TRACKNOSIS

Issue In: 6th July 2026

Tracknosis Education Edition

White Paper

Forensic Observability, Threat Detection and Regulatory Compliance for the Education Sector

Making the Unknown Known

Tracknosis Ltd © 2026

Making the Unknown Known

Executive Summary

Educational institutions manage sensitive student records, research data, and critical digital infrastructure — while facing an escalating wave of ransomware, insider threats, and data breaches. At the same time, regulations including NIS2, CIRCIA, GDPR, and FERPA now mandate that institutions detect, investigate, and report significant incidents within hours, supported by forensic evidence. Tracknosis is a Forensic Observability platform built for Windows environments. It continuously transforms endpoint and server telemetry into trusted forensic evidence, enabling education institutions to detect threats early, perform rapid root cause analysis, and produce regulatory-ready incident reports — without relying on costly external forensic specialists.

The Education Cybersecurity Challenge

Universities, colleges, and schools face a unique threat environment: open campus networks, BYOD policies, thousands of user accounts with varying access levels, and limited security budgets. Conventional monitoring tools generate alerts — but rarely answer the question investigators need most: what actually happened?

Ransomware - Attacks timed around examinations and enrolment deadlines maximise disruption to academic operations.

Insider Threats - Students, staff, and contractors with legitimate access present ongoing data theft and tampering risk.

Research Theft - Nation-state actors target research institutions to exfiltrate intellectual property and grant data.

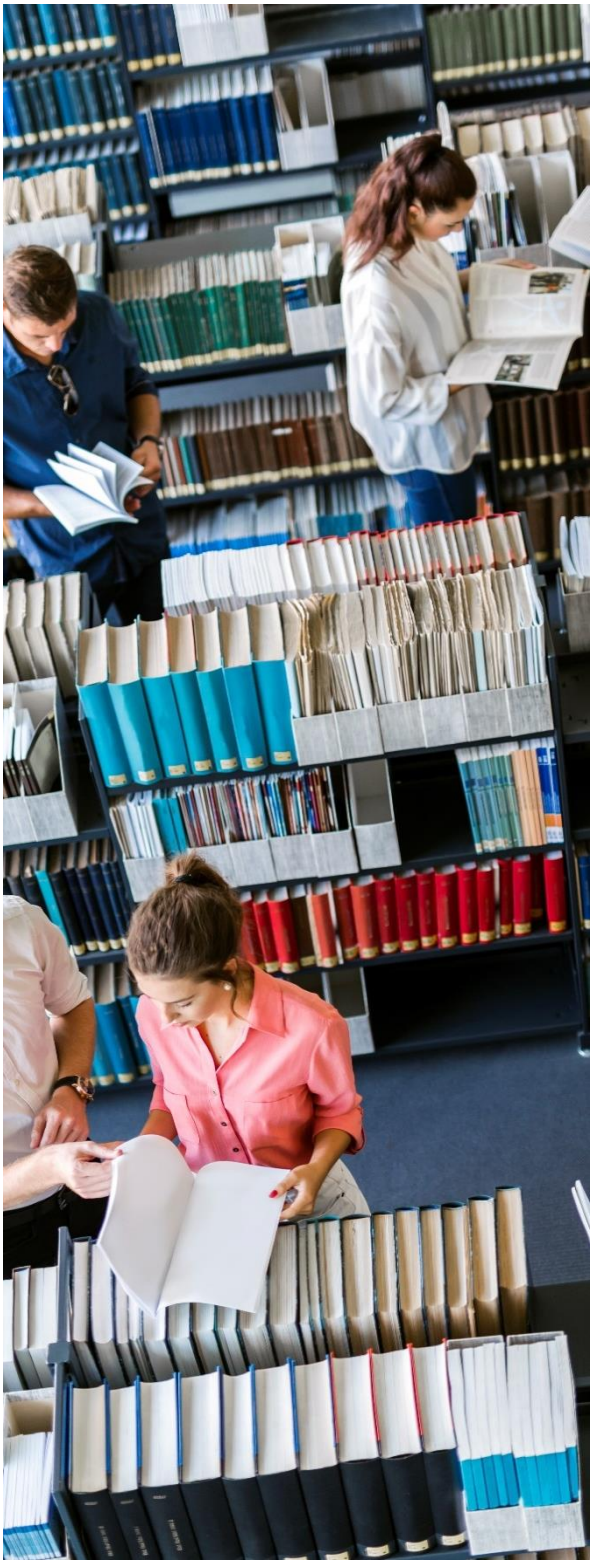
Unknown Attacks - Living-off-the-land techniques and custom malware evade signature-based detection tools.

Alert Fatigue - High volumes of low-fidelity alerts slow investigation and increase mean time to respond.

Regulatory Gap - Without forensic evidence, meeting NIS2, CIRCIA, GDPR, and FERPA reporting 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 student records or research data were affected
- Produce an evidence timeline for regulators and legal counsel

Threat Detection

- Ransomware: mass file modification, extension changes, shadow copy deletion
- Insider threat: bulk data access or copying outside normal working patterns
- Unknown attacks: new persistence artifacts appearing between scan intervals
- 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 education IT 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, CIRCIA, GDPR and FERPA

Education institutions 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	Scope in Education	Key Obligation	Tracknosis Support
NIS2 (EU)	Universities, colleges, and research institutions 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
CIRCIA (US)	Critical infrastructure including federally-funded research institutions	Report significant incidents to CISA within 72 hrs; ransomware payments within 24 hrs	Tamper-evident artifact preservation, incident documentation, and response records
GDPR	All institutions processing EU personal data — student records, staff, research participants	Notify supervisory authority within 72 hrs; identify data categories and affected individuals	Precise identification of affected records, user attribution, and breach notification content
FERPA (US)	US educational institutions receiving federal funding	Safeguard student education records; demonstrate appropriate protective controls	Forensic audit trail of student record access, modification events, and user attribution
NCSC / ISO 27001	UK institutions; institutions seeking or maintaining certification	Baseline security controls; incident management; evidence of control effectiveness	Continuous forensic monitoring; audit-ready evidence for governance and certification review

Education Use Cases

Ransomware Response

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

Student Data Breach

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

Insider Threat Investigation

Attribute file and system changes to specific student or staff accounts; reconstruct timeline of activity

Research Network Protection

Detect data exfiltration and system tampering across collaborative research environments

VLE / LMS Continuity

Identify anomalies and security events affecting learning platforms before academic disruption occurs

Assessment Integrity

Detect unauthorised modification of grade records, exam files, or assessment system configurations

Regulatory Audit Readiness

Maintain continuous forensic audit trails for NIS2, CIRCIA, GDPR, FERPA, and NCSC obligations

Post-Incident Analysis

Reconstruct the complete attack chain; quantify impact for insurance, legal, and governance purposes

Value to CIOs, CISOs, and IT Directors

For educational institutions balancing innovation and stability, Tracknosis delivers measurable operational assurance. It provides early warning of threats and anomalies, accelerates forensic investigation, supports regulatory reporting, and helps maintain uninterrupted academic and research continuity — 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 service reliability across digital learning ecosystems.
- Regulatory reporting compliance — forensic evidence packages ready within hours, not days.
- Evidence-based forensic reporting for audit committees, governing bodies, and board reviews.
- Enhanced collaboration between IT security, governance, legal, and academic leadership.
- Strengthened trust among students, staff, parents, and institutional stakeholders.
- Reduced cost and duration of cyber incident investigations and regulatory responses.

Deployment and Governance

Tracknosis deploys rapidly across Windows workstations, servers, 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 Education

Education institutions 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 demand.

Forensic Observability

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

Regulatory Compliance

- NIS2 · CIRCIA · GDPR · FERPA
- Reports generated within hours
- Structured evidence for regulators
- Board and governance-ready outputs.

Academic Protection

- Ransomware early detection
- Insider threat attribution
- Student data breach forensics
- Research network protection.

Tracknosis Ltd © 2026 | Making the Unknown Known