CXO REvolutionaries

EXECUTIVE REPORT

AI Trends and Security Insights for the C-Suite

CXO REvolutionaries
QUARTERLY CYBER UPDATE

Q3/2024

SPONSORED BY: zscaler™

Executive Summary

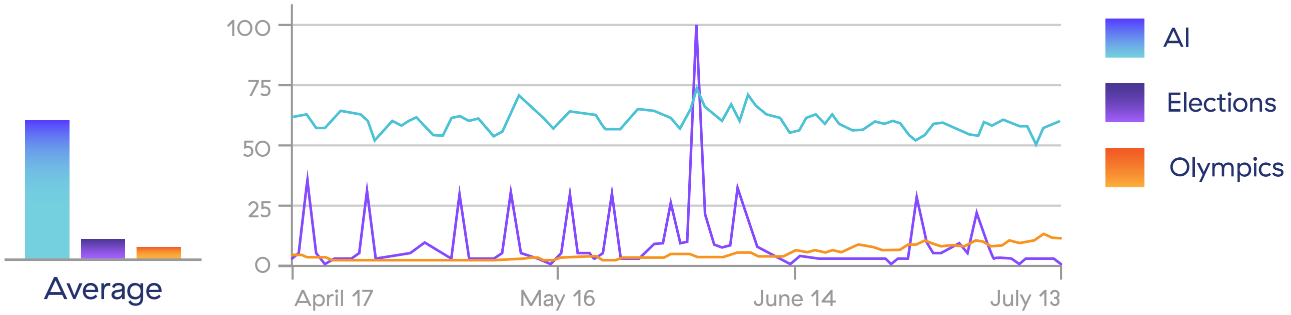
Artificial intelligence (AI) has taken the business world by storm. Leaders across industries are doing their best to stay informed of developments with this fast-paced, disruptive, and game-changing technology. The Zscaler CXO REvolutionaries Quarterly Cyber Update provides executives, board members, and public officials like you the latest information on hot topics and trends that affect cybersecurity and IT. Our goal is to keep you informed of relevant technology issues while steering you toward optimal security strategies.

In this issue you will discover:

- Recent developments in AI that set trends and shape industry directions
- A breakdown of popular AI tools and the industries adopting them
- AI-related security concerns and mitigations
- Effective uses and benefits of AI in cybersecurity

Recent Developments

Stories about AI have captured the public's imagination and led to a flood of related content across media channels. Organizational leaders trying to separate relevant AI insights from marketing hype face a difficult task. This report will help you catch up on the latest trends in AI and offer insights on where, how, and why the technology is being used. We'll share the latest discoveries from Zscaler Threatlabz and other leading sources.



Google Trends shows AI consistently generating more global interest than elections or the Olympics (with one exception – June 4th)

Over the last quarter, website users have heavily searched the term “AI” on Google. Its enduring popularity is clear when compared to other words of global interest, like the Olympics and elections. AI was searched more often than either of those other terms, except for June 4th. Searches for election results (driven by India), made “elections” the most popular term that day.

Notable AI events

MAY 14

Google adds its Gemini-powered AI Overviews to search results for American users. AI Overviews generates a short summary related to a user’s search terms.

MAY 20

Microsoft announces the launch of its AI-infused CoPilot+ PCs. The PCs feature a SnapDragon X processor and run Microsoft’s Copilot AI assistant locally.

MAY 21

The European Union’s AI Act becomes law. The voluminous legislation regulates several aspects of AI usage, and levies fines of up to 7% of annual global revenue on non-compliant businesses.

JUNE 7

Microsoft rolls back plan to make the AI-driven Recall tool enabled by default on future offerings. After receiving pushback from privacy advocates and consumers, Microsoft declares the Recall feature will be optional.

JUNE 10

Apple announces its integration of ChatGPT access into iOS 18, iPadOS 18, and macOS Sequoia.

JUNE 18

NVIDIA, dominant maker of AI chips, becomes the most valuable public company in the world.

JUNE 24

Apple dismisses rumors that it is considering integrating Meta’s Llama LLM (Large Language Model) in its devices.

JULY 10

Samsung announces it will include Galaxy AI features in its Z Fold 6 and Z Flip 6 phones.

Section 1: Current AI prevalence

594%

Increase in AI tool use, April '23 to Jan '24

49.1%

Of surveyed web content partially or fully AI generated

> "AI, as we tend to think of it today, is a newer issue and therefore the challenges are numerous. Organizations must carefully balance enabling their employees to be more productive by using tools like ChatGPT versus the risk of data loss."
>
> — JAY CHAUDHRY,
> CEO , ZSCALER

How fast are AI tools being adopted by global industries? What tools are being used, and how widespread are they among market sectors? These answers are found in the Threatlabz analysis of AI transaction data in the Zscaler Zero Trust Exchange. To provide a sense of scale, the Zero Trust Exchange processes over 400 billion transactions and 5 trillion security signals from around the world every day. An extensive look into ThreatLabz's observations is found in the **Zscaler ThreatLabz 2024 AI Security Report**.

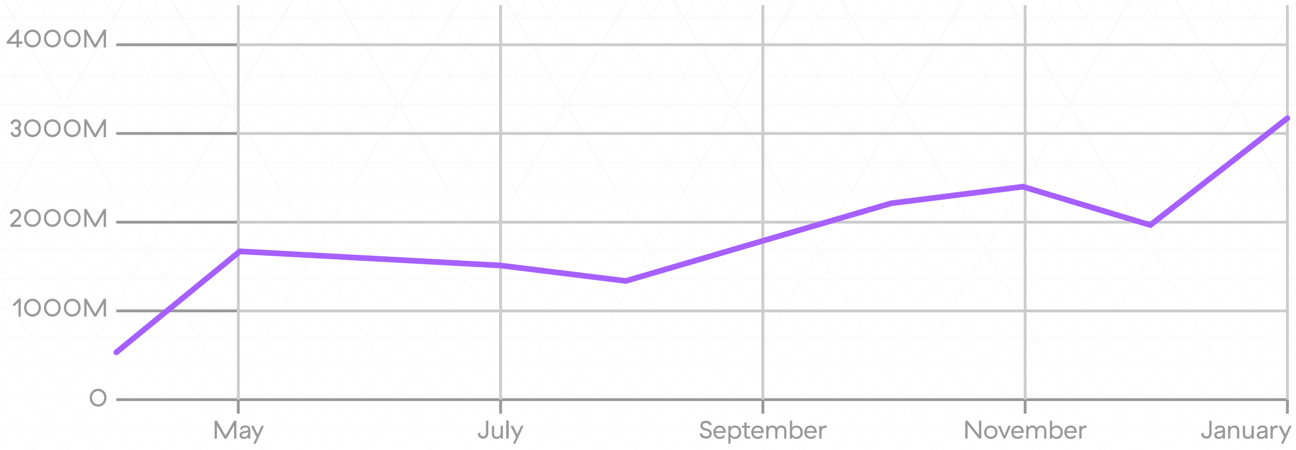
Key findings:

- The Zscaler Zero Trust Exchange logged a 594% increase in AI tool use between the April 2023 and January 2024
- The most widely used AI applications are ChatGPT, Drift, and Writer
- Industries are using AI tools more and more. Manufacturing is the strongest adopter, followed by finance/insurance and services
- Nearly 50% of recently-surveyed internet content showed signs of being AI-generated

AI adoption

The Zscaler Zero Trust Exchange, which tracks global organizations in the public and private sector, recorded a 594% increase in AI-related transactions between April 2023 and January 2024. This explosive growth captures organizations' enormous interest in AI tools beginning in the latter half of 2023 and continuing to this day.

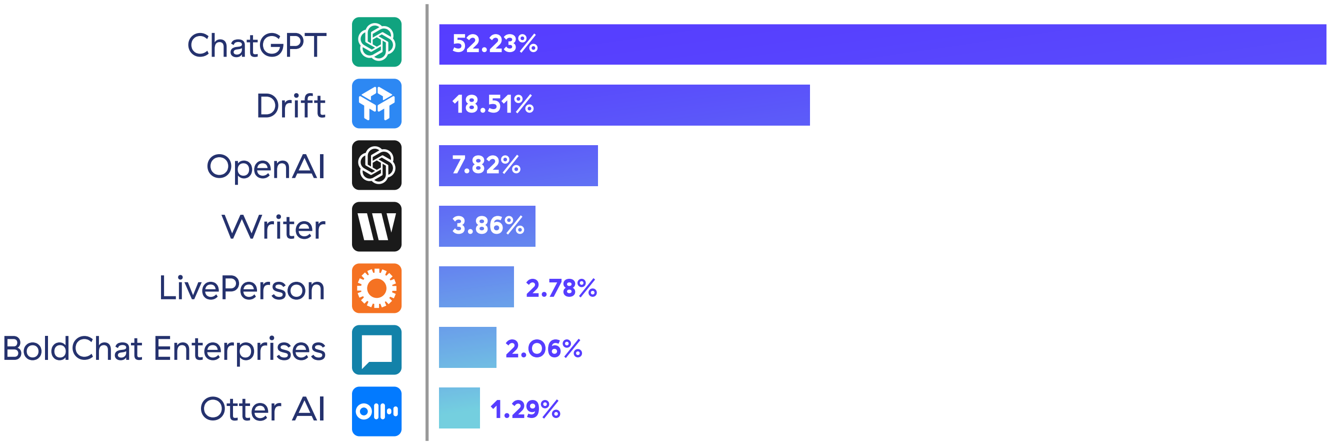
AI and ML transaction trends



Significant rise in AI transactions seen in the Zscaler Zero Trust Exchange from April '23 to Jan '24.

Most AI activity involved a few well-known online tools. In fact, 85% of AI traffic involved one of five applications: ChatGPT, Drift, OpenAI (non-ChatGPT), Writer, and LivePerson.

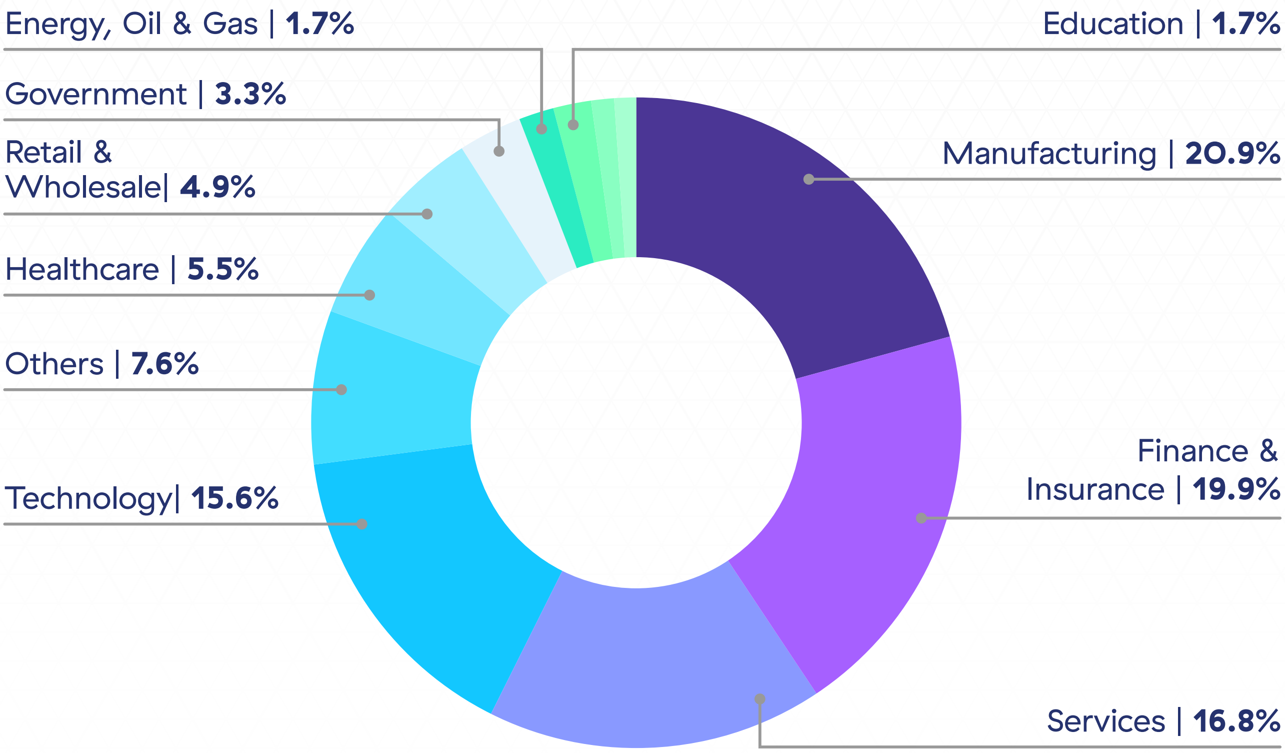
Top AI applications



The large language model (LLM) ChatGPT is the most popular AI application, with other OpenAI offerings collectively placing third

The Manufacturing, finance and insurance, services, and technology sectors generated the most AI-related traffic, accounting for 73.2% of the total. Education, energy, and government contributed the least to AI-traffic, generating only 6.7% combined.

Share of AI transactions by industry vertical

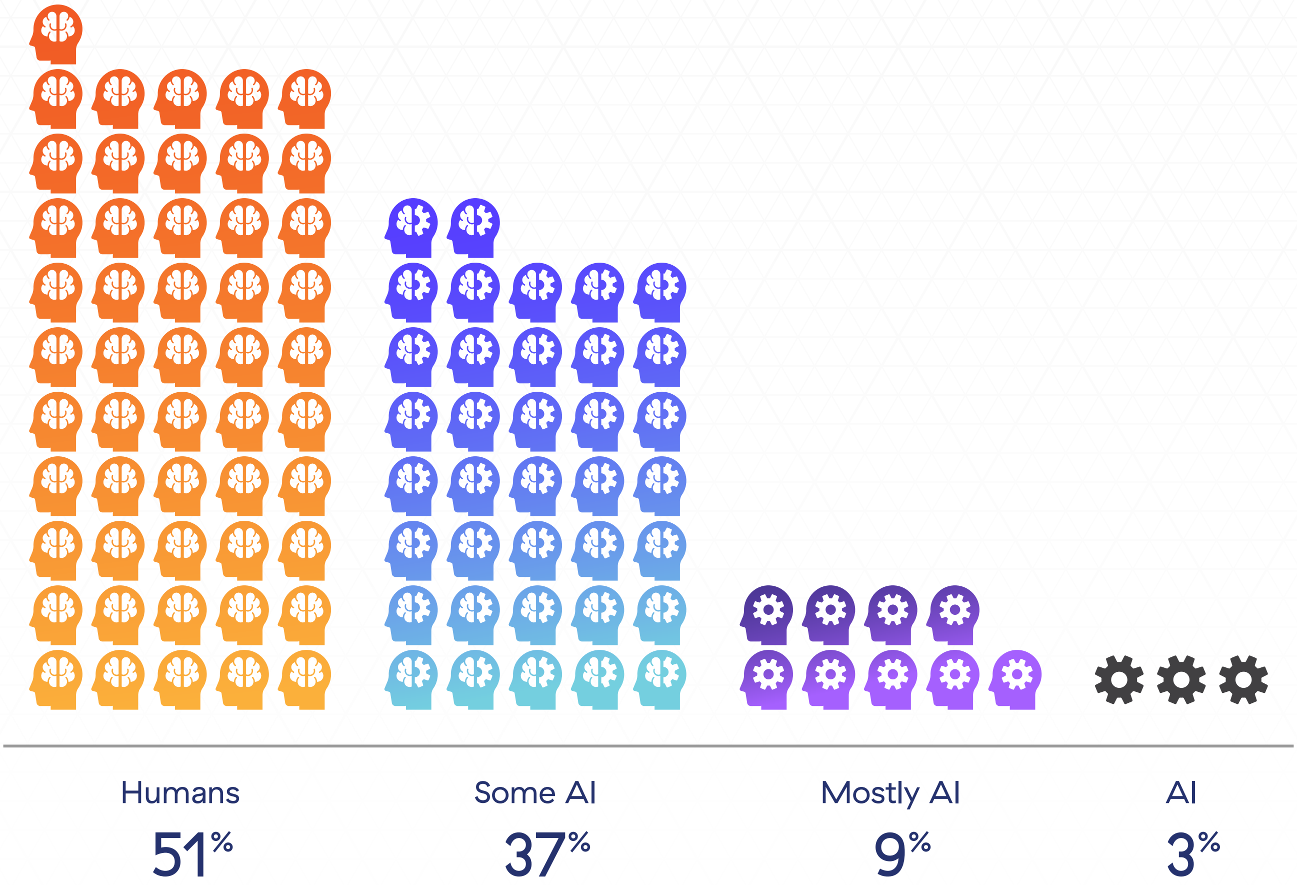


Manufacturing and finance perform the most AI transactions in the Zscaler Zero Trust Exchange

While these numbers indicate a massive upswing in AI-tool usage across industries, they do not reveal whether these tools are visibly changing end user or customer experience. Is the adoption of AI impacting anything customer-facing, or is its influence only noticeable internally?

Researchers at **Graphite**, an AI-powered SEO platform, recently attempted to answer this question. They performed internet searches on 2,200 keywords across 10 highly-traffic topics and analyzed the content returned. Ultimately, they reviewed material from 20,280 URLs. These pages were scanned for signs of AI involvement by **Originality.AI**, a high-fidelity tool for detecting machine-generated content.

Web content generation



AI-generated or AI-assisted web content made up 49% of returned web searches

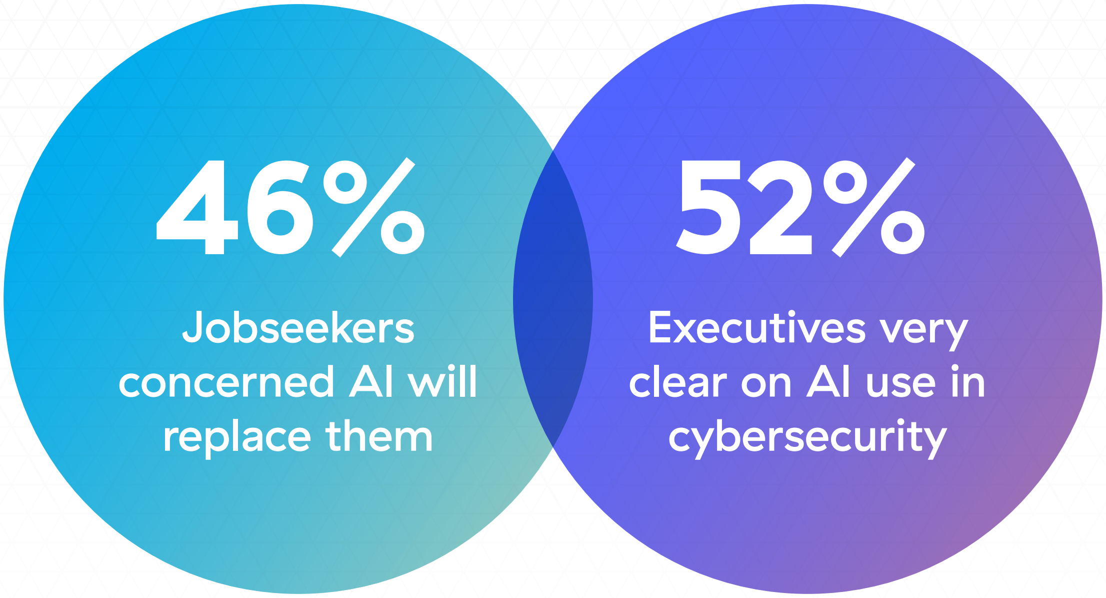
The researchers concluded that 3% of the internet content was completely AI generated, 46.1% was assisted by AI, and 50.9% was created by humans alone. Given public-facing LLM tools are a relatively new phenomenon, their heavy influence on internet content is remarkable. If this trend continues, most new internet content will soon be helped or created by AI.

Section Wrap Up

Section 1: Current AI prevalence

KEY TAKEAWAY	RECOMMENDED APPROACH
Large organizations across industries are adopting AI at a rapid rate.	Plan how your organization will adopt AI with fellow executives. Evaluate how your AI strategy may impact your technology, cybersecurity, organizational risks, and affect customer perception of your company.
Large Language Models (LLMs) are extremely popular with employees across industries.	Investigate how your employees are using LLMs. Is any proprietary data being submitted to third-party AI applications? Do the LLMs generate content aligned with your business values?
Almost half of recently surveyed internet content is AI-assisted or AI-generated.	Consider how your organization wishes to use AI generated content. Will your organization announce when content is AI generated? If not, how will customers react?

Section 2: AI concerns



46%

Jobseekers concerned AI will replace them

52%

Executives very clear on AI use in cybersecurity

The growing adoption of AI technologies has generated some negative sentiment and concerns among workers. People wonder how the technology may impact their jobs, and some worry it may replace them. Security professionals are worried about the disruption AI is causing across cybersecurity and its potential for malicious use. Understanding the concerns people have is key for leaders who want to integrate AI technologies into their organization.

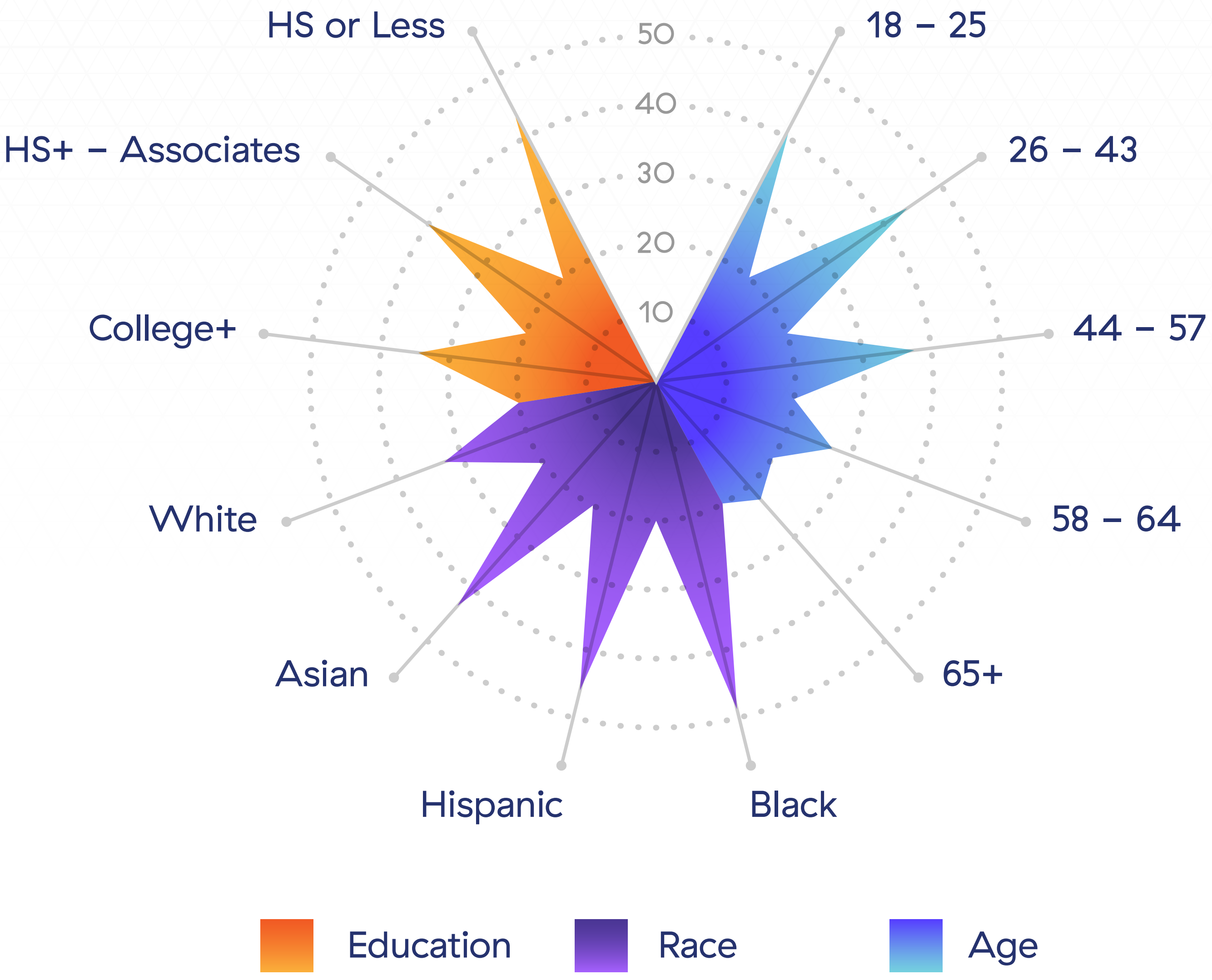
Key findings:

- Executives are considerably more confident that they understand of AI's use in cybersecurity than their employees
- People across age groups, ethnicities, and education levels are worried AI will replace them, with half the membership of some groups reporting anxiety
- Security professionals are wary of implementing AI due to concerns about data quality, transparency, data poisoning, and overcoming an employee skills gap
- AI can help threat actors discover vulnerabilities and create more effective phishing campaigns, deepfakes, and malware.

Fear of replacement

Workers across demographics and age groups are worried that AI may replace their job duties. These concerns were documented extensively in the American Psychological Association (APA) 2023 Work in America survey on artificial intelligence, monitoring technology, and psychological well-being. The results, drawn from the responses of 2,515 US adults, were grouped by age, ethnicity, and education to present a high-level view of AI anxiety.

Worried AI will replace job duties (%)

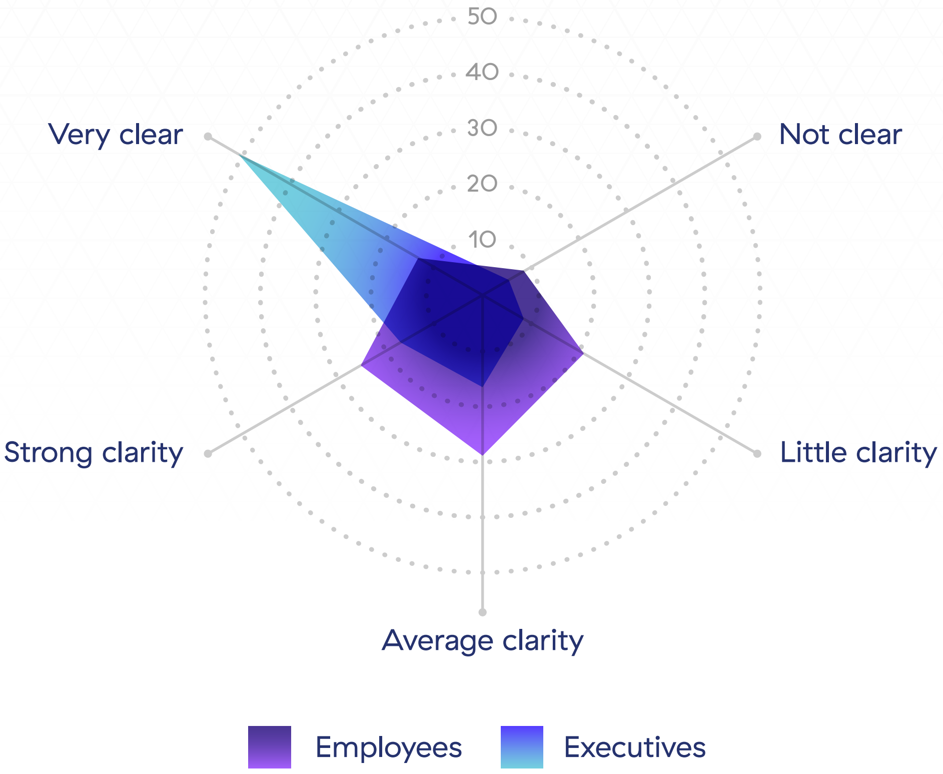


People concerned about losing work to AI according to the APA's 2023 Work in America survey

Another group concerned about AI are workers who plan on seeking new employment within a year. Among them, 46% reported being worried about AI replacing them. By knowing how different groups feel about AI, executives can have important and informed talks about this often-discussed topic. Being mindful of the apprehension employees feel about AI will help leaders address worker's concerns before introducing major changes.

Conversations about integrating AI into cybersecurity will benefit by focusing on use cases. Recent **research** by the **Cloud Security Alliance** (CSA) shows that executives have a much firmer grasp on this topic than their employees.

Clear on potential AI use cases in cybersecurity (%)



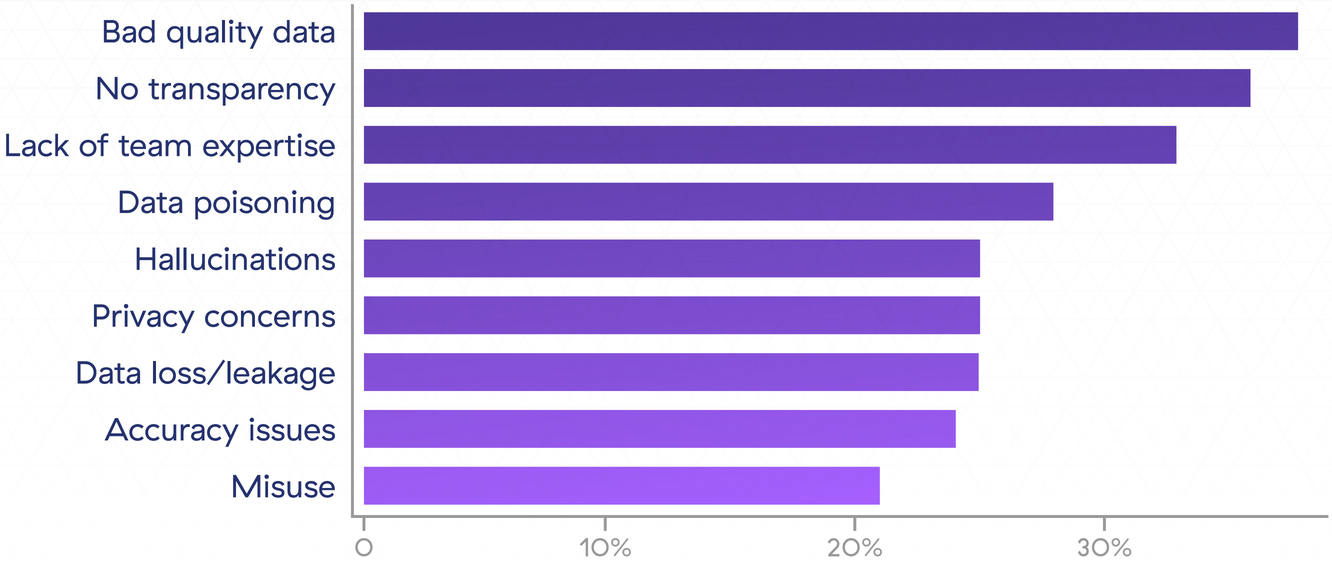
Executives have a much stronger understanding of how AI integrates with cybersecurity according to The State of AI and Security Survey Report (CSA)

The stark contrast between C-level and employee understanding on AI in cybersecurity is highlighted by the extremes. An impressive 52% of executives are very clear on potential use cases of AI in cybersecurity. Almost a third of employees (31%) report having little to no clarity on this subject. This indicates that organizational leaders pushing for AI-enabled cybersecurity measures should share their knowledge with concerned employees. Otherwise, such initiatives may create or exacerbate anxiety over AI in the workplace.

AI integration challenges

Understanding how to implement AI into cybersecurity does not mean knowledgeable security leaders do not have concerns of their own. The CSA's *The State of AI and Security Survey Report* found several AI issues that worry over a fifth of security professionals. Major concerns include bad data quality, AI's lack of transparency, data poisoning, and potential data loss.

Security professionals biggest concerns over using AI in cybersecurity



Security professionals are concerned about the training and opaque decision-making of AI models

Security experts have some doubts about AI, but most (63%) think the technology will benefit cybersecurity. Only 25% of respondents think AI will prove more helpful to attackers.

> "While AI threatens to overwhelm reactive security teams with the pace and sophistication of its onslaught, it can likewise enable proactive prevention through predictive processes and controls. "
>
> — NAT SMITH, SENIOR DIRECTOR OF PRODUCT MANAGEMENT, ZSCALER

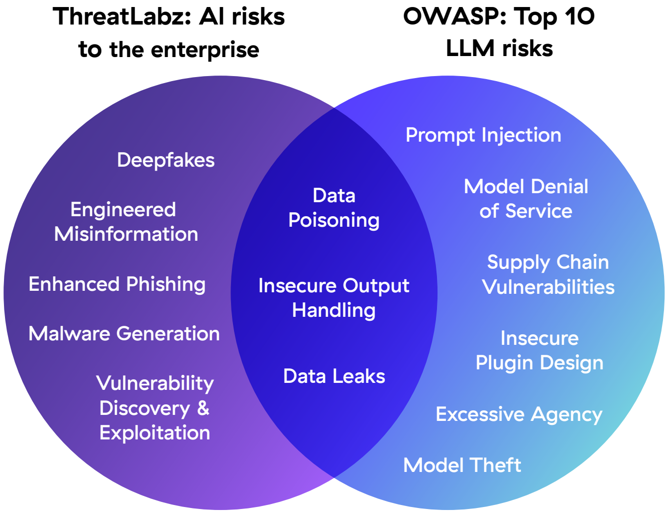
AI-generated, AI-assisted, and AI-native risks

The potential for AI tools to be used maliciously has stirred a lot of discussion among cybersecurity professionals. Executives and board members charged with addressing business risks are keen to stay ahead of a potential surge of AI-generated threats. How can AI help threat actors attack a business, and what can organizations do to remain safe?

The ThreatLabz 2024 AI security report lists the top three enterprise AI concerns as:

- **Protecting intellectual property and non-public information:** Safeguarding your enterprise against AI-leakage of proprietary data and private information is paramount. The mass exposure of GitHub passwords, API keys, and TLS/SSL certificates in 2023 demonstrates the risks of unrestrained and unmonitored AI tool use.
- **Data privacy and security risks of AI applications:** As AI applications and tools proliferate across the enterprise, it can be difficult to track how your organization's data is being used. Which tools are ingesting information training for data? Which have policies granting them ownership of submitted data? It is impossible to safeguard your organization's information without knowing what each AI tool does with the data your employees submit to it.
- **Data quality concerns – garbage in, garbage out:** It is difficult to know whether an AI tool will reliably provide desired performance without knowing how it was trained. An AI model's output is largely a product of the data set it trained upon, and any biases, blind spots, or misinformation therein. Recklessly adopting AI tools without investigating their training could lead to embarrassing and costly results should they make public-facing errors.

In addition to these enterprise business risks, ThreatLabz examined intentionally malicious uses of AI that attackers may employ against your organization. These include data poisoning, deepfakes, phishing, malware generation, and automated vulnerability discovery.



OWASP and ThreatLabz find overlapping AI risks between enterprise users and LLM creators

The Open Web Application Security Project (OWASP), famous for its Top 10 security threat lists, also examined major AI concerns. Their list, ***Top 10 for LLMs and Generative AI Apps***, looks at vulnerabilities in large language models and intentional misuse of the technology. Comparing AI-related enterprise risks with vulnerabilities inherent in the technology reveals that data poisoning, insecure output handling, and data leakage are common concerns. As such, any large-scale AI initiative at your organization should include countermeasures to ensure you are not exposed to preventable risks.

Section Wrap Up

Section 2: AI concerns

KEY TAKEAWAY	RECOMMENDED APPROACH
Employees across demographics and age brackets are concerned that AI will replace their job duties.	Decide how your organization should adopt AI with fellow executives. Put procedures in place to minimize business risk. Consider how customers and employees may react to your AI strategy.
Integrating AI into the business environment carries several inherent risks.	Investigate how your employees are using LLMs. Is any proprietary data being submitted to third-party AI applications? What do AI tools do with the data you submit?
Adversaries can threaten your organization by exploiting vulnerabilities in AI or using it to supplement their attacks.	Use automated and AI-driven technology to discover vulnerabilities within your environment before adversaries do. Understand how threat actors use AI in attacks and give targeted vectors extra attention.

Section 3: AI improves cybersecurity

78%

Organizational leaders think AI will improve detections

468%

Predicted increase of investments into AI by 2027

Cybersecurity specialists, like other professionals, are intrigued by AI and its potential applications in their field. Security leaders are particularly interested in using AI to predict threats and detect attacks. Properly implemented, AI can multiply productivity by automating repetitive tasks, scanning logs, tracking data, detecting anomalies in the environment, and more. Many of the AI-based tactics adversaries use to discover vulnerabilities in your environment can also be used by your security team to fix them.

Key findings:

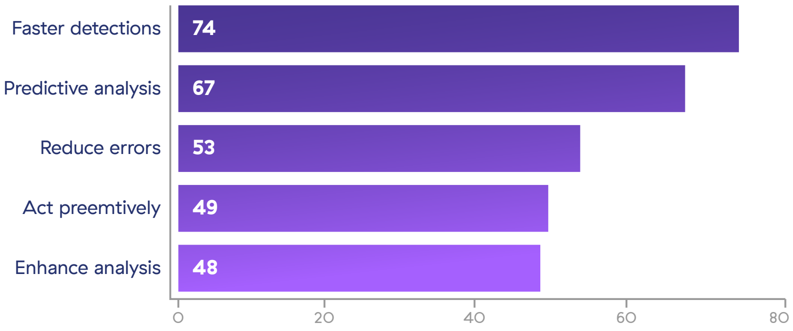
- AI is effective at attack surface discovery, compromise prevention, stopping lateral movement, and protecting data
- Leaders of organizations are looking to AI for its predictive capabilities, speed, and ability to automate tasks
- Market analysts predict AI will be a $468 billion industry by 2027

While AI introduces many new security concerns it also delivers significant cybersecurity benefits. When evaluating AI-enabled cybersecurity solutions leaders should distinguish fact from marketing hype. Here are four areas where AI is improving cybersecurity:

- **Attack surface discovery:** AI tools can automatically discover known vulnerabilities within the enterprise, and on public-facing digital assets. Organizations can use this information to fix security problems before attackers discover and exploit them.
- **Compromise prevention:** AI can be trained to discover attacker infrastructure (the internet assets adversaries use to carry out attacks) and preemptively block them. It can also detect anomalous traffic and access patterns in your environment and alert security teams before a breach occurs.
- **Lateral movement prevention:** Lateral movement is a key part of many cyberattack strategies. Moving freely across an organization's infrastructure is dangerous in traditional enterprises where users, apps, and data are hosted on the same network. AI can reduce the risks of lateral movement by suggesting network segmentation policies and access restrictions based on user role and behaviors.
- **Data exfiltration:** Classifying, monitoring, and tracking data can be an extremely time consuming exercise for security teams. However, AI can automate data classification, monitoring, and create effective data policies, making data loss prevention (DLP) faster and simpler.

The potential benefits of integrating AI into cybersecurity extend far beyond these four use cases. Gartner, an analyst firm, asked decision-makers (directors, VPs, and C-suite) how AI will improve cybersecurity. Their survey included respondents from North America, APAC, and EMEA managing companies ranging from less than a thousand employees to over ten thousand.

Anticipated benefits of AI in cybersecurity according to decision-makers



Gartner survey of organizational leaders finds they favor the predictive capabilities and detection speed of AI

The positive sentiment behind AI is expected to drive market investment in artificial intelligence technology to $407 billion by 2027 according to Forbes. If achieved, this would represent a 468% increase over its value in 2022. Multiple trends in AI adoption and investment indicate that AI is on a sustained growth trajectory with no immediate signs of slowing down. Staying informed of the uses, risks, and capabilities of AI will continue to benefit leaders in the private and public sector.

Section Wrap Up

Section 3: AI improves cybersecurity

KEY TAKEAWAY	RECOMMENDED APPROACH
AI is effective at disrupting specific stages of cyber attacks when properly integrated into the cybersecurity posture.	Discuss which capabilities of AI will best benefit your organization with fellow leaders and your cybersecurity team.
Organizational leaders are bullish on the speed, predictive power, and automation potential of AI technologies.	Consider what aspects of your business could benefit from automation and predictive analytics. Discuss whether adopting AI for these use cases is feasible with the security team.
Market research predicts AI will continue to be increasingly integrated into business operations.	Ask for use cases from everyone in the company. Your business, legal, and technology leaders can and plan for AI integration while keeping security, regulations, and risks in check.

Additional Resources

CXO REvolutionaries

An executive-level resource for actionable, practical, and real-world examples for creating enterprise change through digital transformation initiatives.

Podcasts: Executive-oriented technology podcasts including "The CISO's Gambit," "The CIO Evolution," and "Cloudy with a Chance of Trust."

LinkedIn: Social media updates related to executive events, insights, and content releases.

CXO REvolutionaries

SPONSORED BY: zscaler™

About CXO REvolutionaries

CXO REvolutionaries drive zero trust and digital transformation thought leadership for the global CXO community. Explore our educational and informational resources for insights on successfully transforming your organization’s IT and cybersecurity.

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.

This report has been created by Zscaler for informational purposes only and may not be relied upon as legal advice. We encourage you to consult with your own legal advisor with respect to how the contents of this document may apply specifically to your organization, including your unique obligations under applicable law and regulations. ZSCALER MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT AND IT IS PROVIDED “AS-IS”. Information and views expressed in this document, including URL and other internet website references, may change without notice.