When AI Connects the Factory

The New Path Away From Data Leakage & Downtime

AT-A-GLANCE

Key findings from ThreatLabz 2026 AI Security Report

Manufacturing has traditionally prioritized operational continuity over technology shifts. But stability and innovation are now aligning as artificial intelligence (AI) becomes part of core manufacturing operations. For the past three years, manufacturing has ranked among the top industries generating AI/ML traffic in the Zscaler cloud, confirming the prevalence and acceleration of AI across manufacturing environments. The ThreatLabz 2026 AI Security Report analyzed enterprise AI activity to better understand recent trends, providing manufacturing organizations insights on how their AI adoption usage compares to broader enterprise activity and its security implications.

Manufacturing drove 19.5% of global AI/ML transactions

ThreatLabz analysis found that the manufacturing sector accounted for 19.5% of all AI/ML traffic in the Zscaler Zero Trust Exchange™ in 2025, totaling 192.5 billion transactions, making it the second-most active industry overall. This level of activity confirms how widely AI applications and services are now used across production systems, cloud platforms, and factory environments, and for good reason.

AI applications support critical manufacturing functions, including detecting production issues earlier, improving quality control, and optimizing supply chain operations by analyzing production data and coordinating workflows in distributed environments. Supporting these functions requires AI to interact with factory equipment, enterprise systems, external services, and cloud platforms, creating additional pathways for operational data to move between IT, OT, and cloud environments.

While these capabilities help modernize factories, accelerate manufacturing innovation, and improve operational efficiency, they also expand the manufacturing attack surface. As a result, many manufacturing organizations are actively restricting AI usage.

Blocked AI activity underscores growing risk

Despite the wide usage and adoption of AI in manufacturing organizations, manufacturing, as an industry, accounted for 22.1% of all blocked AI/ML transactions in the Zscaler cloud in 2025. Blocking helps reduce obvious risks, such as:

- **Exposure of proprietary manufacturing processes and intellectual property**
- **Movement of sensitive data outside approved systems**
- **Limited visibility into how AI accesses data**

This risk profile helps explain why manufacturing organizations are limiting certain AI interactions from users and systems within their environments, particularly when sensitive operational data and production-related information are involved.

At the same time, restricting AI can mean missing out on productivity gains and new ways to optimize operations. Security teams must ultimately balance reducing risk with enabling the safe use of AI.

Securing AI across manufacturing environments

As AI adoption continues to accelerate, the new path forward is end-to-end AI security, understanding where AI is used, gaining control over how it interacts with operational systems, and implementing safeguards to prevent unintended access or data exposure.

Without proper controls, AI creates potential new pathways to production systems and sensitive data, increasing the risk of unauthorized access, lateral movement, data leakage, and operational downtime.

KEY SECURITY PRIORITIES FOR MANUFACTURING INCLUDE:

Visibility into AI usage

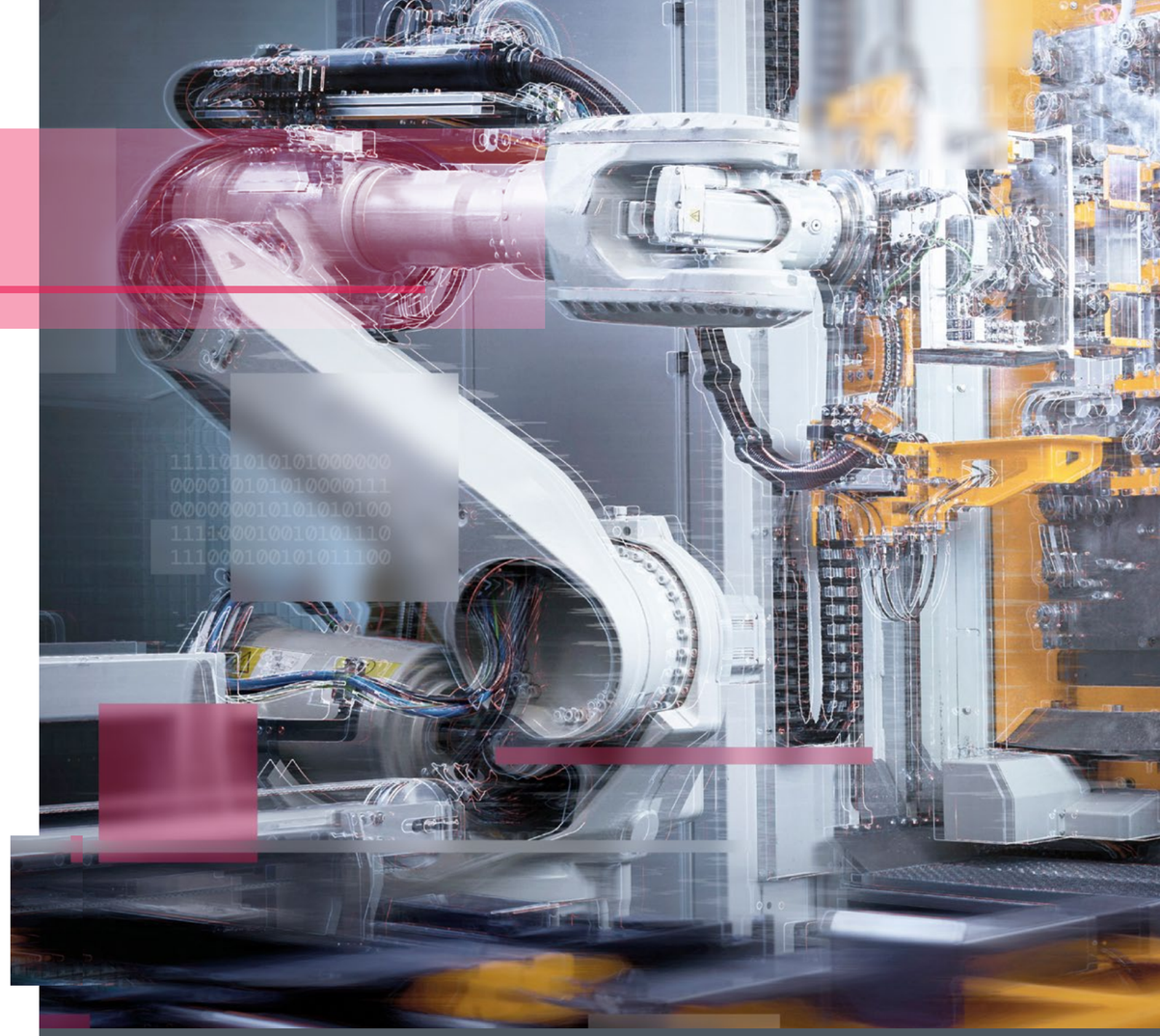
Gain full visibility into AI applications, models, and services accessing factory systems, industrial control environments, and enterprise platforms, including shadow and embedded AI.

Protection of sensitive operational data

Prevent exposure of production data, intellectual property, and proprietary processes by enforcing inline data protection and security policies across AI interactions.

Control over AI system access

Govern how AI systems connect to operational technology, manufacturing systems, and other critical resources using least-privileged access and zero trust controls.



DIVE DEEPER

Read the ThreatLabz 2026 AI Security Report

Learn more about enterprise AI usage patterns and risks, the evolving AI-powered threat landscape, and strategies to secure AI adoption in modern manufacturing environments.

Read Now

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

zscaler™

Act Fast.
Stay Secure.