



Tracknosis Insurance Edition

White Paper

Forensic Observability, Threat Detection and Regulatory Compliance for the Insurance Industry

**Making the
Unknown
Known**





Executive Summary

Insurers, reinsurers, and brokers hold vast repositories of policyholder personal data, claims histories, medical records, and financial information — making them high-value targets for ransomware operators, fraud syndicates, and nation-state actors. A single breach threatens regulatory penalties, policyholder trust, and the integrity of underwriting and claims operations.

Regulations including NIS2, DORA, GDPR, the NAIC Insurance Data Security Model Law, and NYDFS Part 500 now require insurers to detect, investigate, and report significant incidents within hours — supported by defensible forensic evidence.

Tracknosis is a Forensic Observability platform built for Windows environments. It continuously transforms endpoint and server telemetry into trusted forensic evidence, enabling insurers to detect threats early, perform rapid root cause analysis, and produce regulatory-ready incident reports — strengthening both their own cyber posture and the quality of the cyber risk they underwrite — without relying on costly external forensic specialists.

The Insurance Cybersecurity Challenge

Insurance carriers run complex estates spanning underwriting platforms, claims systems, broker portals, and actuarial data lakes — often integrated with third-party administrators and managed service providers. Conventional monitoring tools generate alerts, but rarely answer the question investigators and claims teams need most: what actually happened, and which policyholder records were affected?



Ransomware – Encryption of claims and underwriting systems halts payouts and disrupts policyholder service.



Policyholder Data – Personal, medical, and financial records are prime targets for theft, extortion, and resale.



Claims Fraud – Tampering with claims records and supporting evidence drives fraudulent payouts and leakage.



Third-Party Risk – Brokers, TPAs, and MSPs with system access expand the attack surface beyond the carrier.



Insider Threats – Adjusters, agents, and contractors with legitimate access present data theft and tampering 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. 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.

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 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 initial entry to impact
- ▶ Attribute every forensic change to a specific user and session
- ▶ Quantify which policyholder records or claims data were affected
- ▶ Produce an evidence timeline for regulators, reinsurers, and counsel

Threat Detection

- ▶ Ransomware: mass file modification, extension changes, shadow copy deletion
- ▶ Insider threat: bulk policyholder data access outside normal working patterns
- ▶ Claims tampering: unauthorised modification of claims records 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 insurance security 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 data exfiltration).



Regulatory Compliance: NIS2, DORA, GDPR, NAIC and NYDFS

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

Regulation / Framework	Scope in Insurance	Key Obligation	Tracknosis Support
NIS2 (EU)	Insurers classified as essential or important entities in EU member states	Early warning within 24 hrs; full notification within 72 hrs; board accountability	Forensic timeline, evidence preservation, and structured regulatory report within hours
DORA (EU)	Insurance and reinsurance undertakings as financial entities under EU oversight	ICT risk management, major incident classification and reporting, resilience testing	Forensic incident classification evidence and tamper-evident records for ICT reporting
GDPR / UK GDPR	All insurers processing policyholder, claimant, and employee personal data	Notify supervisory authority within 72 hrs; identify data categories and affected individuals	Precise identification of affected records, user attribution, and breach notification content
NAIC Insurance Data Security Model Law	US insurers and licensees in states that have adopted the model law	Maintain an information security program; notify the commissioner of cybersecurity events	Forensic event documentation, scope determination, and notification-ready evidence
NYDFS 23 NYCRR Part 500	Insurance entities licensed under New York State financial regulation	Report cybersecurity events within 72 hrs; demonstrate controls and audit trails	Continuous forensic monitoring and audit-ready evidence for required certifications

Insurance Industry Use Cases



Ransomware Response

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



Claims Fraud Investigation

Detect tampering with claims records and evidence; attribute changes to specific accounts and sessions



Third-Party & TPA Risk

Detect compromise introduced via brokers, third-party administrators, and managed service providers



Regulatory Audit Readiness

Maintain continuous forensic audit trails for NIS2, DORA, GDPR, NAIC, and NYDFS obligations



Policyholder Data Breach

Identify which records were accessed, when, and by whom; produce GDPR/NAIC/NYDFS notification content



Insider Threat Investigation

Attribute file and system changes to specific adjuster agent, or contractor accounts



Underwriting Continuity

Identify anomalies and security events affecting underwriting and pricing platforms before disruption



Post-Incident Analysis

Reconstruct the complete attack chain; quantify impact for reinsurers, legal, and capital reporting

Value to CIOs, CISOs, and Chief Risk Officers

For insurers balancing growth with stringent regulation, Tracknosis delivers measurable operational assurance. It provides early warning of threats and anomalies, accelerates forensic investigation, supports regulatory reporting, and protects the integrity of underwriting and claims operations — all without replacing existing security investments.

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 underwriting, claims, and policyholder services.
- ▶ Regulatory reporting compliance — forensic evidence packages ready within hours, not days.
- ▶ Evidence-based forensic reporting for boards, risk committees, and reinsurers.
- ▶ Enhanced collaboration between security, risk, compliance, and claims leadership.
- ▶ Strengthened policyholder trust and protection of the carrier brand and reputation.
- ▶ Reduced cost and duration of cyber incident investigations and regulatory responses.

Benefits for Insurers and Impact on Cyber Insurance Premiums

Forensic Observability changes the economics of cyber risk on both sides of the policy. For carriers, it sharpens underwriting and reduces loss severity. For the organisations they insure, demonstrable forensic readiness is increasingly rewarded with more favourable premiums, terms, and coverage. Tracknosis provides the verifiable evidence that links good security practice to measurable pricing outcomes.

Benefits to the Insurer (Underwriter)

Better Risk Selection	Forensic evidence of controls and incident readiness improves the accuracy of underwriting and pricing
Lower Loss Severity	Faster detection and containment reduce breach impact, shrinking claim sizes and loss ratios
Reduced Claims Leakage	Tamper-evident timelines validate claims, expose fraud, and support accurate, defensible payouts
Stronger Subrogation	Defensible evidence chains support recovery actions against negligent third parties and attackers
Portfolio Insight	Aggregated forensic readiness signals improve modelling of systemic and accumulation risk
Faster Claim Validation	Ready-made forensic packages accelerate adjusting, reducing investigation cost and cycle time

Benefits to the Insured (Policyholder)

Demonstrable Controls	Continuous forensic monitoring satisfies insurer questionnaires and security control attestations
Lower Risk Rating	Evidence of rapid detection and response (reduced MTTD/MTTR) supports a lower assessed risk tier
Faster Claims	Ready-made forensic evidence packages accelerate claim validation and payout after an incident
Fewer Coverage Gaps	Documented controls reduce the risk of claim disputes or denials over inadequate security

Impact on Premiums Paid

Cyber insurers increasingly price policies on demonstrable security maturity rather than attestation alone. Organisations running Tracknosis can evidence the specific controls and response capabilities that underwriters reward – directly influencing the premium they pay – while carriers benefit from a lower-risk, better-evidenced portfolio.

Premium Reductions	A stronger, evidenced posture can translate into reduced premiums and a more favourable rate-on-line
Better Terms	Improved readiness can support lower deductibles/retentions and higher coverage limits
Faster Underwriting	Forensic readiness evidence streamlines underwriting reviews and renewal negotiations
Healthier Loss Ratios	For the carrier, reduced breach severity and fraud leakage support sustainable, competitive pricing

Note: Premium outcomes depend on each insurer's underwriting model, the policyholder's overall risk profile, and prevailing market conditions. Tracknosis provides the verifiable forensic evidence that supports these conversations; it does not guarantee a specific premium reduction.



Deployment and Governance

Tracknosis deploys rapidly across Windows workstations, servers, clinical hosts, and Citrix environments with no system reboot required. It integrates with existing IT management tooling and requires no dedicated database infrastructure.

Supported Platforms	Windows 11; Windows Server 2016–2025; 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
SIEM Integration	Splunk, Elastic, Datadog, Cisco XDR, Microsoft Sentinel — extends existing investments
AI Investigation	ChatGPT and Claude integration for natural-language forensic queries and report drafting
Access Control	Granular RBAC and immutable audit logs; data sovereignty and retention controls

Why Tracknosis for Insurance

Insurers cannot afford prolonged investigations, regulatory penalties, or the 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 policyholders demand.

Forensic Observability

- ▶ Continuous disk-level evidence
- ▶ Delta analysis across every endpoint
- ▶ AI-assisted investigation
- ▶ Evidence independent of log tampering

Regulatory Compliance

- ▶ NIS2 · DORA · GDPR · NAIC · NYDFS
- ▶ Reports generated within hours
- ▶ Structured evidence for regulators
- ▶ Board and reinsurer-ready outputs

Academic Protection

- ▶ Ransomware early detection
- ▶ Insider threat attribution
- ▶ Policyholder data breach forensics
- ▶ Claims fraud investigation

TRACKNOSIS

