unosecur

WHITEPAPER

Identity Security in Manufacturing

Why modern manufacturing environments are becoming identity-driven ecosystems, and why every unmanaged trust relationship is an open door for attackers.

Table of contents

Section 1: Executive summary

Manufacturing has become the most attacked industry on the planet. For the third consecutive year, it accounts for more cyberattacks than any other sector, representing 27.7 percent of all incidents globally in 2025. Ransomware attacks against manufacturing environments increased by 56 percent in the same period.

The reasons are structural. Industry 4.0 has connected factory floors, supplier ecosystems, cloud environments, and operational technology into a single interdependent system. Every connection introduced a new trust relationship. Every trust relationship introduced a new identity. And identities, in manufacturing, remain the least governed part of the security environment.

The attacks that have caused the most damage in this sector share a common thread. They did not begin with a zero-day exploit or a sophisticated piece of malware. They began with a credential. A vendor account with excess access. An API key embedded in a web asset. A helpdesk agent was convinced to reset MFA. A service account that no one had reviewed in two years. Identity was the entry point, the escalation path, and in many cases, the reason the damage was as large as it was.

This paper is written for security leaders in manufacturing environments: organizations running complex OT and IT infrastructure, managing extended supplier ecosystems, and now deploying AI-driven systems on the factory floor. It maps the identity threat landscape specific to manufacturing, examines the incidents that define it, and makes the case for a unified identity-first defense.

Section 2: The manufacturing identity landscape

Modern manufacturing environments are not a single type of organization. A diversified heavy manufacturer like Godrej & Boyce runs dozens of business verticals, each with its own systems, vendors, and access patterns. An industrial automation company like ABB builds and operates the control infrastructure that other manufacturers depend on, making its identity perimeter both deep and externally facing. A process manufacturer like Wonder Cement runs continuous production environments, where a system going offline has immediate, measurable consequences.

What these environments share is a common identity challenge across three distinct categories.

Human identities

Employees, contractors, shift workers, and vendor technicians who directly access systems. In manufacturing, this category carries risks that are rarely present in purely digital industries. Engineering workstations are frequently shared across shifts with no individual account controls. Vendor and contractor access is often seasonal or project-based, provisioned quickly and deprovisioned slowly, if at all.

Remote access for maintenance and support is typically granted through jump servers or VPNs with minimal entitlement controls and no session recording.

Non-human identities (NHIs)

APIs, service accounts, tokens, certificates, PLCs, SCADA systems, and the machine-to-machine communication that holds factory operations together. The ratio of non-human to human identities in a large manufacturing environment is extreme. Most of these identities were created without lifecycle governance in mind. Credentials are rarely rotated. Permissions are rarely scoped. Many were provisioned for a specific integration or deployment and never reviewed again.

As Tata Motors' 2023 exposure demonstrated, a single embedded API key in a client-facing web asset can expose decades of operational data.

AI agents

The newest and fastest-growing identity class in manufacturing. Predictive maintenance systems, autonomous quality inspection agents, production scheduling tools, and supply chain optimization platforms are increasingly operating with real credentials, real API access, and real permissions across production systems.

Unlike a service account that executes a fixed task, an AI agent autonomously makes decisions, chains actions, and interfaces with multiple systems. In most current deployments, it holds broad permissions because restricting it would slow the operational efficiency that the business is investing in. The governance frameworks to manage these identities at scale do not yet exist in most manufacturing environments.

Modern manufacturing environments are becoming identity-driven ecosystems in which every vendor, machine, API, engineer, and AI system establishes a new trust relationship. Attackers increasingly exploit those trust relationships rather than breach traditional perimeters.

Human Identities Employees, vendors, contractors	Non-human Identities API's, tokens, PLCs, SCADA	AI Agents Autonomous, decision-making
Shift workers and engineers	PLC and SCADA accounts	Predictive maintenance agents
Seasonal Contractors	Embedded API Keys	Quality Inspection agents
Vendor Technicians	MSE service accounts	Supply chain optimisation
Remote Maintenance Staff	Machine to machine tokens	Production scheduling agents
Shared accounts, poor offboarding	Unrotated, untracked, overprivileged	No governance framework exists yet

Section 3: How identity is being attacked

The following incidents span geographies and manufacturing sub-sectors, but the identity patterns they represent are consistent. In each case, the breach did not require a sophisticated technical exploit. It required access that should not have existed, or access that was valid but should have been detected as anomalous.

1. **2025 | Tata Motors**
   Pattern: NHI and secrets sprawl. Embedded API keys expose 70TB of fleet and operational data

   Public-facing web assets across multiple Tata Motors products contained embedded AWS access keys and third-party API tokens in client-side JavaScript code. Two exposed key pairs provided access to hundreds of S3 buckets containing fleet telemetry, customer data, and internal operational records spanning decades. A Tableau integration issued privileged tokens using only a username and site name, with no password verification required. The breach required no malware, no network intrusion, and no sophisticated attack. Unmanaged non-human identities, left without rotation, scoping, or monitoring, were sufficient. Unosecur's published analysis of this incident is available at unosecur.com.

2. **2025 | Clorox**
   Pattern: Human credential and third-party trust Helpdesk social engineering cascades into supply chain shutdown

   Attackers reportedly convinced a third-party IT helpdesk provider to reset credentials and MFA protections through social engineering, bypassing identity

verification controls. That single failure cascaded into operational shutdowns, forced manual order processing across the supply chain, product shortages on retail shelves, and losses exceeding $350 million. No sophisticated malware was required at the point of entry. The attack began and was sustained entirely through compromised human identity controls, specifically the failure to verify the identity of someone requesting privileged credential change

3. **2026 | Foxconn**
   Pattern: Ransomware via identity and lateral movement. Ransomware disrupts North American manufacturing operations

   A ransomware group claimed responsibility for an attack on Foxconn's North American manufacturing facilities, with Foxconn confirming operational impact. The attackers' alleged theft of engineering and supply chain data, though the full scope of exfiltration was not independently confirmed. The incident is consistent with ransomware group TTPs that rely on credential abuse and lateral movement through supplier and contractor access pathways. It illustrates how attacks targeting manufacturing ecosystems increasingly combine operational disruption with data exposure to maximize leverage.

4. **2025 | Jaguar Land Rover**
   Pattern: Full kill chain via identity abuse. Identity abuse across the kill chain shuts global production for 40 days

   Though automotive in origin, the JLR incident is the defining modern case study for identity-driven operational disruption in manufacturing. Attackers moved through the environment using valid credentials at every stage of the kill chain: initial access via phishing, persistence through overpermissive IAM roles, lateral movement across IT and OT environments using legitimate remote services, and eventual ransomware deployment that halted global production for nearly forty days. The blast radius extended to thousands of suppliers, several of whom were forced to file for bankruptcy. Unosecur has published a full MITRE ATT&CK analysis of this incident at unosecur.com.

Four identity attack patterns

Across these incidents and the broader manufacturing threat landscape, four patterns recur:

- **Vendor and contractor credential abuse:** third-party access provisioned without least-privilege enforcement, used as the initial entry point or lateral movement pathway

- **NHI and secrets sprawl:** unmanaged API keys, service tokens, and embedded credentials left exposed in web assets, repositories, or firmware without rotation or monitoring
- **Human credential compromise:** phishing, social engineering of helpdesk or identity providers, or dark web purchase of valid employee accounts
- **OT identity gap exploitation:** factory floor systems with shared accounts, no MFA, and no audit logging, accessed via legitimate remote pathways once IT network access is established

In every case, the infrastructure was not broken. A trust relationship was abused.

Section 4: The OT/IT convergence identity gap

This section has no equivalent in cybersecurity discussions of most other industries, because most industries do not operate the way manufacturing does. Operational technology in manufacturing, the PLCs, SCADA systems, DCS platforms, and manufacturing execution systems that run factory floors, was designed for one purpose: availability. These systems were built to run continuously, in isolated networks, with no expectation of external connectivity or individual user accountability.

Industry 4.0 changed the operating conditions without changing the underlying architecture. Remote monitoring, cloud-connected analytics, supplier integrations, and AI-driven production systems now depend on OT environments being reachable from IT networks and cloud infrastructure. The identity perimeter has expanded dramatically. The identity controls within OT have not.

What OT identity looks like in practice

- **Shared accounts on engineering workstations:** a single username and password used across an entire shift, making individual attribution after an incident impossible
- **Service accounts on PLCs and SCADA systems** provisioned years ago, never reviewed, never rotated, and in many cases holding administrative permissions because scoping them down would require downtime
- **Remote vendor access via VPN or jump server** with no session recording, no time-limited credentials, and no mechanism to enforce least privilege once access is granted
- **No MFA on OT systems**, because the systems predate MFA, and retrofitting it requires engineering work that competes with production priorities

- **Audit logs in formats that modern SIEM tools cannot parse**, meaning OT activity is effectively invisible to the security operations team

The consequence is that once an attacker establishes a foothold in the IT environment, whether through a phished employee credential, a vendor account, or an exposed API key, the path into OT is often a matter of following existing, legitimate access pathways. There are no additional identity controls to cross. The lateral movement appears to be a normal operation.

OT systems were designed for availability, not accountability. Industry 4.0 connected them to everything. The identity governance layer was never added.

For organizations like Godrej & Boyce, which operate across multiple manufacturing verticals with varying levels of OT maturity, or ABB India, which both operates its own OT environments and supplies the OT infrastructure that other manufacturers depend on, this gap is not theoretical. It is the live attack surface that adversaries understand and actively probe.

Section 5: AI agents - The third identity frontier

Human identities and non-human identities have been the focus of manufacturing security discussions for years. AI agents are changing the equation in ways that existing governance frameworks were not designed to handle, and they are doing so faster than most security teams have anticipated.

An AI agent in a manufacturing environment is not a chatbot or a dashboard. It is an autonomous system that observes operational data, makes decisions, and executes actions across multiple systems. A predictive maintenance agent monitors sensor telemetry across production equipment, identifies anomalies, and triggers work orders or maintenance schedules. A supply chain optimization agent holds access to procurement systems, inventory data, and supplier APIs, and adjusts orders based on production forecasts. A quality inspection agent analyses output data, flags defects, and can halt production lines when thresholds are breached.

Each of these agents requires an identity with credentials, API access, and permissions across multiple systems. Each operates autonomously, without a human reviewing every action. And in most current deployments, each holds broader permissions than it strictly needs, because scoping them precisely requires effort the business is not prioritizing while the technology is still being deployed.

Three manufacturing-specific risk scenarios

1. **Predictive maintenance agent compromised:** an agent monitoring production equipment sensor data is manipulated through prompt injection or credential theft. The attacker uses the agent's existing access to suppress genuine anomaly alerts while equipment degrades, or to trigger false alerts that halt production. Damage occurs operationally before it is ever detected as a security event.

2. **Supply chain AI agent access abused:** an agent with procurement and inventory access has its credentials harvested. The attacker gains visibility into supplier relationships, contract terms, and inventory positions, or the ability to manipulate orders, reroute shipments, or introduce fraudulent supplier records. The agent's trusted identity is the mechanism.

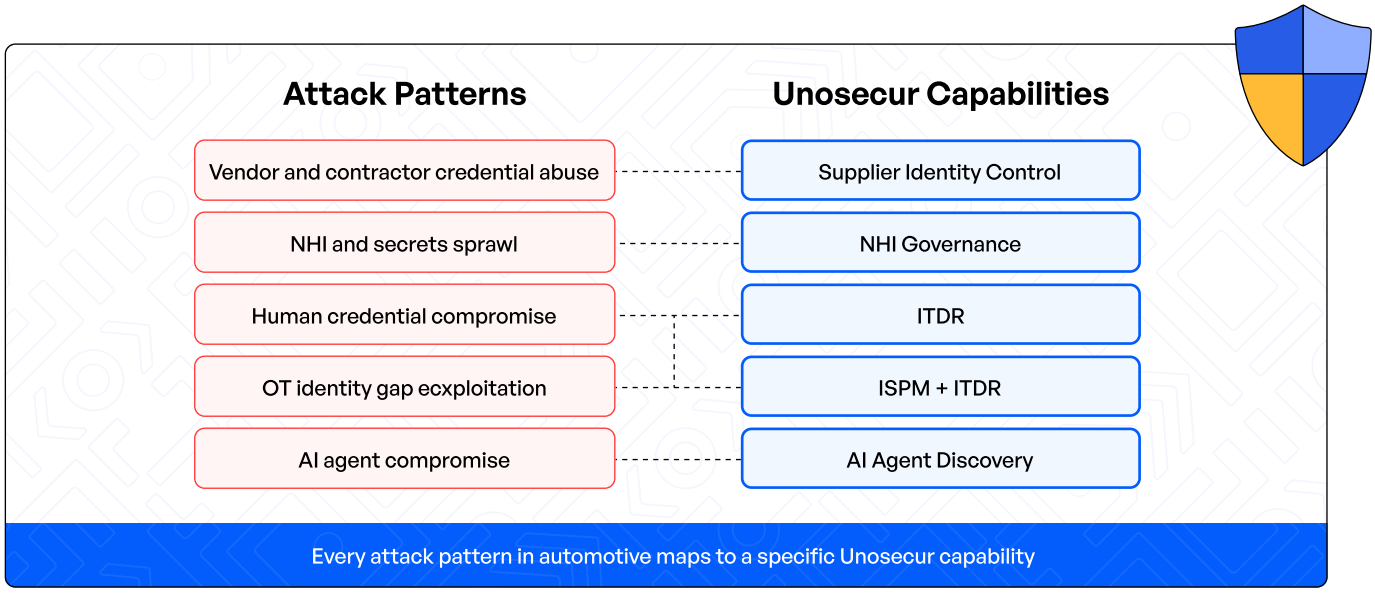
3. **Production scheduling agent manipulated:** an agent responsible for coordinating production output across factory lines is compromised and used to alter scheduling parameters. Output targets, shift allocations, and equipment utilization are all within scope. The impact is measurable in production losses before the breach is identified.

Why AI agents amplify every existing identity risk

- **Confused deputy:** the agent holds legitimate permission to access a system; an attacker tricks it into exercising that permission on their behalf, with no direct login required.
- **Overpermissioned by default:** agents are granted broad access because restricting them requires effort that competes with deployment timelines.
- **Orphaned credentials:** agents provisioned for a pilot or a specific task often retain active credentials long after the original use case has changed.
- **Audit gap:** When an agent acts autonomously across multiple systems, attribution after an incident becomes genuinely difficult.
- **Cross-agent propagation:** In multi-agent architectures, one compromised agent can pass credentials or manipulate downstream agents, spreading the blast radius without any additional attacker action.

AI agents are not just another identity type. They are autonomous, overprivileged, and self-operating identities whose blast radius is defined by their permissions, not their code.

Section 6: What an identity-first defense looks like



An effective response to the automotive identity threat landscape requires visibility and control across all three identity types: human, non-human, and AI agents. It requires that coverage to extend across cloud, SaaS, and on-premise environments simultaneously. And it requires the capability to detect anomalous identity behavior in real time, not after the fact.

Unosecur's Unified Identity Fabric is built to provide exactly that. The platform manages and governs human identities, NHIs, and AI agents within a single framework, designed for the complexity of enterprise environments.

ITDR (Identity Threat Detection and Response)

Monitors identity behavior across OT, IT, and cloud environments in real time. Flags credential use outside normal patterns, lateral movement using valid accounts, and privilege use inconsistent with the role. Addresses the kill-chain movement seen in the JLR incident and the lateral pathways from IT into OT that define the convergence risk.

ISPM (Identity Security Posture Management)

Continuously surfaces overpermissive roles, misconfigured access policies, shared accounts, stale vendor access, and entitlement drift before they become exploitable. Directly addresses the OT/IT convergence gap: shared engineering workstation accounts, unscoped vendor VPN access, and unreviewed service account permissions all surface here.

AI Agent Discovery

Discovers and inventories AI agents operating within the environment, assesses permissions against what each agent's function requires, and enforces least-privilege policies across multi-agent architectures. Tracks MCP server connections and third-party tool integrations that agents rely on. Addresses the governance gap that current AI deployment in manufacturing is creating, before it becomes the next generation's breach pattern.

NHI Governance

Lifecycle management for non-human identities, including API keys, service account tokens, PLC credentials, and embedded secrets. Tracks rotation status, flags unmanaged or long-lived credentials, and enforces scoping policies. Had this capability been in place at Tata Motors, the embedded AWS keys in client-facing assets would have been detected before they were exposed externally.

Supplier Identity Control

Extends identity governance to third-party and contractor access. Provides visibility into external identities operating within the manufacturing environment, enforces time-limited, least-privileged access for vendor sessions, and detects anomalous third-party credential behavior. Addresses the vendor and contractor credential abuse pattern, which is the dominant initial access vector across manufacturing incidents in Section 03.

Mapped against the four attack patterns in Section 03: NHI Governance addresses secrets sprawl. ITDR and ISPM together address credential compromise and lateral movement. Supplier Identity Control addresses third-party entry points. AI Agent Discovery addresses the risk of autonomous identity. ISPM and ITDR together address the OT identity gap by surfacing shared accounts and detecting anomalous behavior in environments that have never had this level of visibility.

Section 7: Conclusion

Manufacturing's digital transformation has made it the most targeted sector in cybersecurity. The attacks that define this era, Tata Motors, Clorox, Foxconn, and JLR, are not the result of inadequate perimeter defenses. They are the result of identity environments that expanded faster than the governance frameworks designed to manage them.

The OT/IT convergence gap is real and live. Factory floor systems that were never designed for identity controls are now reachable from cloud environments and supplier networks. Vendor and contractor access is provisioned faster than it is reviewed. Non-human identities accumulate without rotation or monitoring. And AI agents are now operating with autonomous permissions in production environments that have no governance model for what they can access or how their actions are attributed.

The organizations that will be hit by the next wave of manufacturing cyberattacks will not be those with the most endpoints protected or the most firewall rules. They will be those who have treated identity as the primary control surface, consistently governed all three identity types, and built detection capabilities to act before lateral movement completes.

Three things every automotive CISO should do now:

- **Audit OT identity controls before the next Industry 4.0 integration.** Every new connectivity project expands the identity perimeter into an environment that was not built to support it. Understand what accounts, credentials, and access pathways exist in your OT environment before the next integration adds to them.
- **Enforce individual accountability on shared access.** Shared engineering workstation accounts and unscoped vendor VPN access are not acceptable risk positions in a connected manufacturing environment. The inability to attribute actions after an incident is itself a governance failure.
- **Establish AI agent identity governance before deployment scales further.** The window between deploying AI agents and governing them properly is short. The manufacturing sector is at the beginning of that window. Closing it proactively is significantly less costly than closing it after an incident.

Manufacturing has always understood that operational resilience is not built in a single investment. It is built through consistent discipline across systems, processes, and people over time. Identity security is no different. The organizations that survive the next wave of attacks intact will not necessarily be the ones with the largest security budgets. They will be the ones who treated every vendor credential, every service account, every embedded API key, and every AI agent as a trust relationship worth governing. That discipline, applied consistently across all three identity types, is what converts a fragmented and exploitable attack surface into a defensible one. The threat environment in manufacturing is not slowing down. The window to build that posture before the next incident is open now.