



Issue In: 29th June 2026

Tracknosis Technical

White Paper

Forensic Observability Platform
Version 2.0 | 2026

*Transforming Telemetry into Forensic
Intelligence, AI-Powered Investigation &
Regulatory-Ready Reporting*

Table of Contents

1. Executive Summary.....	3
Key Platform Capabilities.....	3
2. Introduction and Problem Statement.....	4
2.1. The Cost of Investigation Uncertainty.....	4
2.2. Limitations of Existing Approaches.....	5
3. Introducing Forensic Observability	5
3.1. The Six Generations of Cybersecurity.....	5
3.2. Evidence Sources Correlated by Tracknosis.....	6
4. Platform Overview	6
5. Enterprise Reference Architecture	7
5.1. Architecture Components	7
5.2. Data Flow Summary.....	8
6. Technical Components.....	9
6.1. Forensic Data Collection	9
6.2. NTFS Forensic Disk Scanning	10
6.3. Delta Analysis and Change Detection.....	10
6.4 Behavioral Detection Engine	11
6.5 Risk Scoring Methodology	12
6.6. Forensic Timeline Reconstruction.....	12
6.7. AI-Assisted Investigation.....	13
7. Integration Ecosystem.....	14
8. Deployment Model.....	15
8.1. Supported Deployment Modes	15
8.2. Deployment Methods.....	15

8.3. Supported Platforms.....	16
8.4. Performance Considerations.....	16
9. Security and Data Integrity	16
9.1. Encryption at Rest.....	16
9.2. Encryption in Transit.....	16
10. Chain of Custody and Evidence Integrity	17
11. Regulatory Compliance.....	18
11.1. Regulatory Report Content.....	18
12. Use Cases.....	19
12.1. Ransomware Detection and Response.....	19
12.2. Insider Threat Detection.....	19
12.3. Unknown and Zero-Day Threat Detection.....	19
12.4. Incident Response and Post-Breach Analysis.....	20
12.5. Asset Governance and Change Management	20
13. Competitive Positioning	21
14. Future Roadmap.....	22
15. Conclusion.....	23
Appendix A: MITRE ATT&CK Mapping	24
Appendix B: Supported Platforms and Requirements	25
Appendix C: Glossary	26



Confidentiality Notice

This document contains proprietary and confidential information relating to the Tracknosis Platform. It is intended solely for authorised customers, strategic partners, systems integrators, security architects, and technology investors. Reproduction or disclosure without written consent is strictly prohibited.



1. Executive Summary

Tracknosis is a Forensic Observability platform that transforms Windows endpoint and server telemetry into trusted forensic evidence, root-cause intelligence, and regulatory-ready incident reports. It answers the questions that matter most during a cyber incident: What happened? When? Who? Why? What changed?

Modern enterprises generate enormous volumes of security telemetry through SIEM platforms, endpoint detection tools, and observability solutions. Yet security teams routinely spend hours or days reconstructing incidents because telemetry alone does not constitute forensic truth. Tracknosis bridges this gap by combining Windows Security Event Log analysis, direct NTFS forensic disk parsing, and sequential delta analysis into a continuously evolving forensic evidence repository.

The platform integrates seamlessly with Splunk, Elastic, Datadog, Cisco XDR, and Microsoft Sentinel, extending the value of existing investments rather than replacing them. AI-assisted investigation via ChatGPT, Claude, and enterprise LLMs enables natural-language interrogation of forensic evidence, accelerating root-cause analysis and regulatory report generation.

Key Platform Capabilities

Capability	Description
Forensic Data Collection	Windows Security Event Logs, NTFS MFT, \$UsnJrnl, \$LogFile, Registry hives
Delta Analysis	Scan-over-scan change detection identifying file, metadata, and configuration drift
Behavioral Detection	Risk-scored detection of ransomware, insider threats, and living-off-the-land activity
Timeline Reconstruction	Unified forensic timeline correlated from multiple authoritative evidence sources
AI-Assisted Investigation	Natural-language reporting and analysis via ChatGPT, Claude, and enterprise LLMs

Capability	Description
SIEM Integration	Native integration with Splunk, Elastic, Datadog, Cisco XDR, Microsoft Sentinel
Regulatory Reporting	Evidence-backed reports for NIS2, CIRCIA, SOCI, and national cyber frameworks
Evidence Integrity	AES-256 / Blowfish 448-bit encryption; TLS 1.3 transport; cryptographic hashing

Tracknosis is designed for Windows 11, Windows Server 2016 through 2025, and Citrix Virtual Apps and Desktop environments. It requires no dedicated SQL Server or Oracle database, can be deployed in minutes for pilots, and scales enterprise-wide via SCCM, Intune, Group Policy, MSI, or PowerShell.

2. Introduction and Problem Statement

Cybersecurity has evolved through five generations: infrastructure monitoring, log management, SIEM, observability, and AI observability. Each generation improved detection and visibility. Yet a fundamental challenge persists: organizations can collect telemetry at scale, but still struggle to determine with forensic certainty what actually happened during a cyber incident.

2.1. The Cost of Investigation Uncertainty

Security Operations Centre analysts face the following persistent challenges:

- ▶ Alert fatigue from thousands of low-fidelity notifications with limited investigative context
- ▶ An average of 167 days between intrusion and detection for sophisticated threats
- ▶ Manual correlation of evidence scattered across multiple disconnected security consoles
- ▶ Audit logs that are incomplete, rotated, misconfigured, or deliberately cleared by attackers
- ▶ Regulatory obligations requiring evidence preservation and timeline reconstruction within hours

- ▶ High cost of external digital forensics specialists engaged during incident response

2.2 Limitations of Existing Approaches

Technology	Strength	Gap
SIEM	Aggregates and correlates security events at scale	No disk-level forensic truth; no evidence preservation
EDR / XDR	Detects and isolates endpoint threats rapidly	Signature-reliant; agent can be disabled; weak forensic reconstruction
Observability	Application and infrastructure performance insight	Designed for availability, not forensic investigation
Traditional DFIR	Deep forensic analysis capability	Manual, expensive, point-in-time; not continuous

Tracknosis addresses these gaps by introducing Forensic Observability: a continuous, evidence-centric discipline that transforms operational telemetry into trusted investigative intelligence.

3. Introducing Forensic Observability

Forensic Observability is the discipline of transforming telemetry into trusted forensic intelligence. It combines multiple evidence sources into a continuously evolving investigative record capable of reconstructing cyber incidents with the confidence required for regulatory submission and legal proceedings.

3.1. The Six Generations of Cybersecurity

Generation	Discipline	Primary Question Answered
Generation 1	Infrastructure Monitoring	Is the system available?
Generation 2	Log Management	What happened historically?
Generation 3	SIEM	Is there suspicious activity?
Generation 4	Observability	Why is the application behaving this way?
Generation 5	AI Observability	How is the AI model performing?
Generation 6	Forensic Observability (Tracknosis)	What happened, when, who, why, and what changed?

3.2. Evidence Sources Correlated by Tracknosis

Tracknosis correlates evidence from the following sources to produce forensic certainty:

- ▶ Windows Security Event Logs (authentication, object access, privilege use, audit log clearing)
- ▶ Windows Event Forwarding (WEF) – centralised enterprise event collection via WEC
- ▶ NTFS Master File Table (MFT) – comprehensive file system metadata
- ▶ Application and service telemetry (via SIEM integration)
- ▶ Threat intelligence feeds

4. Platform Overview

Tracknosis is a Windows-native forensic observability platform that operates across four functional layers. Each layer is independently testable and replaceable, enabling modular deployment aligned to organisational requirements.



Acquisition Layer

Collects forensic artifacts from NTFS disk structures and Windows Security Event Logs. Operates in read-only mode where applicable to preserve evidence integrity.



Preservation Layer

Applies cryptographic hashing to all collected artifacts. Stores data using Blowfish 448-bit or AES-256 encryption. Maintains a tamper-evident audit trail throughout the data lifecycle.



Analysis Layer

Performs sequential scan delta analysis, forensic timeline reconstruction, behavioral risk scoring, and root-cause correlation across all collected evidence.



Governance Layer

Provides audit logging, structured reporting, SIEM integration, regulatory report generation, and AI-assisted natural-language investigation capabilities.

5. Enterprise Reference Architecture

The Tracknosis enterprise reference architecture illustrates the data flow from protected endpoints and servers through centralised event collection, secure forwarding, and integration with enterprise SIEM and observability platforms.

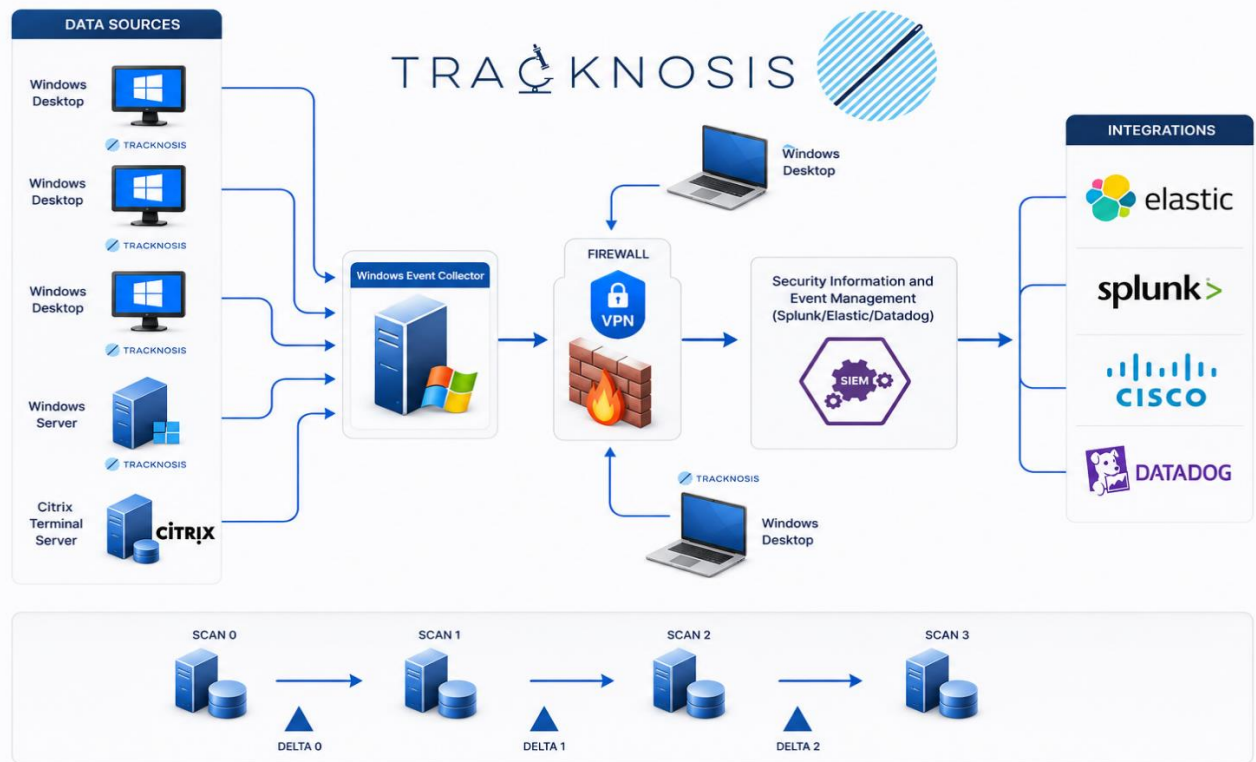


Figure 1— Tracknosis Enterprise Reference Architecture

5.1. Architecture Components

Tracknosis Agent (Windows Endpoint)

A lightweight agent installed on Windows Desktop and laptop endpoints. The agent collects forensic telemetry locally — including NTFS artifacts and Security Event Log data — and forwards events to the Windows Event Collector. No system reboot is required. The agent supports deployment via SCCM, Intune, Group Policy, MSI, and PowerShell.

Windows Server / Citrix Terminal Server

Tracknosis is fully compatible with Windows Server 2016, 2019, 2022, and 2025, as well as Citrix Virtual Apps and Desktop (Terminal Server / Session Host) environments.

The agent collects server-side NTFS and event telemetry using the same collection pipeline as workstation endpoints.

Windows Event Collector (WEC)

The Windows Event Collector centralises Security Event Log data from multiple endpoints and servers using Windows Event Forwarding (WEF). This leverages native Windows infrastructure without requiring a dedicated third-party collection agent on each endpoint.

Firewall / VPN Gateway

All telemetry forwarded from the Windows Event Collector to the central analysis platform traverses the enterprise firewall and VPN boundary. All communications are secured using TLS 1.3 to ensure confidentiality and integrity in transit.

SIEM / Observability Integration

Tracknosis integrates natively with enterprise SIEM and observability platforms including Splunk, Elastic, Datadog, Cisco XDR, and Microsoft Sentinel. Forensic context, risk scores, and timeline data are enriched into existing SIEM workflows rather than replacing them.

Delta Analysis Engine

The delta analysis engine performs sequential NTFS disk scans at configurable intervals. Each scan captures a forensic snapshot of the disk state. The engine computes the difference (delta) between consecutive scans to identify file creations, modifications, deletions, renames, and metadata changes indicative of malicious or unauthorised activity – as illustrated in the architecture diagram (Scan 0 through Scan 3 producing Delta 0 through Delta 2).

5.2. Data Flow Summary

1. Tracknosis agents on Windows endpoints and servers collect NTFS artifacts and Security Event Log data
2. Events are forwarded via Windows Event Forwarding (WEF) to the Windows Event Collector (WEC)
3. Collected telemetry passes through the enterprise firewall/VPN boundary secured by TLS 1.3
4. The Tracknosis Analysis Platform ingests, cryptographically hashes, and encrypts all received artifacts

5. Delta analysis compares sequential disk scans to identify all forensic changes between scan intervals
6. The risk classification engine scores observed changes and generates behavioral detections
7. Timeline reconstruction correlates all evidence sources into a unified investigative record
8. Findings are delivered to SIEM platforms, investigation dashboards, and regulatory report templates
9. AI-assisted investigation enables natural-language queries against the forensic evidence repository

6. Technical Components

6.1. Forensic Data Collection

Tracknosis employs a dual-source collection model combining Windows Security Event Log auditing with direct NTFS forensic disk parsing. This approach ensures forensic completeness even when audit logs are incomplete, rotated, or deliberately cleared by an adversary.

Windows Security Event Log Collection

Event Source	Description
Event ID 4663	File system access — object access performed
Event ID 4656	Object handle requests — access to securable objects
Event ID 4688	Process creation — new process spawned
Event ID 4624 / 4625	Logon success and failure
Event ID 4670	Object permission changes
Event ID 1102 / 104	Audit log cleared — high-fidelity evasion indicator
Registry access events	Modifications to SYSTEM, SOFTWARE, and user hive keys
Privilege use events	Token elevation and sensitive privilege use

6.2. NTFS Forensic Disk Scanning

To complement event-based telemetry, Tracknosis performs direct NTFS disk parsing to extract forensic artifacts independently of the operating system logging subsystem. This enables reconstruction of file system activity even when audit logs have been disabled, rotated, or tampered with.

Master File Table (MFT): Comprehensive file system index containing timestamps, attributes, file sizes, and allocation status for every file and directory on the volume.

\$LogFile Transaction Records: Low-level NTFS transaction log recording file system operations at the driver level, independent of Windows auditing.

\$UsnJrnl Change Journal: NTFS journal recording file creation, modification, deletion, rename, and attribute change events for forensic reconstruction.

SI / FN Timestamp Correlation: Detection of timestamp manipulation (timestomping) by comparing Standard Information and File Name attribute timestamps — a divergence indicates attacker tampering.

Deleted and Hidden Artifacts: Recovery of forensic artifacts from unallocated MFT entries and analysis of hidden or renamed files not visible through normal file system APIs.

Registry Hive Analysis: Offline parsing of SYSTEM, SOFTWARE, SAM, SECURITY, and NTUSER.DAT registry hives to identify persistence artifacts and configuration changes between scans.

6.3. Delta Analysis and Change Detection

At the core of Tracknosis is the delta analysis engine — a forensic change detection system that operates by comparing sequential NTFS disk snapshots over time. Each scan captures a complete forensic state of the disk. The delta between consecutive scans reveals precisely what changed and when.

As illustrated in the architecture diagram: Scan 0 establishes a baseline. Scan 1 produces Delta 0 (changes since baseline). Scan 2 produces Delta 1, and Scan 3 produces Delta 2. This continuous model enables detection of unknown and emerging threats without relying on predefined signatures or indicators of compromise.

Change Categories Detected

- ▶ File creations — new files appearing between scans, including malware drops and staged payloads
- ▶ File modifications — content or metadata changes to existing files
- ▶ File deletions — files present in the previous scan absent from the current scan
- ▶ Rename and extension changes — files moved or renamed (common ransomware staging indicator)
- ▶ Timestamp modifications — SI/FN divergence indicating attacker timestomping
- ▶ Attribute changes — hidden, system, or read-only flag modifications
- ▶ Entropy changes — elevated file entropy indicative of encryption or packing activity
- ▶ Persistence artifacts — new autorun keys, scheduled tasks, or service entries between scans

6.4 Behavioral Detection Engine

Tracknosis combines forensic change analysis with behavioral indicators to detect malicious or unauthorised activity. Rather than relying on signature matching, the behavioral detection engine evaluates patterns of activity across forensic evidence sources.

- ▶ High-frequency file modification or deletion within a defined time window (ransomware pattern)
- ▶ Mass extension changes across multiple directories (encryption staging)
- ▶ Shadow copy and backup artifact deletion following mass file activity
- ▶ Registry persistence modifications (autorun keys, service creation)
- ▶ Abnormal process lineage and execution paths (living-off-the-land techniques)
- ▶ Discrepancies between Windows Security Event Logs and NTFS artifacts (log evasion)
- ▶ Repeated access denials or privilege escalation attempts
- ▶ Unauthorized access to sensitive directories outside normal working patterns
- ▶ Timestomping: SI and FN timestamp divergence exceeding normal thresholds

- ▶ Security audit log clearing (Event ID 1102/104) correlated with disk activity spikes

6.5 Risk Scoring Methodology

Tracknosis employs a transparent, explainable risk scoring model that classifies observed activity based on forensic evidence rather than signatures. Every risk score is fully traceable to underlying forensic artifacts, enabling analysts to understand precisely why an activity was classified as suspicious.

Scoring Inputs

- ▶ Volume of file creations, edits, and deletions relative to established behavioral baseline
- ▶ Rate of change within configurable time windows
- ▶ Sensitivity and criticality of affected directories or files
- ▶ User privilege context and role (standard versus privileged accounts)
- ▶ Evidence of evasion techniques (timestomping, log gaps, audit log clearing)
- ▶ Divergence between Security Event Log records and NTFS disk artifacts
- ▶ Presence of known persistence artifact patterns in registry or scheduled tasks

Risk Classification

Risk Level	Threshold	Typical Activity
Low	Baseline deviation within normal parameters	Expected or policy-compliant changes; routine software updates
Medium	Elevated change rate or unusual pattern	Unusual but potentially benign activity; warrants analyst review
High	Strong indicators of malicious activity	Ransomware staging, privilege abuse, log evasion, mass deletion

6.6. Forensic Timeline Reconstruction

Tracknosis reconstructs a unified, chronological timeline of system activity by normalising and correlating evidence from Windows Security Event Logs and NTFS disk artifacts. Time skew between sources is automatically resolved to produce an accurate sequence of events.

Timeline Data Sources

- ▶ Windows Security Event Logs (process creation, object access, logon and authentication events)
- ▶ NTFS MFT timestamps – Standard Information (SI) and File Name (FN) attributes
- ▶ NTFS \$UsnJrnl change journal records (file modification sequence numbers)
- ▶ NTFS \$LogFile transaction data (low-level file system operations)
- ▶ Registry hive last-write timestamps

Windows Event Forwarding (WEF) collected events from centralised WEC

Timeline Capabilities

- ▶ Identify the initial point of compromise and patient-zero endpoint
- ▶ Trace attacker movement and lateral progression across the environment
- ▶ Correlate file changes, deletions, and creations with specific user sessions
- ▶ Detect log evasion attempts including audit log clearing and timestomping
- ▶ Validate or refute investigative hypotheses with forensic evidence citations
- ▶ Reconstruct timelines from live systems or offline disk images

6.7. AI-Assisted Investigation

Tracknosis integrates with enterprise AI platforms including OpenAI ChatGPT, Anthropic Claude, and organisation-hosted large language models to enable natural-language investigation of forensic evidence. AI assistance is grounded in verifiable forensic data, ensuring that AI-generated findings can be traced to underlying evidence artifacts – preserving evidential integrity for regulatory and legal proceedings.

- ▶ Natural-language querying of forensic evidence repositories
- ▶ Automated hypothesis generation based on observed behavioral patterns
- ▶ AI-assisted root-cause analysis with evidence citations
- ▶ Automated draft generation for regulatory incident reports
- ▶ Prioritisation of high-risk findings during large-scale incidents

- ▶ Translation of technical forensic findings into executive-ready summaries

7. Integration Ecosystem

Tracknosis is designed to complement rather than replace existing enterprise security investments. Forensic context, risk scores, and timeline data are enriched into existing platforms, increasing the return on investment from existing SIEM and observability deployments.

Platform	Integration Method	Forensic Value Added
Splunk	API / HEC / Forwarder	Risk scores, timeline events, and NTFS artifact data enriched into Splunk indexes and dashboards
Elastic	Elasticsearch API / Logstash	NTFS change data, behavioral detections, and timeline records indexed for Kibana investigation
Datadog	Datadog API / Agent	Forensic telemetry and risk events delivered into Datadog SIEM and observability pipelines
Microsoft Sentinel	Azure Monitor / Log Analytics	Forensic timelines and detection findings ingested into Microsoft Sentinel workspaces
ChatGPT (OpenAI)	OpenAI API	Natural-language forensic investigation and AI-assisted regulatory report drafting
Claude (Anthropic)	Anthropic API	AI-assisted root-cause analysis, reasoning, and evidence-backed report generation
Enterprise LLMs	Custom API / On-premise	Organisation-hosted LLM support for air-gapped or data-sovereign environments
SOAR Platforms	Webhook / REST API	Automated playbook triggering based on Tracknosis forensic risk thresholds

8. Deployment Model

Tracknosis is engineered for rapid, flexible enterprise deployment. No system reboot, dedicated database server, or complex infrastructure prerequisite is required for core platform operation.

8.1. Supported Deployment Modes

Windows Service

Deployed as a persistent Windows service via Topshelf or native SCM. Starts automatically on boot and resumes monitoring without manual intervention.

Background Agent

Deployed as a lightweight background agent suitable for endpoints requiring minimal footprint.

Forensic Capture Tool

Deployed on-demand for incident response scenarios where a full agent deployment is not practical; performs one-time or scheduled forensic capture.

Offline Disk Analysis

Supports forensic analysis of offline disk images, enabling investigation of decommissioned or isolated systems without a running agent.

8.2. Deployment Methods

- ▶ Microsoft System Center Configuration Manager (SCCM / MECM)
- ▶ Microsoft Intune (cloud-managed endpoint deployment)
- ▶ Active Directory Group Policy Object (GPO)
- ▶ MSI installer package
- ▶ PowerShell deployment script
- ▶ Manual installation for small environments or pilot deployments

8.3. Supported Platforms

Platform Category	Supported Versions
Windows Desktop / Laptop	Windows 11 (all editions)
Windows Server	Windows Server 2016, 2019, 2022, 2025
Citrix Environments	Citrix Virtual Apps and Desktops (Terminal Server / Session Host)
Disk Image Analysis	NTFS volumes from any supported Windows version

8.4. Performance Considerations

Aggressive early-stage event filtering to eliminate noise before processing

Configurable scan intervals to balance forensic granularity with resource consumption

9. Security and Data Integrity

9.1. Encryption at Rest

All forensic data, scan results, and behavioral telemetry are protected using strong cryptographic encryption:

- ▶ Blowfish 448-bit encryption — the embedded forensic repository uses Blowfish 448-bit for extended cryptographic strength in high-assurance environments
- ▶ AES-256 — available for environments requiring standards-aligned high-performance encryption
- ▶ Encryption keys are managed locally or via enterprise key management solutions

9.2. Encryption in Transit

All telemetry and forensic data transmitted between Tracknosis components and external platforms is protected using TLS 1.3, ensuring confidentiality, integrity, and protection against man-in-the-middle attacks across all communication channels.

10. Chain of Custody and Evidence Integrity

Tracknosis is designed to support forensic best practices and evidential integrity throughout the complete data lifecycle — from acquisition through analysis and regulatory reporting.

Evidence Acquisition

- ▶ Forensic scans operate in read-only mode where applicable to preserve source data
- ▶ Disk artifacts are collected without modification to original evidence
- ▶ All acquisition actions are logged and timestamped with operator attribution

Evidence Preservation

- ▶ All collected artifacts are immediately cryptographically hashed at acquisition
- ▶ Hashes are verified on every subsequent access and analysis operation
- ▶ Encrypted storage using Blowfish 448-bit or AES-256 ensures confidentiality and integrity

Evidence Analysis

- ▶ All analysis operations are logged and attributed to the performing user or process
- ▶ Analysis does not modify original artifacts; working copies are used for all processing
- ▶ Findings are reproducible from preserved artifacts using documented, auditable methodologies

Evidence Reporting

- ▶ Reports include explicit citations to the underlying forensic artifacts supporting each finding
- ▶ Risk scores are fully traceable to the evidence from which they were derived
- ▶ Structured export formats support regulatory submission and legal proceedings

11. Regulatory Compliance

Governments worldwide are strengthening cybersecurity legislation. Tracknosis has been designed with regulatory reporting obligations in mind, enabling organizations to produce structured, evidence-based incident reports suitable for executive review and regulatory submission within mandatory reporting windows.

Regulation	Jurisdiction	Tracknosis Support
NIS2 Directive	European Union	Evidence preservation, timeline reconstruction, and regulator-ready reports within 72-hour windows
CIRCA	United States	Forensic evidence collection, timeline reconstruction, and structured incident reports for critical infrastructure
SOCI Act	Australia	Forensic evidence preservation and timeline reconstruction aligned to SOCI reporting obligations
UK NIS Regulations	United Kingdom	Incident evidence and structured reporting for network and information system operators
Canada CCSP	Canada	Evidence-based reporting aligned to emerging critical cyber systems protection legislation

11.1. Regulatory Report Content

- ▶ Incident summary with executive-ready narrative
- ▶ Forensic timeline from initial compromise through containment and recovery
- ▶ Root-cause analysis supported by evidence citations
- ▶ List of affected systems, users, and data categories
- ▶ Evidence of detection and response actions with timestamps
- ▶ Recommendations for remediation and security control improvement
- ▶ Cryptographic evidence of report integrity for submission authenticity

12. Use Cases

12.1. Ransomware Detection and Response

Ransomware attacks produce distinctive forensic patterns detectable through delta analysis: mass file modification events, extension changes, shadow copy deletion, and entropy spikes consistent with encryption activity. Tracknosis detects these patterns by comparing sequential NTFS scans, enabling early detection before encryption propagates across the entire estate.

- ▶ Mass file modification events within a defined time window
- ▶ Extension and rename patterns consistent with ransomware encryption staging
- ▶ Shadow copy and backup artifact deletion correlated with disk activity
- ▶ Security Event Log gaps correlated with elevated disk modification rates
- ▶ Ransom note file creation across directories

12.2. Insider Threat Detection

By attributing forensic changes to specific users and sessions, Tracknosis identifies insider threat activity that may appear legitimate to signature-based or network-only detection tools.

- ▶ Unauthorised access to sensitive data directories outside normal working patterns
- ▶ Bulk file copying or staging activity before departure events
- ▶ Policy violations and data tampering by privileged accounts
- ▶ Credential sharing or session reuse anomalies
- ▶ Data movement to removable media or external network locations

12.3. Unknown and Zero-Day Threat Detection

Traditional signature-based detection cannot identify unknown malware. Tracknosis identifies suspicious behavioral patterns independent of signatures by analysing what changed on disk rather than relying on memory-resident process telemetry alone.

- ▶ New persistence artifacts appearing between scan intervals without corresponding change records
- ▶ Unusual process execution paths modifying protected system directories
- ▶ Living-off-the-land technique artifacts (LOLBins leaving disk traces)
- ▶ Abnormal configuration changes inconsistent with authorised change management records
- ▶ Behavioral anomalies detected without a corresponding SIEM alert

12.4. Incident Response and Post-Breach Analysis

Tracknosis accelerates incident response by providing investigators with a pre-built forensic evidence repository and timeline, significantly reducing the time required to identify scope, root cause, and business impact.

- ▶ Rapid identification of the initial compromise point (patient zero) and attack vector
- ▶ Chronological reconstruction of attacker activity across affected systems
- ▶ Preservation of forensic evidence in tamper-evident, encrypted storage
- ▶ Quantification of data accessed, modified, or exfiltrated
- ▶ Evidence-backed reporting for board, legal counsel, insurers, and regulators

12.5. Asset Governance and Change Management

Beyond security investigations, Tracknosis provides continuous asset governance by tracking disk-level configuration drift and enforcing change management accountability.

- ▶ Monitoring of critical file and configuration integrity against approved baselines
- ▶ Detection of unauthorised software installation, removal, or modification
- ▶ Tracking infrastructure configuration changes against approved change records
- ▶ Historical records of system state for compliance audit and regulatory review

13. Competitive Positioning

Tracknosis occupies a distinct category between endpoint detection platforms, SIEM solutions, and traditional digital forensic tools. It is not a replacement for any of these technologies — it is the forensic intelligence layer that makes existing investments more effective.

Capability	EDR / XDR	SIEM	Tracknosis
Disk-level forensic truth	Limited	No	Yes — core capability
Signature-free detection	Partial	Partial	Yes — behavioral delta analysis
Log-tamper resilience	No	No	Yes — NTFS independent of logs
Forensic timeline reconstruction	Limited	Limited	Yes — multi-source correlated
Evidence integrity / chain of custody	No	No	Yes — cryptographic hashing
AI-assisted investigation	Emerging	Emerging	Yes — ChatGPT, Claude, LLMs
Regulatory report generation	No	Partial	Yes — structured reports
Unknown threat detection	Partial	Rule-based	Yes — forensic change analysis
Offline disk image analysis	No	No	Yes
Citrix environment support	Varies	Via logs	Yes — native support

14. Future Roadmap

Tracknosis continues to evolve in response to the changing threat landscape, regulatory environment, and enterprise requirements.



Network Telemetry Integration

Ingestion of network flow and DNS telemetry to extend forensic observability beyond endpoint disk artifacts into network-layer activity.



Machine Learning-Assisted Baselineing

Automated establishment of behavioral baselines per user, endpoint, and role to improve signal-to-noise ratio in behavioral detections.



SOAR Integration

Native integration with SOAR platforms to enable automated forensic evidence collection as part of incident response playbooks.



Cloud Platform Support

Extension of forensic observability to cloud-hosted Windows workloads on AWS, Azure, and GCP.



Linux Forensic Support

Expansion of forensic collection capabilities to Linux endpoints and servers for hybrid environment coverage.



Extended AI Investigation

Deeper integration with AI platforms including fine-tuned forensic investigation models and organisation-specific training on security procedures and policy.

15. Conclusion

Modern organisations no longer suffer from a lack of telemetry. They suffer from a lack of forensic truth.

Tracknosis addresses this challenge by introducing Forensic Observability: a continuous, evidence-centric discipline that transforms Windows endpoint and server telemetry into trusted investigative intelligence, regulatory-ready reporting, and AI-assisted root-cause analysis.

By combining Windows Security Event Log collection, direct NTFS forensic disk parsing, and sequential delta analysis, Tracknosis delivers a forensic evidence repository that remains accurate even when audit logs are incomplete, disabled, or tampered with. Its modular architecture integrates seamlessly with existing SIEM, observability, and AI platforms — extending the value of existing investments rather than replacing them.

For security operations, incident response, digital forensics, compliance, and asset governance teams, Tracknosis provides the forensic intelligence layer that answers the questions that matter: what happened, when, why, who, and what changed.

Appendix A: MITRE ATT&CK Mapping

Tracknosis detection capabilities map to the following MITRE ATT&CK technique categories:

Technique ID	Technique Name	Tracknosis Detection Method
T1486	Data Encrypted for Impact	Mass file modification and extension change detection via delta analysis
T1070	Indicator Removal on Host	Audit log clearing event correlation; NTFS artifact recovery independent of logs
T1547	Boot or Logon Autostart Execution	Registry persistence artifact detection between scans
T1036	Masquerading	Extension and rename pattern analysis; SI/FN timestamp divergence detection
T1083	File and Directory Discovery	Access pattern analysis correlated with Security Event Logs
T1490	Inhibit System Recovery	Shadow copy and backup deletion detection via delta analysis
T1078	Valid Accounts	Anomalous access pattern detection via user attribution on forensic evidence
T1562	Impair Defenses	Audit policy change and log clearing events correlated with disk activity
T1005	Data from Local System	Bulk file access and staging detection via behavioral analysis
T1027	Obfuscated Files or Information	File entropy change detection and attribute modification analysis

Appendix B: Supported Platforms and Requirements

Requirement	Specification
Supported OS (Agent)	Windows 11; Windows Server 2016, 2019, 2022, 2025
Citrix Support	Citrix Virtual Apps and Desktops (Terminal Server / Session Host)
File System	NTFS (required for forensic disk scanning)
Encryption at Rest	Blowfish 448-bit (embedded repository); AES-256 (optional)
Encryption in Transit	TLS 1.3
Database Requirement	None required for core platform operation
Event Collection	Windows Security Event Log; Windows Event Forwarding (WEF)
Deployment Methods	SCCM, Intune, Group Policy, MSI, PowerShell, manual
Reboot Required	No
Disk Image Support	NTFS volumes from any supported Windows version (offline)
AI Integration	OpenAI API (ChatGPT), Anthropic API (Claude), enterprise LLMs
SIEM Integration	Splunk, Elastic, Datadog, Cisco XDR, Microsoft Sentinel

Appendix C: Glossary

Delta Analysis: Comparison of two sequential forensic snapshots to identify file system changes between scan intervals.

Forensic Observability: The discipline of continuously transforming operational telemetry into trusted forensic evidence supporting cyber investigations and regulatory reporting.

MFT: Master File Table — the primary NTFS data structure recording metadata for every file and directory on an NTFS volume.

NTFS: New Technology File System — the primary Windows file system providing journaling, permissions, and forensic artifacts.

\$UsnJrnl: NTFS Update Sequence Number Journal — records all file system changes for forensic reconstruction.

\$LogFile: NTFS transaction log recording low-level file system operations at the driver level.

Timestomping: Attacker technique of modifying file timestamps to evade forensic timeline analysis; detectable by comparing SI and FN NTFS timestamp attributes.

WEF / WEC: Windows Event Forwarding / Windows Event Collector — native Windows infrastructure for centralising Security Event Logs.

TLS 1.3: Transport Layer Security v1.3 — current standard for secure communications in transit.

Chain of Custody: The documented, unbroken sequence of evidence handling from acquisition through analysis and reporting.

LotL / LOLBins: Living-off-the-Land — attacker use of legitimate OS tools to conduct malicious activity, evading signature-based detection.

Root-Cause Analysis: The process of identifying the original cause of an incident by tracing the sequence of events back to the initial compromise.

Patient Zero: The first endpoint or user account compromised in an attack campaign, from which the threat propagated.



TRACKNOSIS



Tracknosis Ltd © 2026 | Making the Unknown Known