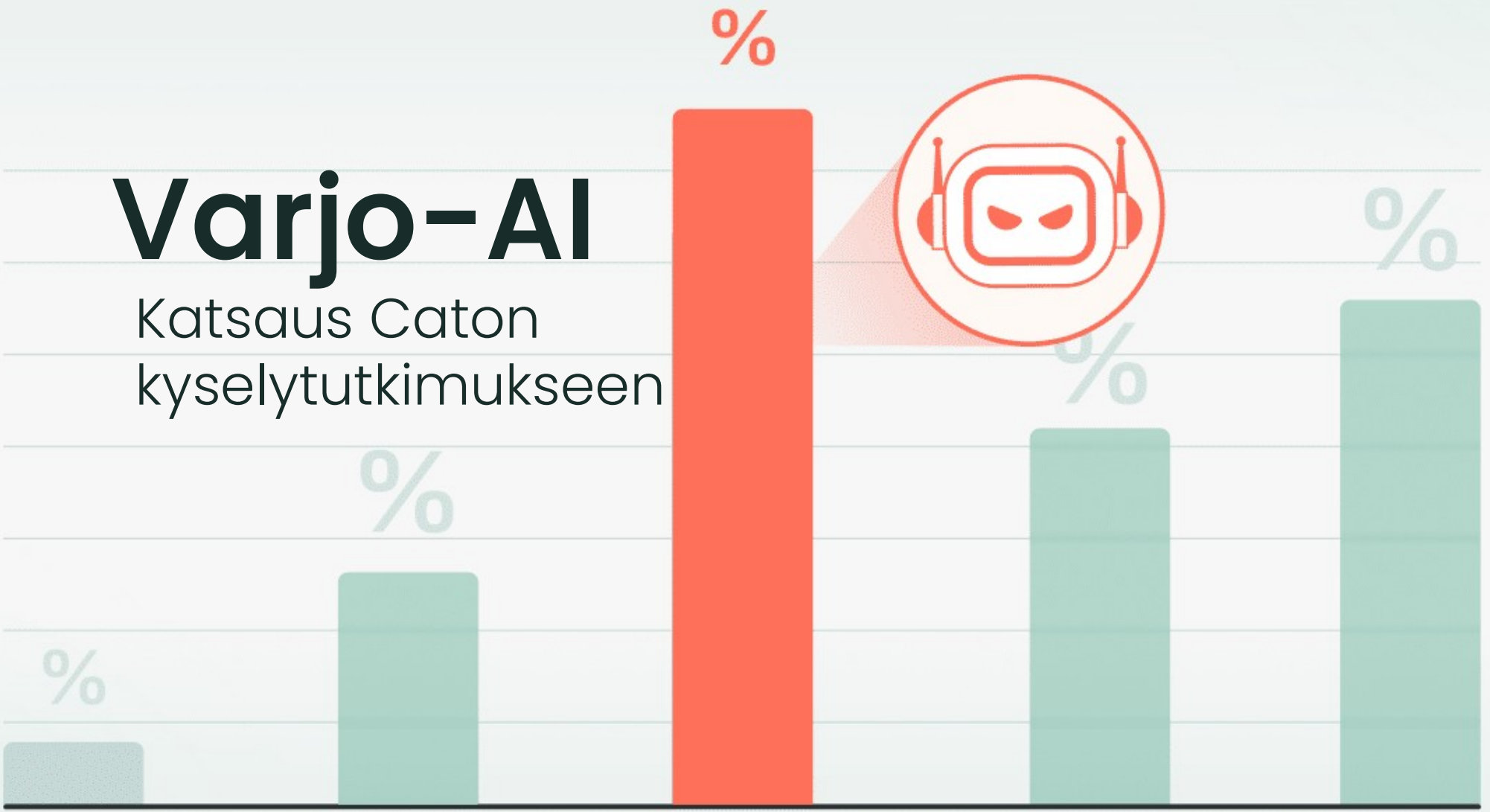
Varjo-AI

Katsaus Caton
kyselytutkimukseen

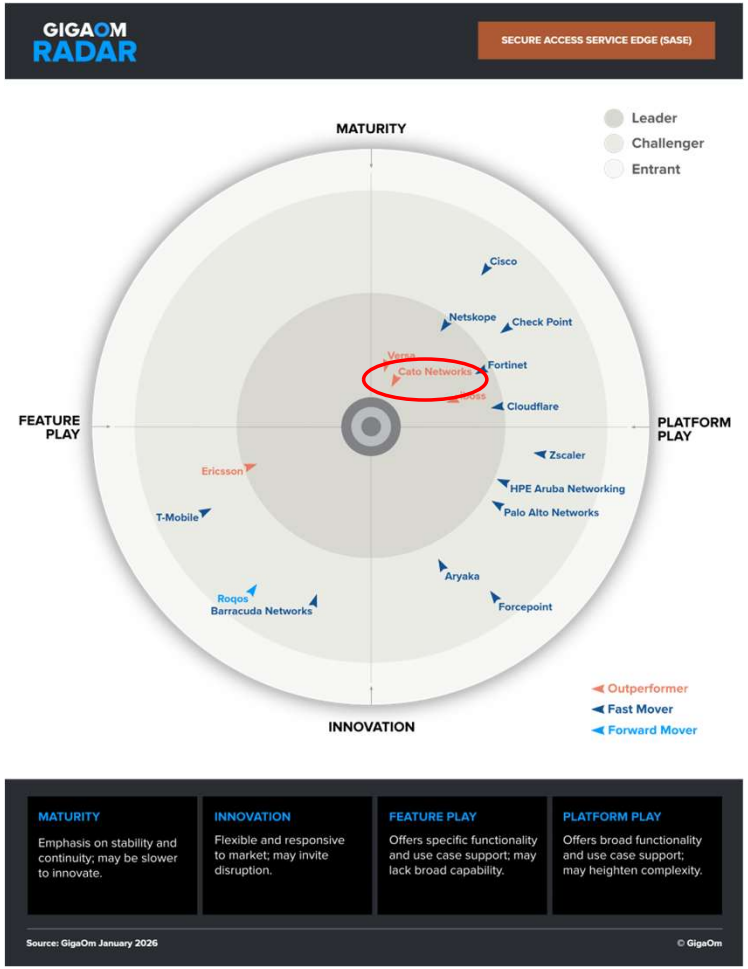


tommi.saxelin@catonetworks.com

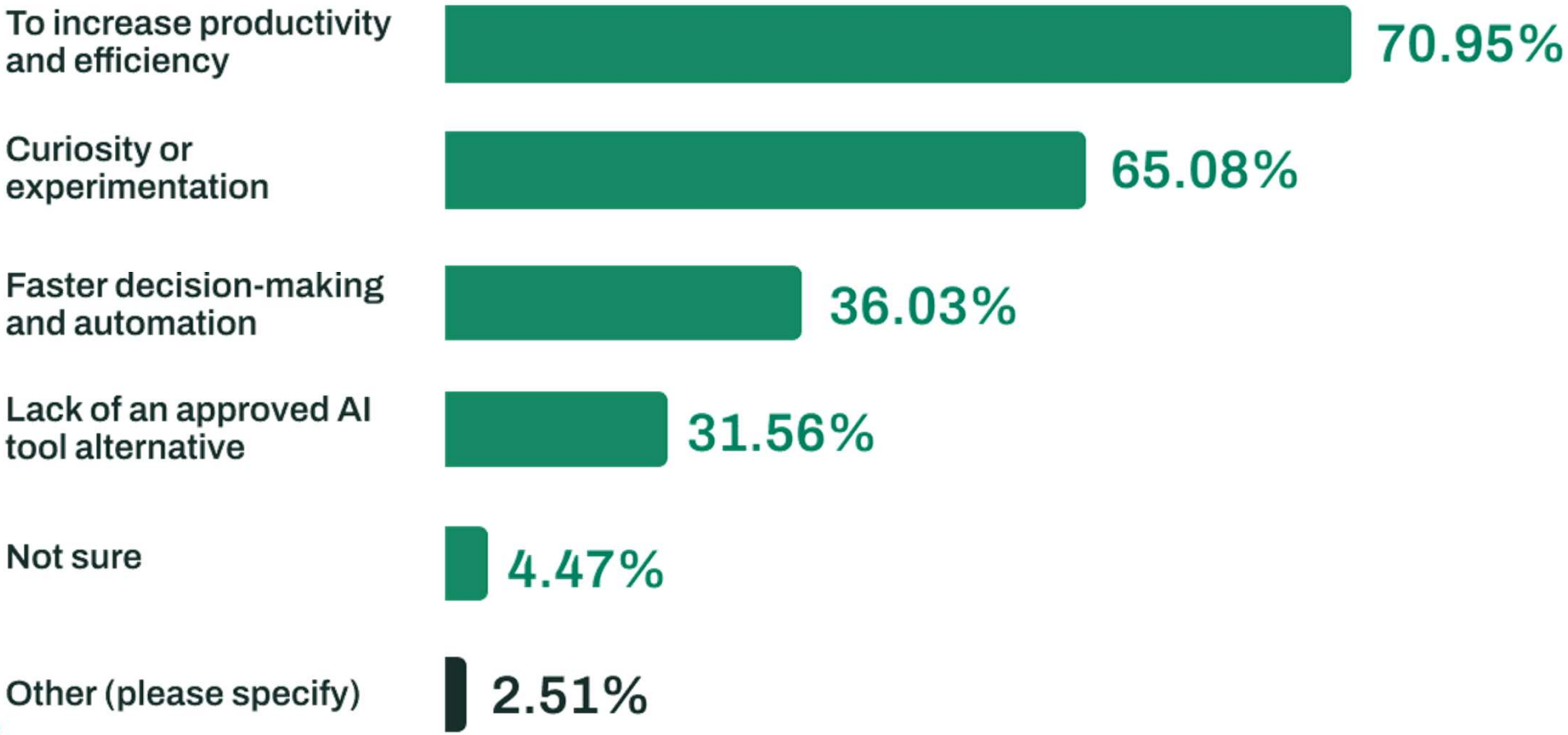
Cato Networks

Figure 1: Magic Quadrant for SASE Platforms

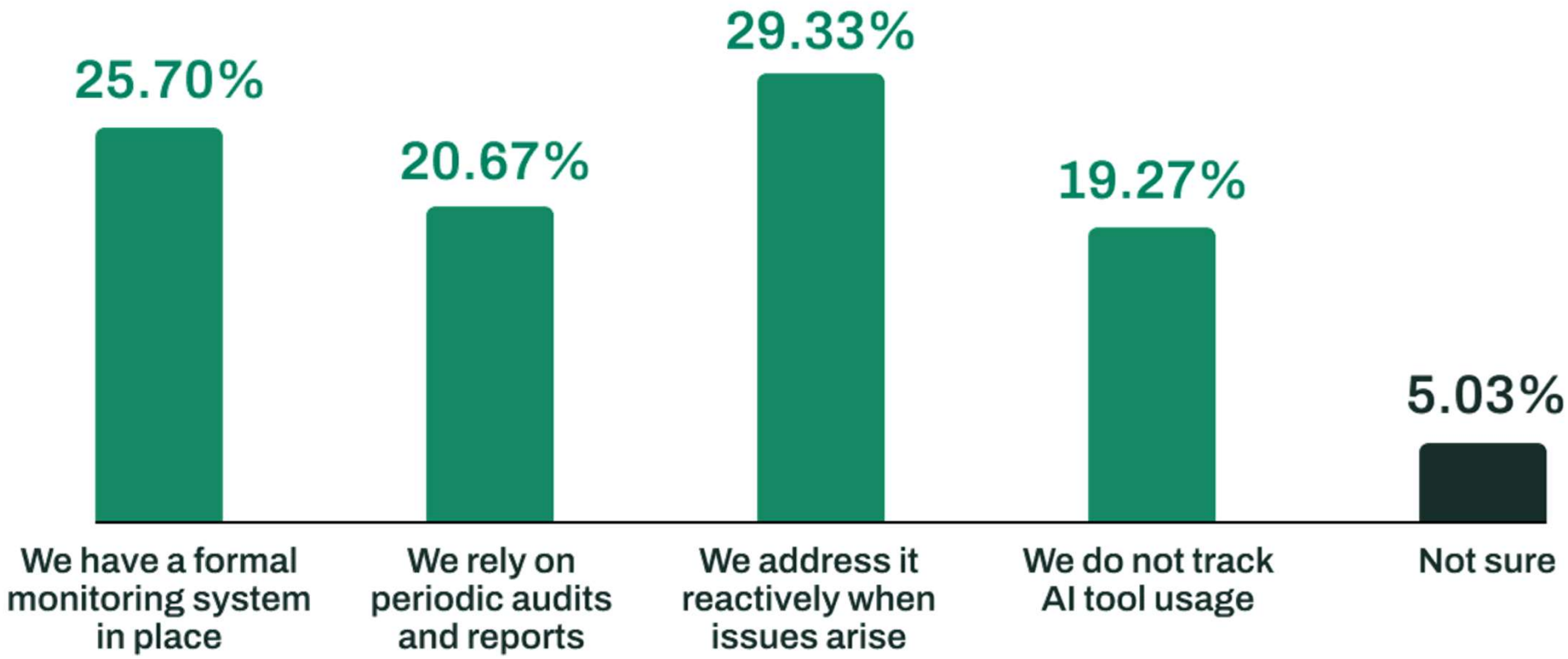
Gartner



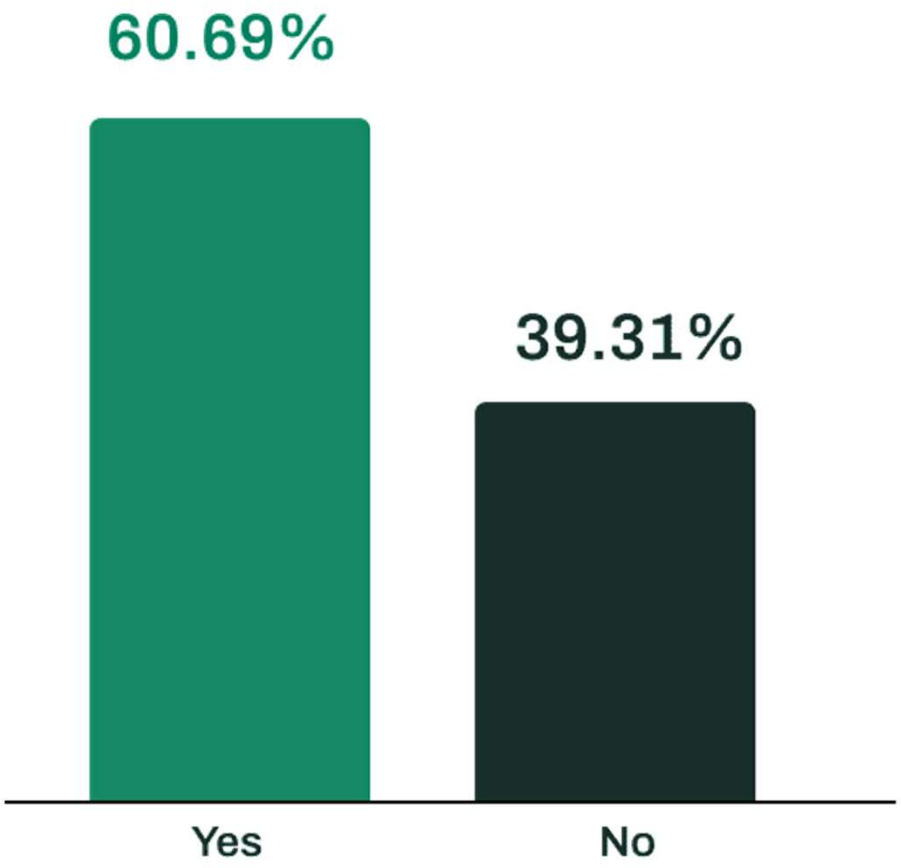
What are the primary reasons employees use unapproved AI tools?



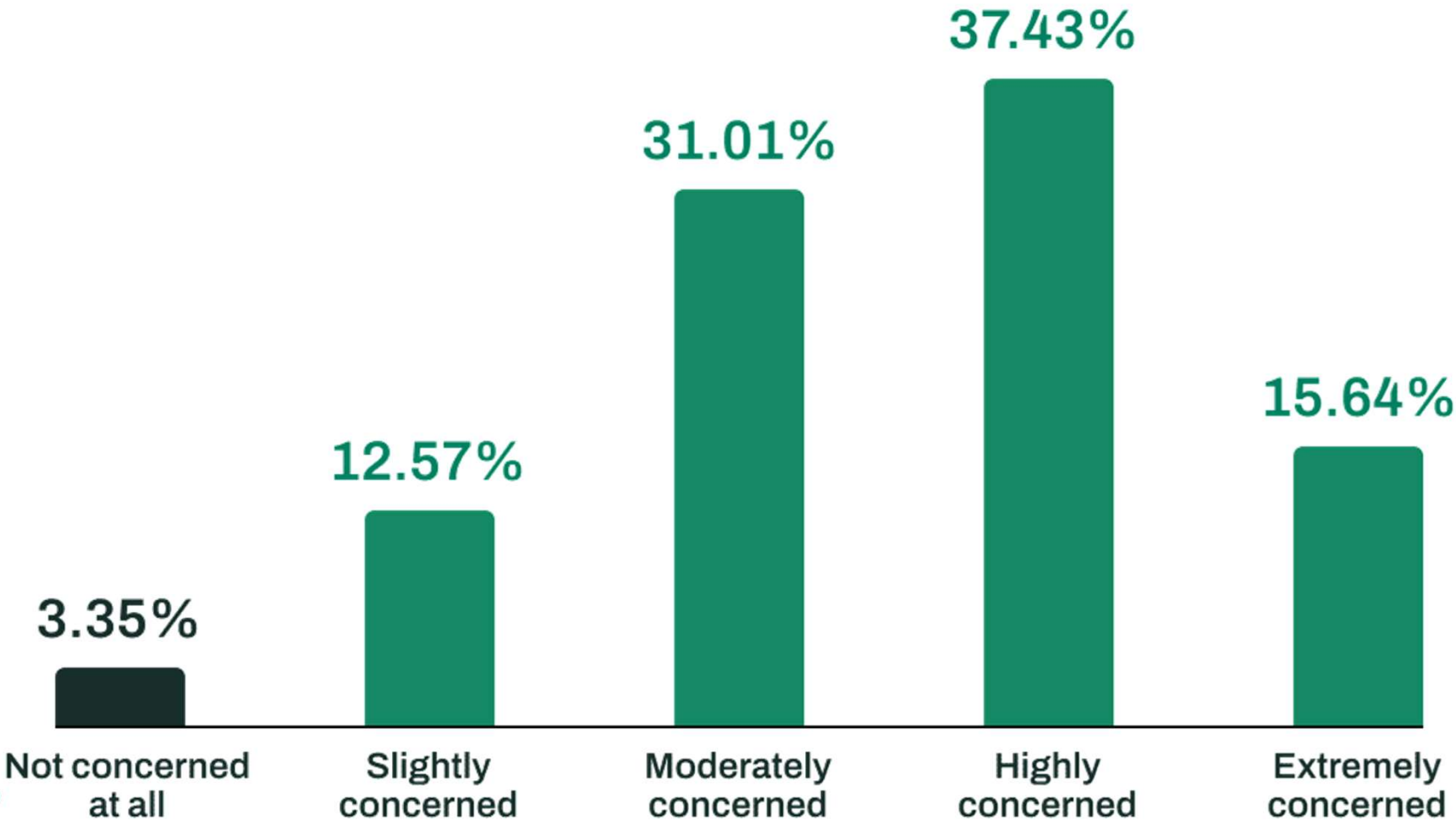
How do you currently monitor or track unauthorized AI tool usage within your organization?



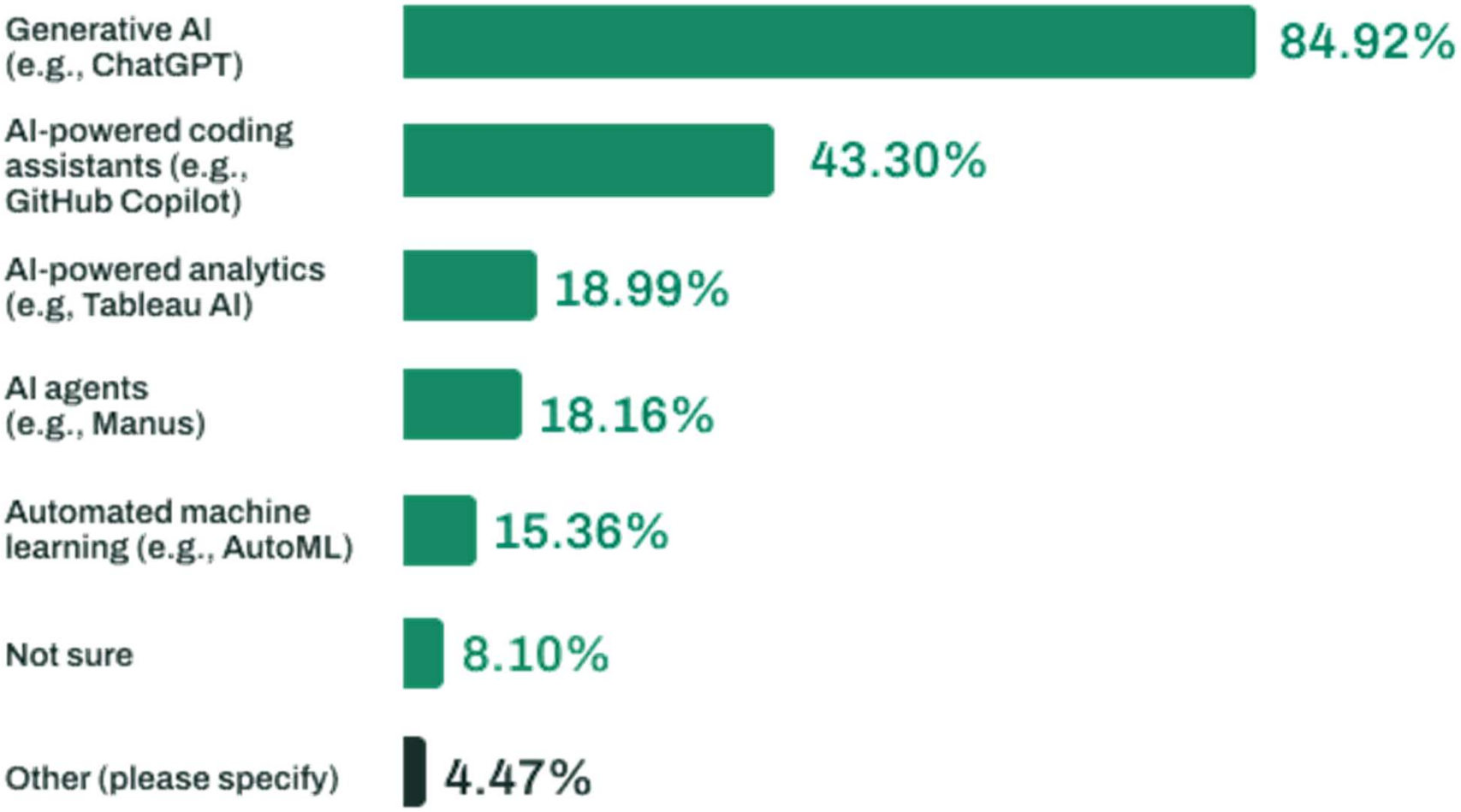
Have you found unauthorized AI tools being used within your organization?



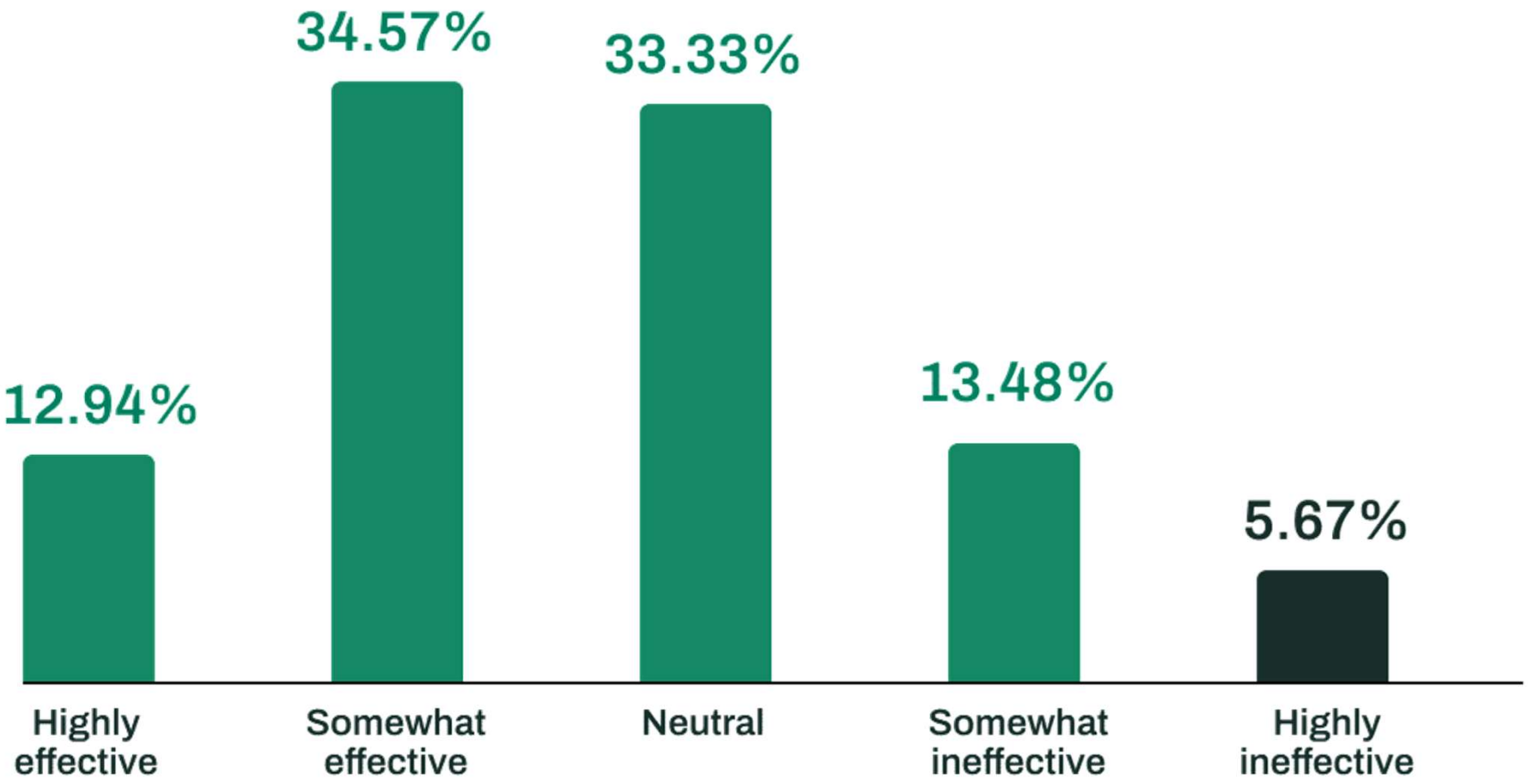
How concerned are you about data security risks associated with the usage of unauthorized AI tools?

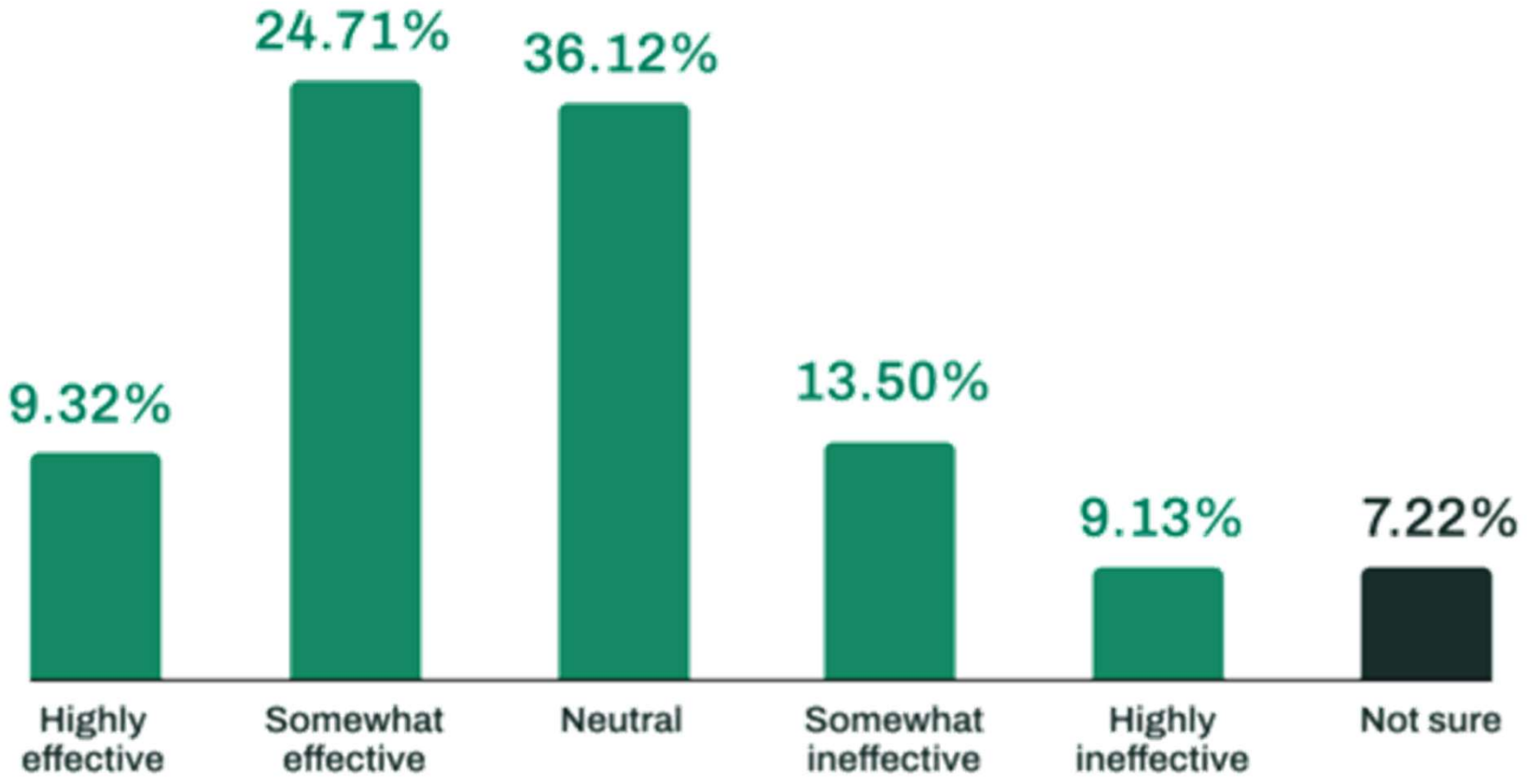


What types of shadow AI applications have employees in your organization used without formal approval?



How effective would you consider your organization's response to managing shadow AI risks?




How effective do you believe your organization's current defenses are against AI-generated cyber threats (e.g., deepfakes, prompt injection, AI hallucinations)?
9.32%
24.71%
36.12%
13.50%
9.13%
7.22%
Highly effective
Somewhat effective
Neutral
Somewhat ineffective
Highly ineffective
Not sure

The Cato AI Security Solution

Protecting the AI You Use — and the AI You Build.

AI Security for Users

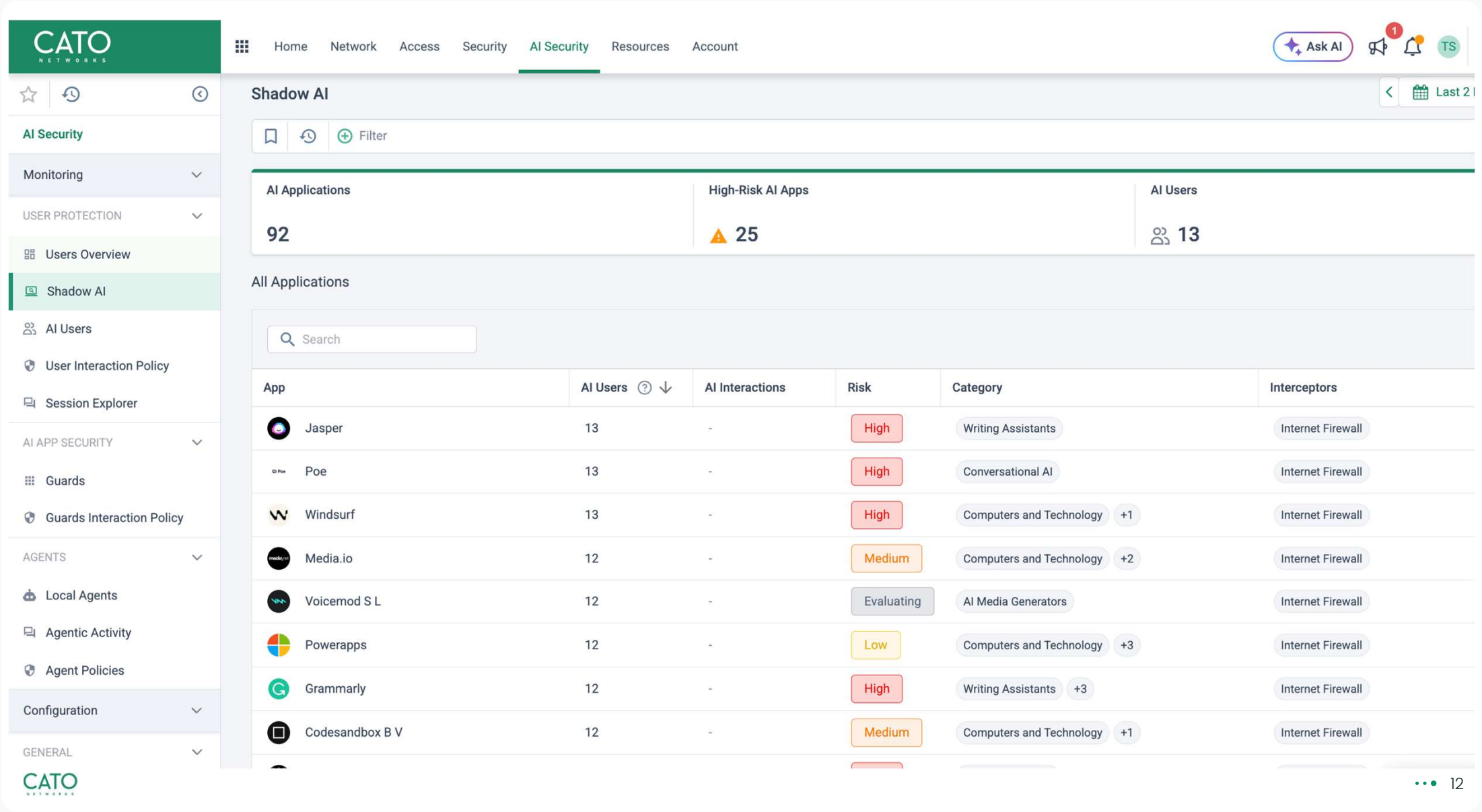
Enabling safe, governed use of AI productivity tools without sacrificing security or compliance.

- **Shadow AI Discovery**
  Discover every AI tool in use, sanctioned or not
- **Prompt & Action Visibility**
  See what is being shared and control what is allowed
- **AI Interaction DLP**
  Prevent sensitive data from leaving through prompts and responses
- **Agentic AI Visibility**
  Discover and monitor AI agents accessing data and systems

AI Security for Apps

Securing homegrown applications and agents that use AI — protecting against model abuse, data leakage, and unauthorized actions.

- **AI App & Agent Inventory**
  Discovery of all AI applications and agentic workflows
- **AI Firewall (Runtime Protection)**
  Block prompt injection, model abuse, and unauthorized agent actions
- **Data Exfiltration Prevention**
  Stop sensitive data leaving through AI API calls and responses
- **Agentic Policy Enforcement**
  Define and enforce what every agent is allowed to do


CATO NETWORKS
Home
Network
Access
Security
AI Security
Resources
Account
Ask AI
TS
Shadow AI
Last 2
AI Security
Monitoring
USER PROTECTION
Users Overview
Shadow AI
AI Users
User Interaction Policy
Session Explorer
AI APP SECURITY
Guards
Guards Interaction Policy
AGENTS
Local Agents
Agentic Activity
Agent Policies
Configuration
GENERAL
Filter
AI Applications
92
High-Risk AI Apps
25
AI Users
13
All Applications
Search
App
AI Users
AI Interactions
Risk
Category
Interceptors
Jasper 13 - High Writing Assistants Internet Firewall
Poe 13 - High Conversational AI Internet Firewall
Windsurf 13 - High Computers and Technology +1 Internet Firewall
Media.io 12 - Medium Computers and Technology +2 Internet Firewall
Voicemod S L 12 - Evaluating AI Media Generators Internet Firewall
Powerapps 12 - Low Computers and Technology +3 Internet Firewall
Grammarly 12 - High Writing Assistants +3 Internet Firewall
Codesandbox B V 12 - Medium Computers and Technology +1 Internet Firewall

CATO
NETWORKS

Thank you