



Tracknosis Utilities Edition

White Paper

Forensic Observability, Threat Detection and Regulatory Compliance for Energy and Water Utilities

Making the
Unknown
Known



Executive Summary

Energy and water utilities operate the critical national infrastructure that society depends on every hour of every day — power generation and distribution, gas networks, water treatment and supply, and wastewater services. They are prime targets for nation-state actors, ransomware syndicates, and hacktivists seeking to disrupt essential services, endanger public safety, or extract ransom under the threat of blackout or contamination.

At the same time, regulations and mandates including NIS2, CIRCIA, NERC CIP, the EU Critical Entities Resilience (CER) Directive, and America's Water Infrastructure Act (AWIA) now require utilities 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, and SCADA servers that sit at the IT/OT boundary. It continuously transforms endpoint and server telemetry into trusted forensic evidence, enabling utilities 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 Energy and Water Cybersecurity Challenge

Utilities run converged IT and operational technology (OT) estates: corporate networks alongside SCADA, distributed control systems, and remote field assets — often blending modern platforms with decades-old equipment. Conventional monitoring tools generate alerts, but rarely answer the question investigators and control-room engineers need most: what actually happened, and did it cross from IT into the systems that keep the lights on and the water safe?



Nation-State Attacks - Advanced persistent threats target grids, pipelines, and water systems for disruption and coercion.



Ransomware - Attacks on billing, SCADA, and engineering systems can halt operations and threaten public safety.



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



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



Insider Threats – Operators, engineers, and contractors with privileged access present sabotage and data theft risk.



Reporting Gap – Without forensic evidence, meeting NIS2, DORA, GDPR, NAIC, and NYDFS 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. 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
SIEM / OT Integration	Forensic enrichment of Splunk, Elastic, Datadog, Cisco XDR, and Microsoft Sentinel

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 customer records were affected
- ▶ Produce an evidence timeline for regulators, safety bodies, and counsel

Threat Detection

- ▶ Ransomware: mass file modification, extension changes, shadow copy deletion
- ▶ OT pivot: unexpected changes on engineering workstations, HMIs, and historians
- ▶ Nation-state: new persistence artifacts and lateral movement between scans
- ▶ Timestamping: 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 utility 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, NERC CIP, CER and AWIA

Utilities face mandatory cyber incident reporting obligations that require forensic evidence, structured timelines, and regulator-ready reports — often within 72 hours, and in some cases far sooner. Tracknosis generates this evidence automatically from its continuously maintained forensic repository.

Regulation / Framework	Scope in Utilities	Key Obligation	Tracknosis Support
NIS2 (EU)	Energy and water operators classified as essential 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 infrastructure including electric, gas, and water utilities	Report significant incidents to CISA within 72 hrs; ransomware payments within 24 hrs	Tamper-evident artifact preservation, incident documentation, and response records
NERC CIP (North America)	Bulk electric system owners, operators, and users	Protect critical cyber assets; report reportable cyber security incidents to E-ISAC	Forensic evidence of changes to in-scope Windows assets and audit-ready control records
EU CER Directive	Critical entities in the energy and drinking-water sectors	Resilience measures, incident notification, and demonstrable risk management	Continuous forensic monitoring and evidence supporting resilience and notification duties
AWIA / EPA (US Water)	US community water systems and wastewater utilities	Risk and resilience assessments; safeguard treatment and supply control systems	Forensic audit trail of changes to water-system Windows hosts and user attribution

Energy and Water Use Cases



Ransomware Response

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



Nation-State Sabotage

Detect stealthy persistence and tampering on control-system hosts; reconstruct the attack for national authorities



Supply Chain Compromise

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



Customer & Billing Data

Identify which customer or metering records were accessed; produce GDPR/CCPA notification content



IT-to-OT Intrusion

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



Insider Threat Investigation

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



Service Continuity

Identify anomalies affecting generation, distribution, treatment, or supply before customer-facing outages



Post-Incident Analysis

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

Value to CIOs, CISOs, and OT Security Leaders

For utilities balancing public service, safety, and national-security obligations, Tracknosis delivers measurable operational assurance. It provides early warning of threats and anomalies, accelerates forensic investigation, supports regulatory reporting, and helps protect the IT/OT boundary – all without replacing existing security investments or disrupting control systems.

Measurable Outcomes:

- ▶ Reduced mean time to detect (MTTD) and mean time to resolve (MTTR) cyber incidents.
- ▶ Rapid root cause identification — reducing reliance on scarce external forensic specialists.
- ▶ Improved uptime and reliability across generation, distribution, treatment, and supply.
- ▶ Regulatory reporting compliance — forensic evidence packages ready within hours, not days.
- ▶ Evidence-based forensic reporting for boards, regulators, and safety authorities.
- ▶ Enhanced collaboration between IT security, OT engineering, compliance, and operations.
- ▶ Strengthened public and regulator trust in the resilience of essential services.
- ▶ Reduced cost and duration of cyber incident investigations and regulatory responses.

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, sovereign, and segmented OT-aligned deployments.

Supported Platforms	Windows 11; Windows Server 2016–2025; engineering/HMI 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 Energy and Water Utilities

Utilities cannot afford prolonged investigations, regulatory penalties, or the public-safety and reputational consequences 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, safety authorities, and the public demand.

Forensic Observability	Regulatory Compliance	Academic Protection
<ul style="list-style-type: none"> ▶ Continuous disk-level evidence ▶ Delta analysis across IT and OT hosts ▶ AI-assisted investigation ▶ Evidence independent of log tampering 	<ul style="list-style-type: none"> ▶ NIS2 · CIRCIA · NERC CIP · CER · AWIA ▶ Reports generated within hours ▶ Structured evidence for regulators ▶ Board and safety-authority outputs 	<ul style="list-style-type: none"> ▶ IT-to-OT intrusion detection ▶ Insider and sabotage attribution ▶ Ransomware early detection ▶ Service continuity assurance

