

# **AITHREAT**

## LANDSCAPE REPORT



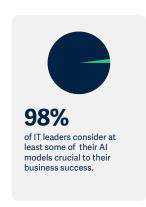
**Overview** 

To help understand the evolving cybersecurity environment, we developed the 2024 AI Threat Landscape Report as a practical guide to understanding the security risks that can affect every industry and to provide actionable steps to implement security measures at your organization.

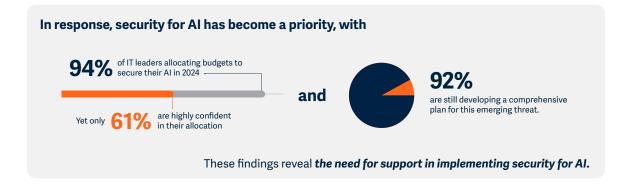
### **SURVEY FINDINGS**

We commissioned a survey of 150 security and data science leaders to reveal the current state of securing AI. The survey uncovered AI's widespread utilization by today's businesses, but there's still a lot of work to be done to implement proper security measures.









#### **RISKS INVOLVED WITH AI USE**

Adversaries can use a variety of methods to utilize Al to their advantage. The most common include:

- Manipulation to give biased, inaccurate, or harmful information.
- Creation of harmful content, such as malware, phishing, and propaganda.
- Development of deep fake images, audio, and video.

### **COMMON TYPES OF ATTACKS ON AI**

There are three major types of attacks on Al:

- Adversarial Machine Learning Attacks
- Generative Al System Attacks
- Supply Chain Attacks

GET THE FULL REPORT →









