TRACKNOSIS

Issue In: 6th July 2026

Tracknosis Finance Edition

White Paper

Forensic Observability, Threat Detection and Regulatory Compliance for the Financial Services and Banking Industry

Making the Unknown Known

Tracknosis Ltd © 2026

Making the Unknown Known

Executive Summary

Banks, payment providers, asset managers, and fintechs sit at the centre of the global economy — holding customer funds, account data, and transaction histories that are among the most valuable targets on the planet. They face relentless pressure from ransomware operators, organised fraud syndicates, and nation-state actors, while remaining accountable to regulators, boards, and customers for the security and continuity of financial services. Regulations including NIS2, DORA, PCI DSS, GDPR, SOX, and GLBA now require financial institutions 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 financial institutions to detect threats early, perform rapid root cause analysis, and produce regulatory-ready incident reports — protecting both the institution and the customers it serves — without relying on costly external forensic specialists.

The Financial Services Cybersecurity Challenge

Financial institutions run vast, interconnected estates: core banking platforms, payment rails, trading systems, customer channels, and data lakes — increasingly integrated with fintech partners and cloud services. Conventional monitoring tools generate alerts, but rarely answer the question investigators, fraud teams, and regulators need most: what actually happened, and which customer accounts and funds were affected?

Ransomware - Encryption of core banking and payment systems halts transactions and threatens financial stability.

Account & Funds Fraud - Account takeover, payment fraud, and unauthorised transfers directly harm customers and the bank.

Customer Data Theft - Personal and financial records are prime targets for theft, extortion, and resale.

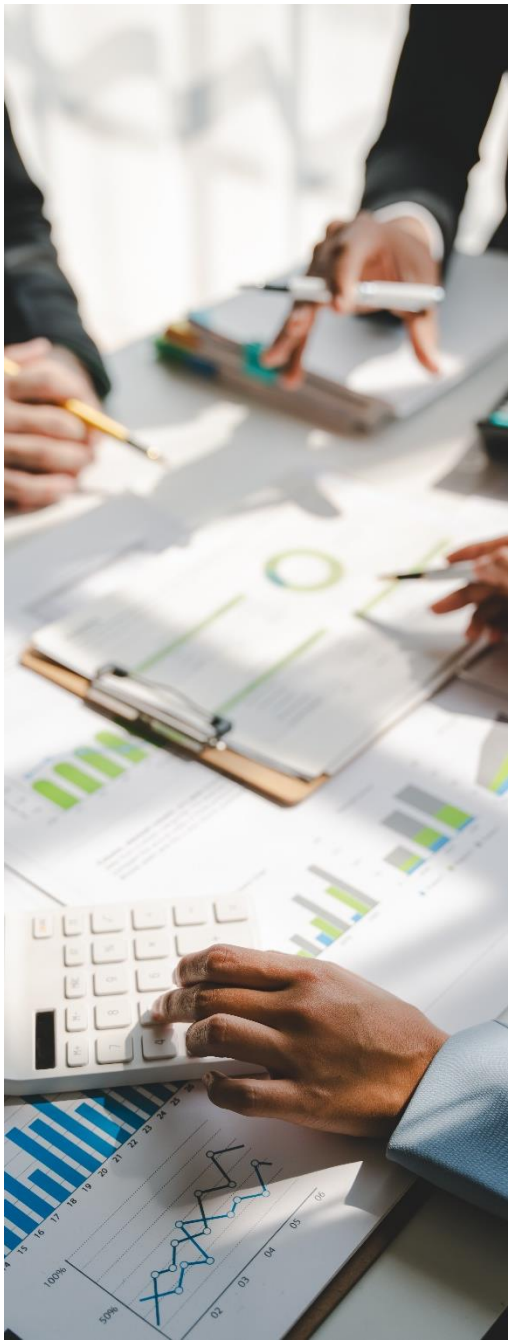
Third-Party Risk - Fintech partners, processors, and MSPs with system access expand the attack surface.

Insider Threats – Traders, operations staff, and contractors with privileged access present theft and tampering risk.

Regulatory Gap – Without forensic evidence, meeting NIS2, DORA, PCI DSS, GDPR, and SOX 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 customer accounts, funds, or records were affected
- Produce an evidence timeline for regulators

Threat Detection

- Ransomware: mass file modification, extension changes, shadow copy deletion
- Insider threat: bulk customer data access outside normal working patterns
- Fraud staging: unauthorised changes to payment or account systems 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 financial 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, PCI DSS, GDPR and SOX

Financial institutions 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 Finance	Key Obligation	Tracknosis Support
NIS2 (EU)	Banking and financial market infrastructure classified as essential entities	Early warning within 24 hrs; full notification within 72 hrs; board accountability	Forensic timeline, evidence preservation, and structured regulatory report within hours
DORA (EU)	Banks, payment institutions, and 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
PCI DSS	Any institution storing, processing, or transmitting cardholder data	Protect cardholder data; detect and respond to breaches; maintain audit trails	Forensic evidence of access to in-scope systems and cardholder data environments
GDPR / GLBA	Institutions processing EU personal data (GDPR) and US customer financial data (GLBA)	Notify authorities within 72 hrs (GDPR); safeguard customer data and notify (GLBA)	Precise identification of affected records, user attribution, and notification content
SOX / SEC	US public financial institutions and listed companies	Internal controls over financial reporting; timely disclosure of material cyber incidents	Tamper-evident audit trail of changes to financial systems and control evidence

Financial Services and Banking Use Cases

Ransomware Response

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

Customer Data Breach

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

Payment & Account Fraud

Detect tampering with payment and account systems; attribute changes to specific accounts and sessions

Insider Threat Investigation

Attribute file and system changes to specific trader, operations, or contractor accounts

Third-Party & Fintech Risk

Detect compromise introduced via fintech partners, processors, and managed service providers

Core Banking Continuity

Identify anomalies and security events affecting core banking and payment platforms before disruption

Regulatory Audit Readiness

Maintain continuous forensic audit trails for NIS2, DORA, PCI DSS, GDPR, and SOX obligations

Post-Incident Analysis

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

Value to CIOs, CISOs, and Chief Risk Officers

For financial institutions balancing growth, customer trust, and 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 core financial 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 core banking, payments, and customer channels.
- Regulatory reporting compliance — forensic evidence packages ready within hours, not days.
- Evidence-based forensic reporting for boards, risk committees, and regulators.
- Enhanced collaboration between security, risk, compliance, fraud, and operations leadership.
- Strengthened customer trust and protection of the institution's brand and reputation.
- Reduced cost and duration of cyber incident investigations and regulatory responses.

Benefits for Customers in Financial Services and Banking

Forensic Observability does not only protect the institution — it directly protects the customers who entrust it with their money and data. When a bank can detect, investigate, and contain incidents in hours rather than weeks, customers experience faster protection, clearer communication, and stronger safeguards for their funds and personal information.

Direct Benefits to the Customer

Funds Protection	Rapid detection of fraud staging and account tampering helps stop unauthorised transfers before loss
Faster Breach Notice	Precise identification of affected records enables prompt, accurate notification so customers can act
Data Privacy	Continuous evidence of who accessed personal and financial data strengthens privacy safeguards
Service Continuity	Faster containment keeps payments, cards, and online banking available with less disruption
Fair Dispute Handling	Tamper-evident forensic timelines support accurate, defensible resolution of fraud disputes
Confidence & Trust	Demonstrable forensic readiness reassures customers their bank can detect and respond to threats

How Customers Experience the Difference

- Quicker fraud detection and intervention — reducing financial loss and recovery time.
- Transparent, evidence-based communication when an incident affects their account.
- Fewer and shorter service outages across cards, payments, and digital banking.
- Stronger protection of personal and financial data against theft and misuse.
- Greater confidence that disputes and claims are resolved fairly and accurately.

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 Financial Services and Banking

Financial 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 and customers demand

Forensic Observability

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

Regulatory Compliance

- NIS2 · DORA · PCI DSS · GDPR · SOX
- Reports generated within hours
- Structured evidence for regulators
- Board and auditor-ready outputs.

Academic Protection

- Funds and fraud protection
- Faster, accurate breach notification
- Customer data privacy safeguards
- Service continuity assurance.

Tracknosis Ltd © 2026 | Making the Unknown Known