November 2026
InfoBrief
Sponsored by NTT DATA

Accelerating Competitive Advantage in Manufacturing and Automotive Sectors: Private and Sovereign AI

How to Plan, Design, and Implement AI Factories to Meet Sovereign AI Objectives



Lorenzo Veronesi
Associate Research Director, IDC Manufacturing Insights

Table of contents

Click any title to navigate directly to that page.

Across global markets, enterprise adoption of AI is accelerating as it becomes more critical to business success 3

AI-driven transformation in manufacturing 4

Sovereign AI and private AI: Rewriting how AI is built, governed, and scaled 5

Sovereign AI and private AI: Where the complexity shows up 6

The automation gap must be bridged to enable scaling AI successfully across private and public AI 7

In manufacturing, organizations redesigning for private and sovereign AI today are creating a lasting advantage 8

AI is reshaping manufacturing, but fast adoption demands responsible AI governance to protect operational continuity, IP, and compliance across OT and IT environments 9

De-risking AI adoption in manufacturing with private and sovereign AI 11

Manufacturers must address three layers: OT and IT data, the AI model, and hybrid infrastructure 12

Engineered AI factory approaches can help simplify, speed up, and secure enterprise AI solutions 13

AI factories in action 14

AI factories in action: IP-driven product innovation 16

From pilot to production: Steps to full-stack sovereign AI in manufacturing 17

Expert partners help accelerate sovereign AI time to value, reduce risk, and boost ROI 18

About the IDC analyst 19

Message from the sponsor 20

Across global markets, enterprise adoption of AI is accelerating as it becomes more critical to business success

AI is driving the **strongest IT spending growth** since 1996.

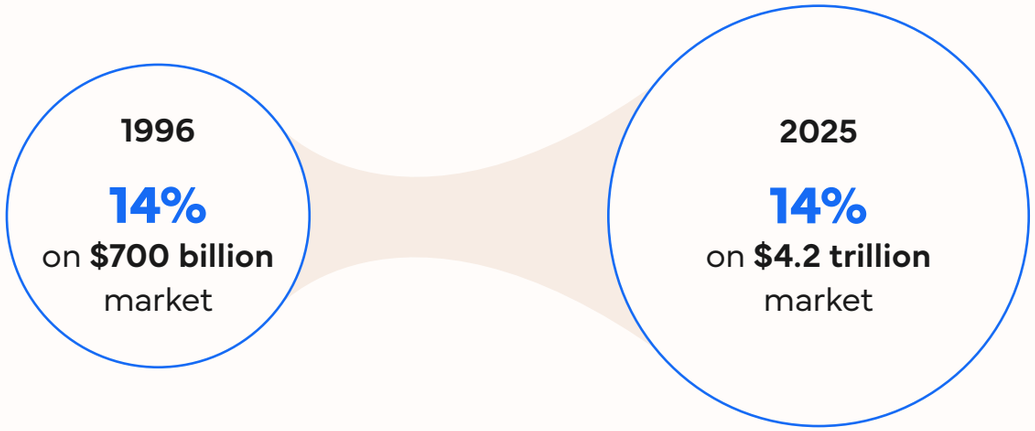


Figure 1

5x growth in **enterprise AI** investment



AI is the most significant IT infrastructure buildout in the history of IT, set to reach $1 trillion by 2029.

In 2026, many enterprises are seeing the impact of AI on their markets and business and are investing in their own AI use cases, as well as private AI infrastructure on which to run them.

Note: Data represents the total worldwide market for IT and enterprise AI spending.
Sources: IDC Worldwide Black Book, March 2026 Forecast; IDC Quarterly AI Infrastructure Tracker, 2026

AI-driven transformation in manufacturing

Three key drivers are shaping the transformation of the manufacturing industry:



Supply chain disruption

Geopolitical tensions and trade fragmentation are straining global manufacturing networks, forcing organizations to manage distributed sourcing with greater agility. Hardware supply constraints and export controls compound the pressure.



Asset-cycle tension

Manufacturing operates on asset life cycles measured in decades, while AI evolves in months. Disconnected legacy OT environments were never designed for AI-native architectures; bridging that gap remains the defining constraint on scaling industrial AI.



Industrial AI revolution

The industrial data revolution enables manufacturers to leverage OT and IT data for real-time quality, yield, and operational intelligence but only with governed, sovereign AI architectures.

AI adoption in the manufacturing industry is growing rapidly.

2025
Over
$106B
Total worldwide spending in the manufacturing industry.

2026
53%
YoY growth
Manufacturing is a powerhouse AI sector in Europe.

2025–2029
37%
CAGR
AI spending in Europe is on a rapid growth trajectory.

AI enables organizations to handle the paradigm shift efficiently to provide customers with secure, ubiquitous, real-time services.

While AI is transforming manufacturing, its adoption introduces new challenges around OT/IT governance, IP protection, and operational control. Addressing these challenges requires architectures with sovereignty, IP protection, and OT/IT control designed in, whether AI runs at the edge, on-premises, in private cloud, in a sovereign cloud region, or in public cloud.

Source: Worldwide AI and GenAI Spending Guide, September 2026

Sovereign AI and private AI: Rewriting how AI is built, governed, and scaled



Sovereign AI

A country or organization's **capacity to build and run AI on its own terms,** using its own infrastructure, data, models and talent, all anchored in national priorities, laws, and culture



Private AI

AI that runs in an environment **the organization controls** (on-premises and fully air-gapped, in private cloud, or in an accredited sovereign cloud region) alongside its data, with full governance, security, and ownership

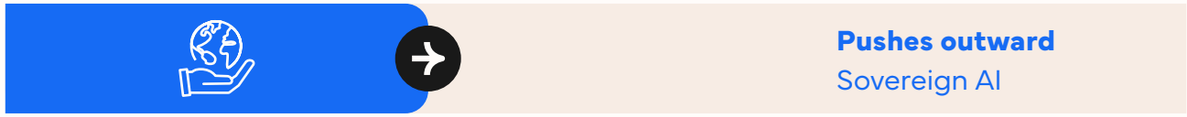


75%

of enterprise AI workloads will run on fit-for-purpose hybrid infrastructure by 2028.

Note: Worldwide market
Source: *IDC FutureScape: Worldwide Digital Infrastructure 2025 Predictions*

Sovereign AI and private AI: Where the complexity shows up



Pushes outward
Sovereign AI

Complexity spans regions, providers, and regulatory regimes.

Pulls inward
Private AI



Complexity stays inside and means securing environments, integrating systems, and keeping internal data flowing cleanly.

Running **AI in either** of these **environments** means **integrating** infrastructure, cloud, data, models, and governance across **hybrid environments:** on-premises, private cloud, sovereign hyperscaler cloud, public cloud, and edge, selected workload by workload, with classification level deciding which are permitted.

Navigating the complexity

The harder organizations push for control, the more interdependent their AI ecosystems become. It is not about owning every piece. Instead, it's about making a multi-provider system run reliably inside defined boundaries. Progress comes from ecosystems with tighter orchestration, clearer accountability, and stronger alignment across partners.

The automation gap must be bridged to scale AI successfully across private and public AI

Agile IT based on a modern digital platform

Inflexible IT based on a legacy architecture

1 **Digital Leaders**
Top 26%
Digitally transformed

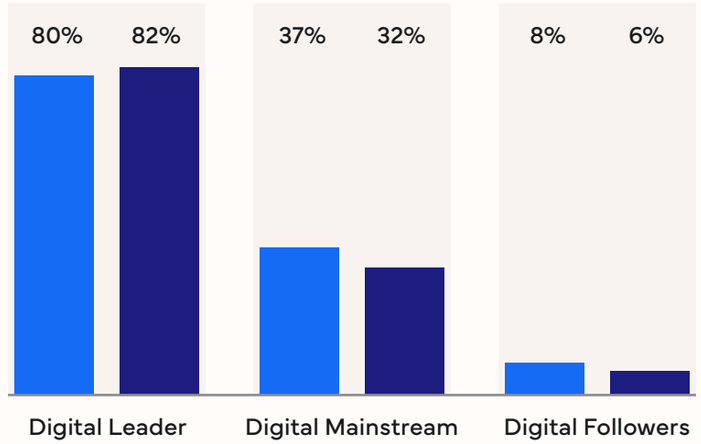
2 **Digital Mainstream**
Middle 49%
Digitally transforming

3 **Digital Followers**
Final 26%
Digitally resisting

Percentage of respondents:

Extensive adoption of automation and orchestration

Extensive use of AI for business use cases



Organizations that have successfully scaled AI use cases have typically extensively deployed:

- Automation and orchestration
- AIOps
- Cloud-native development practices
- Strong security and risk management
- Hybrid and multicloud adoption
- Integrated real-time data

Solutions designed to enable and integrate these capabilities will help accelerate and derisk AI use case deployments.

Digital Leaders invest broadly and deeply across their IT infrastructure, with strategic support and funding; this pays dividends with demonstrably higher business agility and revenue growth. Companies in the Digital Mainstream and Digital Follower segments that are striving to become Digital Leaders should engage with proven transformation partners to assess their current capabilities and plan a journey together to deliver this transformation.

The architecture gap

In manufacturing, organizations redesigning for private and sovereign AI today are creating a lasting advantage

A clear divide is opening between manufacturers that have redesigned their AI architecture by incorporating sovereignty, governance, and public and private AI foundations and those that are still running isolated pilots on infrastructure never built to scale. The impact of this gap extends beyond operational aspects: It also encompasses production performance, supply chain resilience, IP protection, and regulatory dimensions.

	Leaders	Followers
AI strategy	Enterprise-wide, targeting full operating model transformation	Select functions or no enterprise AI strategy
Data governance	Automated, full traceability and real-time controls; GDPR and NIS2 for OT and similarly aligned regulations	Fragmented, inconsistent, still being built
Infrastructure	Purpose-built; public and sovereign foundations in place, data residency assured where required	Reactive deployment, minimal scalability planning
Risk management	Dynamic, real-time risk management	Manual reviews, inconsistent human oversight
AI road map	Agentic workflows, cross-functional orchestration, predictive maintenance, supply chain orchestration, and quality control	Isolated pilots, short-term use case focus

Only **46%**
of manufacturers have reached repeatable, multi-site AI.

Only **22%**
manage the AI and analytics models running in operations through a comprehensive platform

Only **22%**
have dynamic, real-time risk management with strict sovereignty enforcement.

The cost of waiting

The compliance landscape and AI use case expectations are constantly evolving. Manufacturers running AI on ungoverned architectures face a growing challenge: Each new regulation or guideline increases the distance between the current state and where they need to be (e.g., in technology, operations, risk management, or institutional readiness).

Sources: IDC *Worldwide Manufacturing Survey,* Aug 2026 (n = 1065); IDC's *IT-OT Survey, Jul 2026 July* 2026 (n = 678); IDC *Future Enterprise Resiliency Survey, Wave 1,* 2026 — Manufacturing (n = 124)

AI is reshaping manufacturing, but fast adoption demands responsible AI governance to protect operational continuity, IP, and compliance across OT and IT environments

AI adoption: A market imperative in manufacturing

Manufacturing organizations must adopt AI to remain competitive and operationally resilient. AI transforms how manufacturers innovate and execute: accelerating process optimization on the shop floor, enabling predictive and autonomous maintenance across aging asset bases, and orchestrating supply chains that are increasingly fragmented by geopolitical disruption. From real-time quality control at the line level to dynamic demand sensing and supplier risk management across global networks, AI is reshaping every layer of industrial operations.

In a highly regulated sector, AI deployment must simultaneously drive innovation and comply with multiple mandatory requirements (e.g., the EU AI Act, NIS2 and IEC 62443 for OT, GDPR, and export controls). As with NIS2 and IEC 62443 for OT, the EU AI Act is paving the way for dedicated AI legislation elsewhere.

Responsible AI: Governance is the industrial imperative

Sound AI governance that ensures explainability, auditability, and human oversight is the foundation for safe AI at scale in manufacturing. Governance is central to the EU AI Act, NIS2 and IEC 62443 for OT environments, and emerging industrial AI frameworks worldwide.

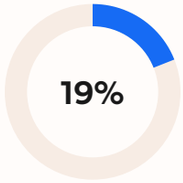
Manufacturers must de-risk AI and agentic AI adoption, ensuring operational resilience, security, and compliance while addressing the need for:

- Edge and hybrid computing to support real-time OT workloads without uncontrolled data egress
- Expert skills, with clear control of AI models trained on proprietary process and product data
- Redesigned operational processes with AI-in-the-loop governance and human oversight
- Regulatory-aligned architectures spanning the EU AI Act, NIS2 and IEC 62443 for OT, GDPR, and export control requirements

Ensuring compliance across diverse jurisdictions while maintaining OT continuity is essential for responsible, production-grade AI adoption.

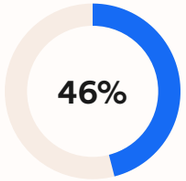
Sources: IDC's *AI MaturityScape Benchmark 2026*, April 2026, manufacturing (n = 345); IDC *Future Enterprise Resiliency Survey, Wave 1*, 2026 — Manufacturing; IDC's *Manufacturing Technology Buyer Outlook on AI and Agentic*, March 2026

AI is reshaping manufacturing, but fast adoption demands responsible AI governance to protect operational continuity, IP, and compliance across OT and IT environments



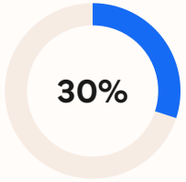
Operational efficiency

of manufacturers rank operational efficiency as a top-three AI objective.



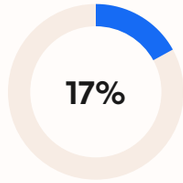
Lack of governance

identify a lack of AI governance expertise as a top barrier to scaling.



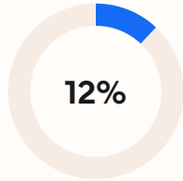
Generative AI

of manufacturing organizations are deploying agentic AI.



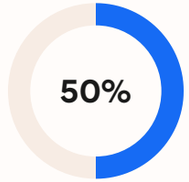
Quick adoption

of manufacturers already have AI agents in pilot or production.



Competitive positioning

of manufacturers prioritize deployment environments optimized for cost, security, and data sovereignty.



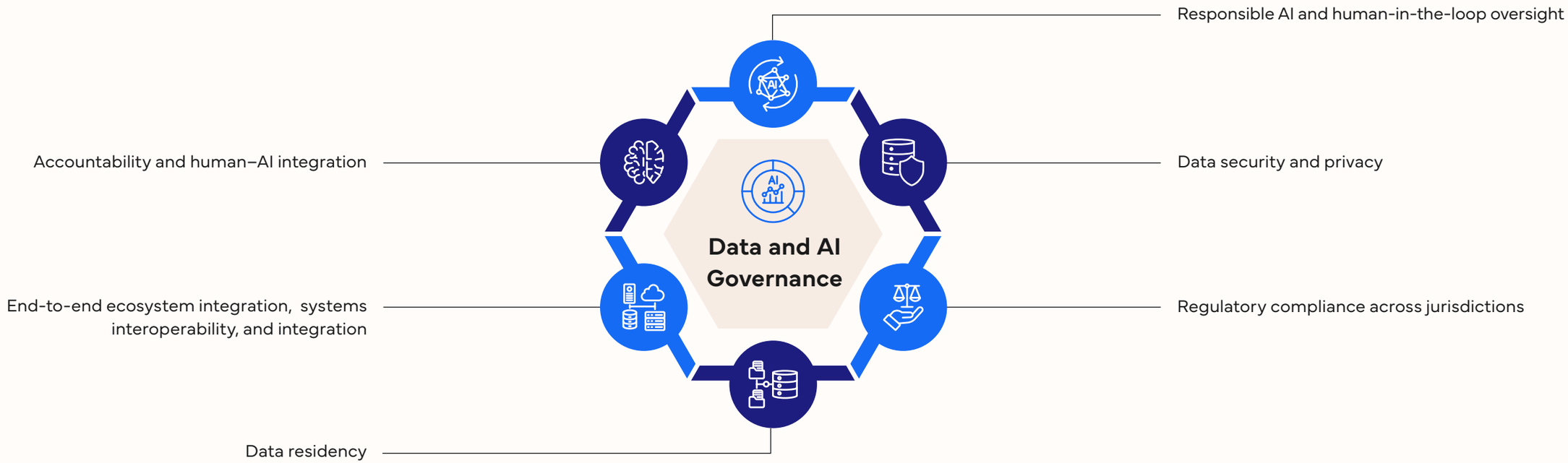
Reduction in routine tasks

of manufacturing IT leaders are accelerating AI infrastructure investment as the foundation for scaled, governed AI deployment.

Sources: IDC's *AI MaturityScape Benchmark 2026*, April 2026, manufacturing (n = 345); IDC *Future Enterprise Resiliency Survey, Wave 1*, 2026 — Manufacturing; IDC's *Manufacturing Technology Buyer Outlook on AI and Agentic*, March 2026

De-risking AI adoption in manufacturing with private and sovereign AI

Six AI governance dimensions



Sources: IDC *FutureScape: Worldwide Cloud 2026 Predictions* (IDC #US53859425, October 2025); IDC's *WW C-Suite Tech Survey,* September 2025, EMEA (n = 300)

Manufacturers must address three layers: OT and IT data, the AI model, and hybrid infrastructure

Where the complexity shows up

Sound AI governance that ensures explainability, auditability, and human-in-the-loop control is the foundation for safe AI at scale. Manufacturing organizations must de-risk AI adoption, addressing:

- **Infrastructure:** Managed edge and hybrid AI computing for OT workloads
- **AI model control:** Domain expertise to train on proprietary process data and ensure explainability
- **Operating model:** Redesigned plant and supply chain processes with governed, AI-in-the-loop workflows

Manufacturers must manage these requirements across every jurisdiction in which they produce or operate. Data residency requirements, IP protection mandates, and OT security obligations directly shape how the AI factory architecture is engineered across the edge, on-premises, and cloud layers.

AI model control as a priority

76% of these organizations say retaining full AI model controls is important or critical.

Sovereignty interest surge

44% of manufacturers say geopolitical tensions have increased interest in sovereign AI infrastructure.

Differentiated governance

58% apply differentiated AI governance standards depending on where AI runs.

Security concerns

49% say AI applied to R&D and intellectual property requires sovereign cloud infrastructure.

Compliance with regulations

46% of those increasing sovereign AI cloud use cite growing compliance requirements as a top driver.

Private cloud adoption for AI

49% expect to increase the use of sovereign cloud for AI workloads over the next two years.

Private and sovereign AI provide the technological foundation to meet regulatory requirements, protect IP, and deliver operational intelligence securely and at scale across production environments.

Sources: IDC *FutureScape: Worldwide Cloud 2026 Predictions* (IDC #US53859425, October 2025); IDC's *WW C-Suite Tech Survey,* September 2025, EMEA (n = 300)

Engineered AI factory approaches can help simplify, speed up, and secure enterprise AI solutions

AI factories are:

- Industrialized, scalable digital infrastructure platforms
- Purpose-built to automate and operationalize the development, deployment, and management of AI at enterprise or national scale across AI-related hardware, software, and services
- Vertically integrated platforms with specialized AI accelerators, fabrics, orchestration software, AI/ML frameworks, and cloud/hybrid infrastructure
- Able to deploy a combination of commercial or open AI models from large to small to support multi-modal solutions, including general-purpose LLMs, optimized SLMs, and diffusion models
- Able to streamline the transformation of enterprise data into actionable intelligence

Benefits which you can expect:



Accelerate time to value



Cut costs



Reduce risk

Expert partners with end-to-end engineered AI factory platforms that are right-sized for your private AI workload needs will be critical to meeting business value outcomes and overall objectives.

AI factories in action

Use case 1:

Shop-floor intelligence and predictive operations

Geopolitics drives scenario planning

57% of manufacturers cite geopolitical impacts as a top technology risk, driving near-real-time supply chain scenario planning.

Hardware and export constraints

48% flag hardware supply or export constraints as a top technology risk, driving demand for sovereign AI infrastructure.

Models trained on an organization's own products, tolerances, and failure histories, under its own controls, deliver precision that generic models cannot match. The value of these models compounds as more operational data flows in. Agentic maintenance workflows covering predictive diagnostics, scheduling, and parts ordering operate within defined authority boundaries, with human-in-the-loop governance and full audit trails, enabling confident scaling without surrendering operational control. Worker copilots for assembly, quality inspection, and diagnostics run at the edge with no uncontrolled data egress, keeping proprietary process intelligence under the manufacturer's control while delivering real-time response at the point of work.

- **Sovereign model deployment:** Process data, failure histories, and product tolerances stay under the enterprise's control, wherever the workload runs, protecting the IP that underpins competitive advantage and enabling continuous model improvement on live production data.
- **Regulatory compliance:** EU AI Act and NIS2 and IEC 62443 for OT requirements (auditability, explainability, and human oversight) are built in from deployment, not retrofitted. Compliance becomes a structural property of the AI factory, not a governance overhead.
- **Governed autonomy at scale:** Agentic workflows operate within defined authority boundaries with escalation protocols, ensuring human accountability at each consequential decision point: a governance model that makes it safe to expand from pilot plant to global network.

Early shop-floor AI deployments were overly constrained by security policy, and workers often find enterprise copilots inferior to consumer tools. A lack of AI governance expertise is the #1 governance barrier for 46% of manufacturers.

Sources: IDC *Future Enterprise Resiliency Survey, Wave 1,* 2026 — Manufacturing

AI factories in action

Use case 2:

Agentic supply chain resilience

Autonomous decisioning is a top-three priority

46% prioritise autonomous action as top agent capability.

Autonomous action leads agentic priorities

66% of manufacturers measure AI success via operational efficiency metrics.

Agentic workflows shift the operating model from reactive to proactive: Supply drift signals are flagged weeks earlier, with human planners retaining full decision-making authority in high-stakes scenarios. Sovereign deployment ensures that sensitive supplier contracts, demand forecasts, competitive pricing intelligence, and proprietary logistics data under the organization's control, transforming supply chain data into a sovereign competitive moat that compounds with every planning cycle.

- **Sovereign intelligence by design:** Proprietary models trained continuously on live supplier, demand, and inventory data improve scenario accuracy over time in ways generic planning tools cannot replicate; the longer the model runs inside the sovereign perimeter, the wider the competitive gap it creates.
- **Governed orchestration across the full supply chain life cycle:** AI agents orchestrate across ERP, WMS, demand sensing, and supplier portals within governed, auditable workflows, with human planners retaining decision-making authority in high-stakes scenarios.
- **Confidence to manage global complexity at scale:** The enterprise AI factory's sovereign perimeter gives manufacturers the governance foundation to extend AI orchestration beyond a single plant or region without exposing proprietary intelligence or surrendering regulatory control.

As autonomous production and supply chain decisioning become the operational norm, human–AI interactions must evolve, making responsible AI and private and sovereign AI models strategic key success factors in line with the EU AI Act mandate.

Sources: IDC *Future Enterprise Resiliency Survey, Wave 1,* 2026 — Manufacturing

AI factories in action: IP-driven product innovation

Use case 3:

IP-driven product innovation

New revenue streams

34% of manufacturers plan to use AI for new revenue streams In the next 12 months.

Data quality

59% cite data quality and lineage as their top data priority.

IP as a competitive asset

23% already monetize it through verified business outcomes.

What private AI infrastructure enables

- **Domain-specific LLMs** fine-tuned on proprietary materials, from CAD libraries and process recipes to quality specifications, built and updated inside a controlled environment
- **AI-accelerated new product introduction:** Recipe generation, design optimization, and failure mode prediction, all within the enterprise perimeter
- **Open-weight model foundations** that reduce vendor dependency risk (if a provider changes terms, the enterprise retains its trained weights and data; license terms vary, so permissive licenses such as Apache 2.0 carry the least residual dependency)

For manufacturers for whom differentiation lies in design and process data (e.g., those in automotive, specialty chemicals, aerospace, or food and beverages), there is no version of the AI opportunity that does not involve proprietary data. However, this is precisely the data that cannot be exposed to a third-party model without control over where it goes, who can train on it, and how long it is retained.

Sources: IDC *Future Enterprise Resiliency Survey, Wave 1,* 2026 — Manufacturing; IDC's *Manufacturing Technology Buyer Outlook on AI and Agentic,* March 2026; IDC's *AI MaturityScape Benchmark 2026,* April 2026, manufacturing (n = 345)

From pilot to production: Steps to full-stack sovereign AI in manufacturing

1 Assess and prioritize

Classify AI workloads against IP sensitivity, latency requirements, and regulatory jurisdiction. Identify high-risk AI systems under the EU AI Act, including AI safety functions in machinery falling under the Machinery Regulation from January 2027, and map OT security obligations under NIS2 and IEC 62443. Conduct feasibility and readiness assessments across the OT/IT infrastructure, data maturity, and governance layers. Define the private and sovereign AI strategy and prioritize use cases.

2 Design and architect

Define an AI factory strategy and a three-layer sovereign architecture spanning edge, on-premises, private cloud, sovereign hyperscaler cloud, and public cloud, with each workload placed by latency, IP sensitivity, and jurisdiction. Establish OT/IT data governance, an MLOps framework, and compliance controls. Engage an expert ecosystem partner with full-stack and cross-environment capability.

3 Deploy priority use cases

Launch priority use cases (shop-floor intelligence or supply chain resilience) within the AI factory. Ensure regulatory compliance by design, meeting the mandatory requirements arising from the EU AI Act, NIS2, and any other requirements applicable in the jurisdiction. Measure operational outcomes.

4 Scale and compound

Expand to predictive quality, autonomous logistics, and engineering AI. Reinvest ROI in deeper capabilities, since proprietary model intelligence, trained on unique process, product, and failure data, compounds to build competitive advantages that peers cannot replicate.

Choose the right expert partner that can support your journey toward private and sovereign AI and offers technical and business expertise to address all concerns, with a long-term collaboration perspective. To select the right partner, look at capabilities in relation to:



Full-stack coverage
From factory floor edge to enterprise cloud

OT/IT regulatory knowledge
EU AI Act, NIS2 and IEC 62443 for OT, GDPR, and local sovereignty requirements

Edge-native and multicloud deployment
OT-compatible architectures with no vendor or cloud lock-in

OT and operational security
Cybersecurity and physical safety across shop floor and IT environments

Local expertise and global reach
With proven delivery track records

AI model governance
Transparency by design

TCO and ROI
Frameworks for optimized deployment cost

Expert partners help accelerate sovereign AI time to value, reduce risk, and boost ROI

Consulting, integration, and operations services for private and sovereign AI

- Workload assessment and placement across on-premises, private, sovereign, and public cloud
- Vendor-agnostic, turnkey, prevalidated infrastructure deployment
- Integration and operations across hyperscaler, private AI, edge, and legacy estates
- AI strategy and roadmap
- Feasibility and readiness assessments
- Data governance and strategy
- Use case prioritization
- Data pipeline engineering
- MLOps and model management
- Dealing with skills shortages

Enterprise benefits

- Accelerated time to deploy with validated blueprints, reference architectures, repeatable methodologies, and technical expertise
- Resource optimization and utilization for greater TCO/ROI across private, public, and on-premises locations (FinOps best practices)
- Reduced operational risk through improved configuration, expert resources, and knowledge transfer sessions
- Improved security and compliance through secure firewalls and deep understanding of regulated industries

Partners can help pinpoint the areas of greatest business impact in your organization and develop roadmaps for responsible, enterprise-wide AI transformation, addressing every dimension of privacy and sovereignty.

About the IDC analyst



Lorenzo Veronesi

Associate Research Director, IDC Manufacturing Insights

Lorenzo Veronesi is an associate research director for IDC Manufacturing Insights EMEA. In this role, Veronesi leads the Worldwide Smart Manufacturing research program and supports all the IDC MI research services for EMEA, by looking at Digital Transformation drivers in multiple manufacturing industry sub-verticals. He is also often involved in consulting projects across the world for end-users, IT vendors and public authorities. During the last decade his research has focused across key processes such as manufacturing operations management, supply chain management, and product lifecycle management in multiple manufacturing verticals, including - among others - automotive, aerospace, machinery, high-tech, chemicals, CPG, and fashion. Before joining IDC, Veronesi worked as analyst in multiple projects including research in the industrial logistics sector and as advisor for public authorities in Italy. Veronesi holds an MSc Degree in Regional Science at the London School of Economics and Political Science and has graduated cum laude at the Bocconi University in Milan.

More about Lorenzo Veronesi →

Message from the sponsor



Manufacturers are reaching an inflection point as AI adoption expands across core operations, engineering, and supply chain ecosystems. As this report highlights, organizations must balance innovation with control, specifically as regulatory complexity, IP protection, and geopolitical considerations increasingly shape technology decisions.

Private and sovereign AI approaches are emerging as a pragmatic pathway to scale AI responsibly, enabling greater governance, data sovereignty, and alignment with enterprise-specific environments spanning edge and cloud.

Realizing value from AI will require more than infrastructure choices. It demands integrated data foundations, domain-specific intelligence, and operating models that connect strategy to execution. Organizations that adopt a structured, outcome-driven approach, supported by partners with deep industry and full-stack capabilities, will be better positioned to unlock measurable impact while maintaining trust, security, and compliance.

Learn more about enabling scalable, governed AI in manufacturing.

IDC Custom Solutions

IDC Custom Solutions produced this publication.
The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies.

This IDC material is licensed for external use and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

IDC.com | IDC on LinkedIn | IDC Blog

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

©2026 IDC. Reproduction is forbidden unless authorized. All rights reserved. CCPA