."

**How does the implementation of AI for cybersecurity rank among your organization's cybersecurity priorities?**




**How do you anticipate the impact of AI on cybersecurity to evolve in the next five years?**



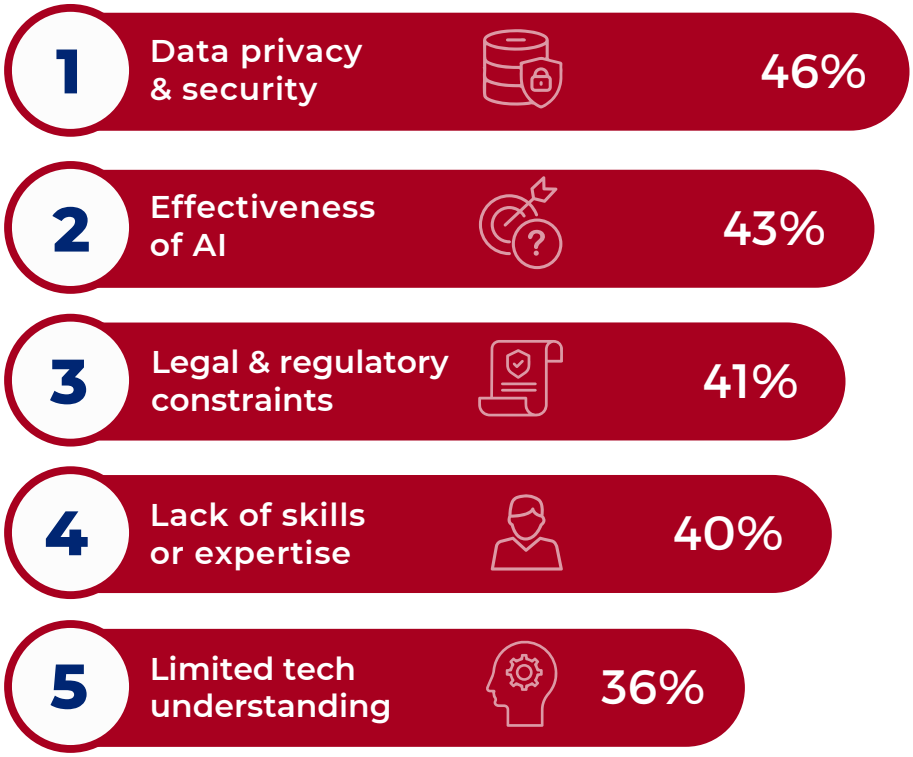
# Adoption Roadblocks

Respondents attach a fairly uniform level of concern to quite diverse subjects. They rank data privacy and security as their top concern (46%), revealing that organizations are wary of how AI algorithms will handle sensitive data. Following closely are uncertainty about the effectiveness of AI-driven solutions (43%) and legal and regulatory constraints (41%).

Lack of skills and expertise (40%) and limited understanding of AI technology (36%) were also relatively high concerns, which is to be expected given the pace at which AI is penetrating the industry. Interestingly, of least concern among the dozen choices offered were "Dependence on vendor" (28%) and "Resistance to change or internal organizational challenges" (23%).

Understanding these diverse concerns and their relative priority levels is essential for effective planning and risk mitigation and overcoming any internal objections to AI adoption. Beyond understanding, taking concrete actions to manage risks in each of these contexts is necessary to successfully use AI to strengthen an organization's defenses. This could include ensuring robust encryption and compliance with data protection regulations, conducting pilot testing on a subset of the security infrastructure before full-scale implementations, setting clear KPIs to measure effectiveness, securing outside guidance as needed on legal and regulatory matters, and conducting regular ML/AI training and establishing AI mentorship programs.

**What are your top concerns about integrating AI into your cybersecurity operations?**




Also cited: Dependence on vendor (28%), Resistance to change or internal organizational challenges (23%)

# Adoption Accelerators

Addressing barriers to AI adoption in cybersecurity is crucial to unlocking advanced capabilities and defenses against evolving threats. The most significant facilitator to faster AI adoption, according to 35% of the respondents, would be the implementation of data privacy and security guidelines for AI-driven solutions. This aligns well with the concerns about data privacy and security of AI implementations discussed earlier. Greater awareness and promotion of AI applications from industry leaders was also notably high at 30%, followed by increased funding for AI-driven cybersecurity initiatives (27%).

To act on these findings, organizations would benefit from both establishing and adhering to specific AI security guidelines and policies. Leadership should also actively promote awareness and education regarding the use of AI in cybersecurity. Where funding is an issue, advocating for budget reallocations can be guided by data-driven proof of AI effectiveness in cybersecurity applications.

**What do you believe would help your organization overcome these barriers and accelerate the adoption of AI-driven cybersecurity solutions?**

**35%**
Guidelines for data privacy & security in AI

**30%**
More awareness & promotion of AI apps by industry leaders

**27%**
Increased funding or allocation for AI

**25%**
Clearer proof of AI effectivenes & value

**23%**
Access to AI training, workshops, or educational resources

**16%**
Legal & regulatory frameworks for AI

# Workforce Impact & Training Needs

**What steps should organizations take to prepare for sophisticated or overwhelming AI attacks?**

- Increasing cybersecurity training and awareness for employees: 68%
- Developing incident response plans specifically tailored to AI attacks: 65%
- Conducting regular security assessments and audits: 61%
- Investing in AI/ML-powered cybersecurity solutions: 56%
- Strengthening traditional security controls such as Zero Trust, multi-factor authentication, next-gen firewalls, threat intelligence, etc.: 50%
- Other: 3%

**What skills and training do you believe will be most needed in the future for AI in cybersecurity?**

- AI programming and development: 72%
- Security management: 67%
- Ethics and responsible AI use: 64%
- Data management: 47%
- Other: 0%

**How would you describe your understanding of AI and ML as applied to cybersecurity?**

- Minimal knowledge: 2%
- Basic knowledge: 13%
- Moderate knowledge: 19%
- Extensive knowledge: 50%
- No knowledge: 16%

**How has the adoption of AI affected the cybersecurity workforce in your organization?**

- New skills are required: 45%
- Too early to tell: 40%
- Job roles have been redefined: 27%
- Workforce size has been reduced: 23%
- Job satisfaction has improved: 16%
- Workforce size has increased: 15%
- Job satisfaction has declined: 12%
- Unsure: 8%
- Other: 0%

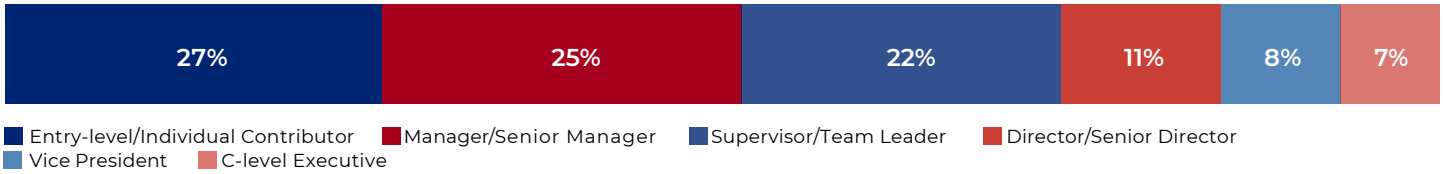
**What role do you think AI can play in alleviating the cybersecurity skills and talent shortage?**

- Automating routine tasks to free up time for more complex tasks: 72%
- Improving the accuracy and efficiency of cybersecurity operations: 63%
- Providing insights and recommendations to help bridge the skills gap: 55%
- Other: 3%

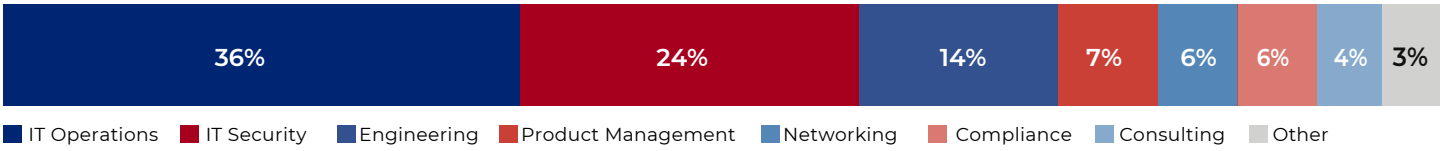
# Methodology and Demographics

This Artificial Intelligence in Cybersecurity Report is based on the results of a comprehensive online survey of 457 cybersecurity professionals, conducted in September 2023, to gain deep insight into the latest trends, key challenges, and solutions. The respondents range from technical executives to managers and IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

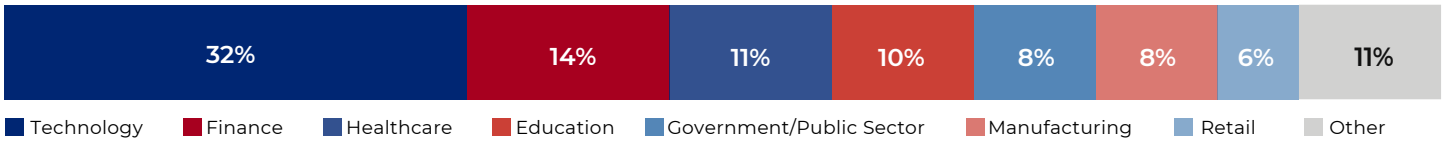
## CAREER LEVEL



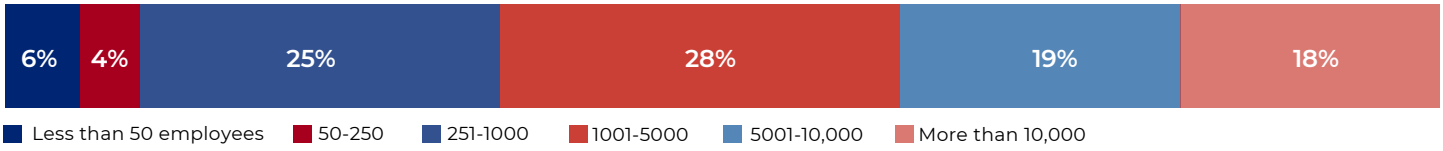

## DEPARTMENT




## INDUSTRY




## COMPANY SIZE




## YEARS OF EXPERIENCE

**About Arista Networks**
Arista Networks is an industry leader in data-driven, client to cloud networking for large data center, campus and routing environments. Arista's award-winning platforms deliver availability, agility, automation, analytics and security through an advanced network operating stack.

[arista.com](arista.com)



**About Enea**
Enea is a world-leading specialist in software for telecom and cybersecurity. The company's cloud-native solutions connect, optimize, and secure services for mobile and fixed subscribers, enterprises, and the Internet of Things. More than 100 communication service providers and 4.5 billion people rely on Enea technologies every day.

Enea has strengthened its product portfolio and global market position by integrating a number of acquisitions, including Qosmos, Openwave Mobility, Aptilo Networks, and AdaptiveMobile Security. Enea is headquartered in Stockholm, Sweden, and is listed on Nasdaq Stockholm.

[enea.com](enea.com)

**About Zscaler**
Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform.

[zscaler.com](zscaler.com)

Cybersecurity
INSIDERS

Cybersecurity Insiders brings together 600,000+ IT security professionals and world-class technology vendors to facilitate smart problem-solving and collaboration in tackling today's most critical cybersecurity challenges.

Our approach focuses on creating and curating unique content that educates and informs cybersecurity professionals about the latest cybersecurity trends, solutions, and best practices. From comprehensive research studies and unbiased product reviews to practical e-guides, engaging webinars, and educational articles - we are committed to providing resources that provide evidence-based answers to today's complex cybersecurity challenges.

Contact us today to learn how Cybersecurity Insiders can help you stand out in a crowded market and boost demand, brand visibility, and thought leadership presence.

Email us at **info@cybersecurity-insiders.com** or visit **cybersecurity-insiders.com**