SWIMLANE

Reality Check

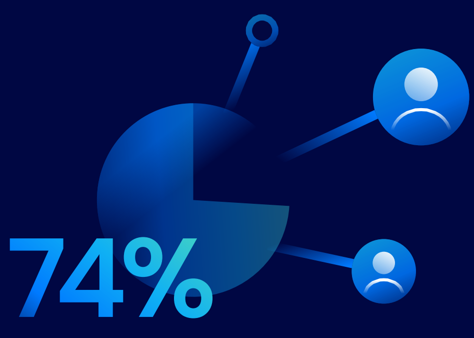
Is AI Living Up to Its Cybersecurity Promises?

AI is raising discussions about its responsible use, including challenges related to data security, privacy, accountability, and pervasive hype that can lead to fatigue.

Swimlane surveyed 500 cybersecurity decision-makers in the US and UK to illuminate the growing need for a balanced approach to AI adoption, one that addresses both the opportunities and risks associated with this technology.

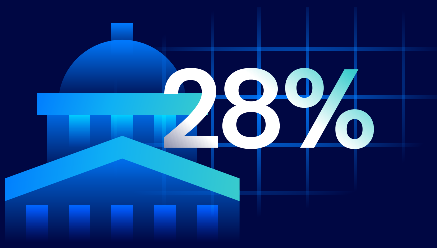
Is AI Making It Impossible to Balance Innovation and Confidentiality?

70% of organizations have protocols for sharing data with a public Large Language Model.

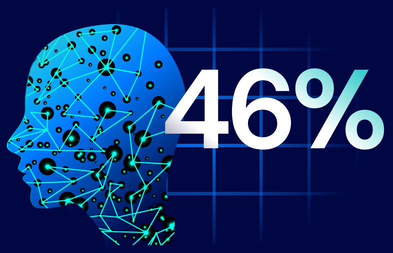


74% of organizations have individuals inputting sensitive data into a public Large Language Model.

Who Should Govern AI?

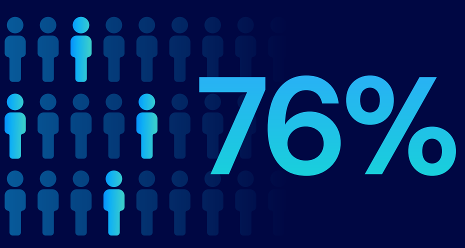


Only **28%** believe the government should be responsible for setting and enforcing guidelines.

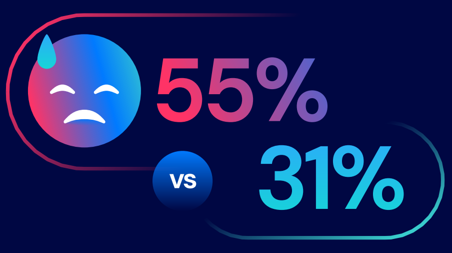


46% believe the AI developer should be primarily responsible for harm caused by AI systems.

AI Hype or Growth Engine?



76% believe the current market is saturated with AI hype.

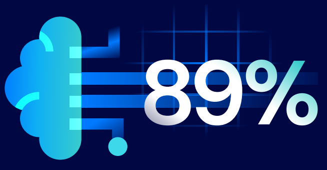


55% are starting to feel fatigued by the constant focus of AI, while 31% disagree.

Are AI Skills Essential to the Cyber Workforce?

86% said AI and Machine Learning experience is influencing hiring decisions.

Will AI Adoption Fuel Efficiency Gains and Increased Budgets?



89% report that GenAI and LLMs improved productivity and efficiency for their cybersecurity teams.

33% have over 30% of their (current cybersecurity) budget allocated to AI solutions.

90% anticipate an increase in the overall cybersecurity budget in 2025.

Dual-Edged Nature of AI Technology

While AI can enhance security and efficiency, it also brings significant risks that must be managed carefully. By automating routine tasks and enhancing threat detection, AI empowers human experts to focus on complex and strategic challenges.

Download the full report here. ↗