



Tracknosis Manufacturing Edition

White Paper

Forensic Observability, Threat Detection and Regulatory
Compliance for the Manufacturing and Industrial Sector

**Making the
Unknown
Known**



Executive Summary

Manufacturers run the production lines, smart factories, and supply chains that the modern economy depends on — from automotive and aerospace to electronics, pharmaceuticals, food, and heavy industry. They are increasingly targeted by ransomware operators, nation-state actors, and competitors seeking intellectual property, where a successful cyber attack can halt production, damage equipment, compromise product quality, and disrupt just-in-time supply chains. At the same time, regulations and frameworks including NIS2, CIRCA, GDPR, IEC 62443, and customer and sector requirements such as TISAX and CMMC now require manufacturers to detect, investigate, and report significant incidents within hours — supported by defensible forensic evidence.

Tracknosis is a Forensic Observability platform built for Windows environments — including the engineering workstations, HMIs, historians, MES, and SCADA servers that sit at the IT/OT boundary on the factory floor. It continuously transforms endpoint and server telemetry into trusted forensic evidence, enabling manufacturers to detect threats early, perform rapid root cause analysis, and produce regulatory-ready incident reports — without relying on scarce and costly external forensic specialists.

The Manufacturing and Industrial Cybersecurity Challenge

Manufacturers run converged IT and operational technology (OT) estates: enterprise systems alongside production lines, industrial control systems, robotics, and manufacturing execution systems (MES) — often blending modern Industry 4.0 platforms with decades-old machinery. Conventional monitoring tools generate alerts, but rarely answer the question investigators and plant engineers need most: what actually happened, and did it cross from IT into the systems that keep production running?



Ransomware – Encryption of production and MES systems halts the line, idling plants and disrupting supply.



IP & Design Theft – Nation-state actors and competitors target product designs, formulas, and process know-how.



IT/OT Convergence – Attackers pivot from corporate IT into OT via engineering workstations, HMIs, and historians.



Production Tampering – Manipulation of control systems can damage equipment or compromise product quality and safety.



Supply Chain Risk – Compromise of vendors, integrators, and remote-access tooling grants a route into plant networks.



Compliance Gap – Without forensic evidence, meeting NIS2, CIRCIA, TISAX, and CMMC windows is very difficult.

Forensic Observability

Tracknosis introduces Forensic Observability – the discipline of continuously transforming telemetry into trusted forensic evidence. Rather than collecting logs and waiting for alerts, Tracknosis analyses what actually changed on disk, attributing every change to a specific user, process, and timestamp.

How It Works

Tracknosis performs sequential forensic scans of Windows NTFS disk structures across IT and OT Windows assets – from corporate endpoints to engineering workstations, MES, and historians on the plant floor. Each scan captures a complete forensic snapshot. The difference between consecutive scans – the delta – reveals precisely what changed, when, and by whom. This approach detects threats that leave no signature but always leave a forensic trace – including the stealthy tradecraft used to manipulate control-system hosts.

Windows Security Event Logs	Authentication, object access, privilege use, and audit log clearing events
NTFS Master File Table (MFT)	Metadata for every file and directory – timestamps, attributes, allocation status
\$UsnJrnl Change Journal	Complete record of file creates, modifications, deletions, and renames
\$LogFile Transactions	Low-level file system operations independent of Windows auditing
Registry Hive Analysis	Persistence artifacts, configuration changes, and attacker backdoors between scans

Root Cause Analysis and Threat Detection

Root Cause Analysis

- ▶ Identify patient zero — the first compromised endpoint or account
- ▶ Reconstruct the full attack chain from IT entry to OT impact
- ▶ Attribute every forensic change to a specific user and session
- ▶ Quantify which control-system hosts or design data were affected
- ▶ Produce an evidence timeline for regulators, customers, and counsel

Threat Detection

- ▶ Ransomware: mass file modification, extension changes, shadow copy deletion
- ▶ OT pivot: unexpected changes on engineering workstations, HMIs, and historians
- ▶ IP theft: bulk access or copying of design and process files between scans
- ▶ Timestomping: SI/FN attribute divergence indicating attacker log evasion
- ▶ Zero-day: behavioral detection without any signature or IoC required

Risk Scoring

Every detected behavioral pattern receives an explainable risk score — fully traceable to the underlying forensic artifacts — so manufacturing security and OT teams can prioritise response effectively. Scores range from Low (routine changes) through Medium (anomalies warranting review) to High and Critical (ransomware staging, active encryption, confirmed control-system tampering).



Regulatory Compliance: NIS2, CIRCIA, IEC 62443, TISAX and CMMC

Manufacturers face mandatory cyber incident reporting obligations and customer security requirements that demand forensic evidence, structured timelines, and audit-ready reports – often within 72 hours. Tracknosis generates this evidence automatically from its continuously maintained forensic repository.

Regulation / Framework	Scope in Retail	Key Obligation	Tracknosis Support
NIS2 (EU)	Manufacturers of critical products and important entities in EU member states	Early warning within 24 hrs; full notification within 72 hrs; senior accountability	Forensic timeline, evidence preservation, and structured regulatory report within hours
CIRCIA (US)	US critical manufacturing sector entities	Report significant incidents to CISA within 72 hrs; ransomware payments within 24 hrs	Tamper-evident artifact preservation, incident documentation, and response records
IEC 62443	Industrial automation and control systems across manufacturing environments	Secure control systems; manage change; maintain auditable security controls	Forensic evidence of changes to control-system Windows hosts and audit-ready records
TISAX (Automotive)	Automotive suppliers and partners handling sensitive OEM information	Demonstrate information security maturity; protect prototype and design data	Continuous forensic monitoring and evidence of controls protecting sensitive data
CMMC / NIST 800-171 (US Defense)	Defense industrial base manufacturers handling controlled unclassified information (CUI)	Protect CUI; implement and evidence required security controls; report incidents	Forensic audit trail of access to CUI and control evidence aligned to NIST 800-171

Manufacturing and Industrial Use Cases



Ransomware Response

Detect encryption activity through delta analysis; generate forensic evidence package and regulatory report rapidly



Production Line Protection

Detect tampering and persistence on MES and control-system hosts before output is impacted



Insider & Contractor Risk

Attribute file and configuration changes to specific operator, engineer, or contractor accounts



Quality & Safety Integrity

Detect unauthorised changes to recipes, parameters, and control logic that affect product quality



IT-to-OT Intrusion

Detect attacker pivots onto engineering workstations, HMIs, and historians; reconstruct the crossover timeline



IP & Design Theft

Detect bulk access or exfiltration of product designs, formulas, and process know-how



Supply Chain Compromise

Detect tampering introduced via vendors, integrators, and remote-access tooling



Post-Incident Analysis

Reconstruct the complete attack chain; quantify impact for regulators, customers, and insurers

Value to CIOs, CISOs, and OT / Plant Leaders

For manufacturers balancing throughput, quality, and resilience, Tracknosis delivers measurable operational assurance. It provides early warning of threats and anomalies, accelerates forensic investigation, supports regulatory and customer reporting, and helps protect the IT/OT boundary — all without replacing existing security investments or disrupting production.

Measurable Outcomes:

- ▶ Reduced mean time to detect (MTTD) and mean time to resolve (MTTR) cyber incidents.
- ▶ Rapid root cause identification — reducing reliance on costly external forensic specialists.
- ▶ Improved uptime and reliability across POS, e-commerce, and supply-chain systems.
- ▶ Regulatory reporting compliance — forensic evidence packages ready within hours, not days.
- ▶ Evidence-based forensic reporting for boards, audit committees, and card acquirers.
- ▶ Enhanced collaboration between IT security, loss prevention, compliance, and operations.
- ▶ Strengthened customer trust and protection of the retail brand and reputation.
- ▶ Reduced cost and duration of cyber incident investigations and regulatory responses.

Benefits for Customers and the Supply Chain

Forensic Observability does not only protect the manufacturer — it protects the customers, OEMs, and partners who depend on reliable supply and trustworthy products. When a manufacturer can detect, investigate, and contain incidents in hours rather than weeks, the wider supply chain benefits from continuity, product integrity, and protected intellectual property.

Direct Benefits to Customers and Partners

Supply Continuity	Faster detection and containment keep production and deliveries on schedule, protecting just-in-time supply
Product Integrity	Detecting tampering with recipes and parameters helps ensure product quality and safety for end users
IP Protection	Safeguarding shared designs and prototype data protects customers' and partners' intellectual property
Supply Chain Trust	Demonstrable forensic readiness reassures OEMs and customers their supplier manages cyber risk
Faster Notification	Precise identification of affected data and systems enables prompt, accurate notification to partners
Audit & Assurance	Tamper-evident evidence supports TISAX, CMMC, and customer security audits across the supply chain

Wider Impact

- ▶ Fewer and shorter production disruptions affecting downstream customers.
- ▶ Stronger protection of shared designs, formulas, and process know-how.
- ▶ Greater assurance of consistent product quality and safety.
- ▶ Transparent, evidence-based communication with OEMs and partners after an incident.
- ▶ Stronger, more resilient

Deployment and Governance

Tracknosis deploys rapidly across Windows workstations, servers, engineering hosts, and Citrix environments with no system reboot required. It integrates with existing IT management tooling, requires no dedicated database infrastructure, and supports on-premises, segmented, and air-gapped deployments suited to plant-floor and OT-aligned networks.

Supported Platforms	Windows 11; Windows Server 2016–2025; engineering/HMI/MES hosts; Citrix Virtual Apps and Desktops
Deployment Methods	SCCM, Intune, Group Policy, MSI, PowerShell — pilot in minutes, estate-wide in hours
Encryption at Rest	Blowfish 448-bit (forensic repository) and AES-256
Encryption in Transit	TLS 1.3 across all communication channels
Evidence Integrity	Cryptographic hashing of every artifact at acquisition; read-only forensic collection
OT-Aware Deployment	Low-footprint collection suited to segmented OT networks; on-premises and air-gapped support
SIEM Integration	Splunk, Elastic, Datadog, Cisco XDR, Microsoft Sentinel — extends existing investments
Access Control	Granular RBAC and immutable audit logs; data sovereignty and retention controls

Why Tracknosis for Manufacturing

Manufacturers cannot afford prolonged investigations, regulatory penalties, lost intellectual property, or the disruption and reputational damage of a poorly managed cyber incident. Tracknosis provides the forensic intelligence layer that transforms existing security investments into a platform capable of answering the questions that matter most – and meeting the obligations that regulators and customers demand.

Forensic Observability

- ▶ Continuous disk-level evidence
- ▶ Delta analysis across IT and OT hosts
- ▶ AI-assisted investigation
- ▶ Evidence independent of log tampering

Regulatory Compliance

- ▶ NIS2 · CIRCIA · IEC 62443 · TISAX · CMMC
- ▶ Reports generated within hours
- ▶ Structured evidence for regulators
- ▶ Board and customer-audit outputs

Academic Protection

- ▶ IT-to-OT intrusion detection
- ▶ Production line protection
- ▶ IP and design theft forensics
- ▶ Supply chain continuity.

TRACKNOSIS 