cyberhaven

2026 AI Adoption & Risk Report

Manufacturing

Cyberhaven Labs

Introduction

Since the launch of ChatGPT in 2022, AI has become one of the fastest-adopted workplace technologies in history.

What began as individual experimentation has rapidly evolved into tools embedded in core business workflows. The speed of this shift, from novelty to operational dependency, has often outpaced enterprises' ability to understand, govern, and secure AI usage.

Cyberhaven Labs' 2025 research captures this shift, analyzing usage across generative AI SaaS, endpoint AI applications, and AI agents. Leveraging billions of real-world data movements from 222 companies, we measured adoption via active users and event-level activity, revealing not just presence, but deep integration into workflows.

While traditional chat-based GenAI SaaS adoption is plateauing, AI coding assistants, browser-based agents, and custom AI agents are growing rapidly, operating inside development environments and workflows with limited oversight.

As AI becomes infrastructure rather than a standalone interface, security risks intensify: employees are inputting source code, financial data, and intellectual property into a fragmented ecosystem of tools, many outside traditional IT visibility, across personal accounts and SaaS platforms without enterprise-grade security. Shadow adoption increases, controls are inconsistent, and risk accumulates faster than organizations can manage.

These risks are real, material, and concentrated among aggressive adopters.

This report provides a data-driven view of 2025 enterprise AI usage, highlighting where adoption is accelerating and where security risk is compounding across manufacturing enterprises. By analyzing real-world patterns across industries, departments, tools, and data types, Cyberhaven Labs helps security and technology leaders understand not just the scale of adoption, but the context needed to govern AI safely in 2026.

1

An AI Adoption Gap is Emerging

Artificial intelligence (AI) and large language models (LLMs) are becoming increasingly embedded in organizational workflows.

Today, 62% of organizations[1] are experimenting with AI agents, enterprises are spending four times more on AI software than on traditional software, and 74% of executives stated[2] they achieve returns within the first year of AI tool deployment.

The manufacturing industry is no exception. A survey by Cisco found that 59% of manufacturers surveyed reported that they had already actively deployed AI at scale, while a Research and Markets report showed that the global AI in manufacturing market is expected to rise from $34 billion in 2025 to $155 billion by 2030.

However, AI adoption is not unfolding as a steady, industry-wide wave. Instead, it is becoming increasingly polarized.

A widening gap is emerging between AI early adopters and organizations that remain hesitant to embrace these technologies.

Frontier enterprises — those in the 99th percentile of GenAI adoption — were interacting with hundreds of GenAI applications over the course of 2025. In the most advanced cases, organizations are using almost 300 GenAI tools. By contrast, cautious enterprises, making up the 5th percentile, typically employ around 30 GenAI tools.

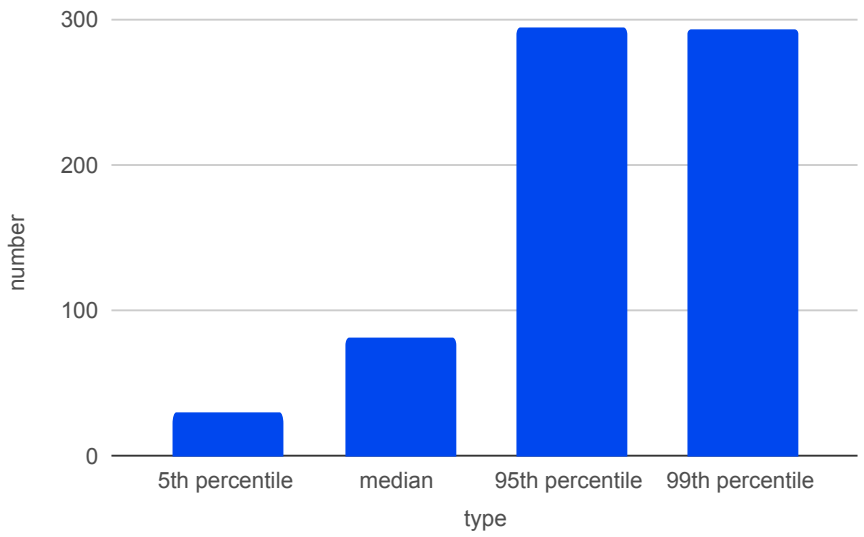
That is a 10x difference.

1 https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai

2 https://blog.arcade.dev/ai-integration-platform-trends

GenerativeAI SaaS

Distribution of Number of GenAI SaaS Applications Used by an Enterprise



Most Organizations Remain Hesitant to Adopt AI

While frontier organizations are rapidly experimenting with GenAI, the majority of enterprises remain cautious. Manufacturing organizations have cited "reliable networks, stronger cybersecurity and better IT/OT collaboration" as barriers to AI adoption. The median manufacturing enterprise utilizes less than a third of the volume utilized by the 99th percentile.

This polarized adoption pattern reveals two realities. Some organizations are aggressively adopting AI and may realize outsized gains in innovation and growth. At the same time, these frontier enterprises are also assuming a disproportionate share of AI risk.

As data flows through hundreds of GenAI tools, rapid adoption multiplies risk points, governance complexity, and potential sensitive data exposure. Many organizations appear to be trading coordination and security controls for experimentation, creating a growing gap between AI adoption and AI security. This challenge is further amplified by uneven employee adoption rates, making one-size-fits-all AI security approaches ineffective. Effective AI security will depend not only on which tools are deployed, but on how and by whom they are actually used.

2

Top GenAI Apps Used By Manufacturing Organizations

1. chatgpt.com
2. app.devin.ai
3. gemini.google.com
4. chat.deepseek.com
5. copilot.microsoft.com
6. doubao.com
7. claude.ai
8. zerogpt.com
9. perplexity.ai
10. grok.com
11. midjourney.com
12. sora.chatgpt.com
13. aistudio.google.com
14. elis.rossum.ai
15. poe.com
16. higgsfield.ai
17. kimi.moonshot.cn
18. chatgptwriter.ai
19. elevenlabs.io
20. app.roboflow.com
21. notebooklm.google.com
22. krea.ai
23. blackbox.ai
24. openart.ai
25. ai.azure.com

When we compare this top 25 list to the top 25 GenAI applications used across industries, a few outliers emerge, as 11 GenAI applications appear here that did not appear in the industry-agnostic list. These applications, such as openart.ai, higgsfield.ai, and ElevenLabs are centered around multi-media creation, while others are clustered around computer vision, robotics, and model prototyping. Manufacturing appears to be utilizing AI applications more for industry-specific needs rather than the knowledge-work and productivity assistants more common across other industries.

Most GenAI SaaS Tools Are Objectively Risky

When GenAI tools are evaluated by risk level, the results are stark. Across the top 100 most-used GenAI SaaS applications within manufacturing, **80.5%** are deemed "medium," "high," or "critical" risk. Even when excluding "medium" risk and considering only "high" and "critical," **67%** of tools still fall into these categories.

For security leaders, this means that most AI usage today occurs in tools that would not meet traditional enterprise risk standards, yet employees continue to input sensitive data into them at high rates.

Agentic AI Adoption Slower Among Manufacturing Orgs

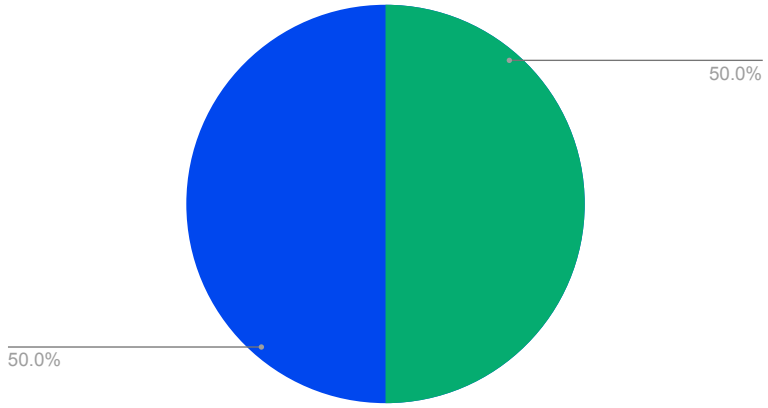
Workplace AI is entering a "second wave," moving beyond general-purpose tools to more specialized applications that directly enhance workflows. Coding assistants and AI agents are no longer niche experiments. Instead, they are rapidly becoming embedded in the daily operations of developers and teams across enterprises.

However, when we compare the manufacturing industry to others, we see a major shift in adoption trends. Across industries, **77.3%** of organizations are building with agentic SaaS platforms such as Glean or CoPilot Studio. For manufacturing specifically, that number drops to **50%**.

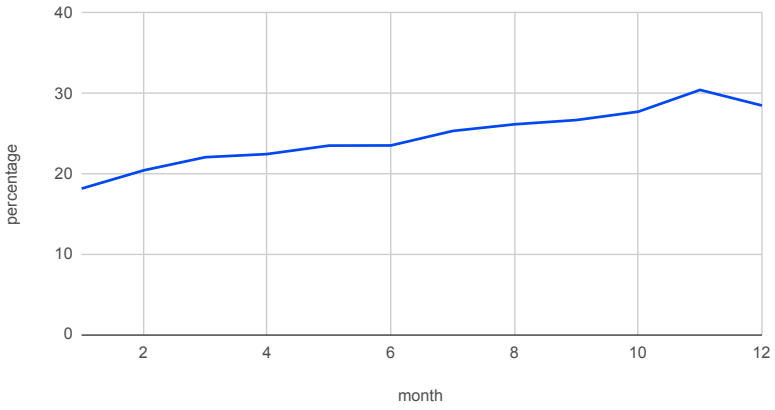
When we zoom in on the conditions under which many manufacturing organizations operate, however, this drop makes sense. Production factories often run on decades-old operational technology (OT) that was never designed to integrate with modern AI agents, and may not have the unified data layer needed for continuous and integrated data flows to AI agents. Additionally, manufacturing organizations contend with low risk tolerances, high regulation requirements, and are historically late-adopters of technology.

Additionally, the usage of AI Coding Agents, now rising in popularity, remained steady over 2025, growing roughly **10%** over 12 months. If we look at that same use case across industries, there was about a **30%** jump over the same time period. This stark difference highlights both the industry's slower adoption rate and how AI use cases vary industry by industry.

Percentage of Companies using Agent-building SaaS Platforms



Percentage of Developers Using AI Coding Assistants



Conclusion:

AI Security Is Paramount As Organizations Race To Adopt New Technology

AI adoption is accelerating, but unevenly. A small group of frontier organizations is driving rapid usage, while others move more cautiously. In many cases, innovation and experimentation are prioritized ahead of security and governance. At the same time, employees are actively using high-risk AI tools and inputting sensitive data across a growing ecosystem of GenAI applications, coding assistants, and custom agents.

For many organizations, this reflects an ungoverned environment where tools proliferate faster than policy, usage often exceeds visibility, and sensitive data moves across systems with limited centralized control. Without clear insight into how AI is used across teams, workflows, and data types, the gap between innovation and security will continue to widen.

As adoption diverges across industries, teams, and users, AI security must become a core priority. One-size-fits-all policies are unlikely to work. Effective governance depends on understanding real usage patterns and applying controls based on data sensitivity, user maturity, and tool risk.

The challenge is complex. The scale and speed of AI adoption make manual oversight insufficient. Many organizations will benefit from specialized security solutions that unify visibility, context, and enforcement across data, users, and AI systems. Those that invest early in comprehensive AI security will be best positioned to innovate with confidence while maintaining trust, compliance, and resilience.