

Tracknosis Retail Edition

White Paper

Forensic Observability, Threat Detection and Regulatory Compliance for the Retail and E-Commerce Industry

**Making the
Unknown
Known**



Executive Summary

Retailers and e-commerce businesses process enormous volumes of payment card data, customer accounts, and loyalty information across stores, websites, and supply chains. They are prime targets for payment-skimming malware, ransomware, and organised fraud — where a single breach threatens revenue, regulatory penalties, and the customer trust that underpins the brand. Regulations including PCI DSS, GDPR, NIS2, CCPA, and CIRCIA now require retailers 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 point-of-sale (POS) systems, back-office servers, and e-commerce infrastructure that run the business. It continuously transforms endpoint and server telemetry into trusted forensic evidence, enabling retailers to detect threats early, perform rapid root cause analysis, and produce regulatory-ready incident reports — protecting both the business and its customers — without relying on costly external forensic specialists.

The Retail and E-Commerce Cybersecurity Challenge

Retailers run distributed, high-volume estates: point-of-sale terminals across many sites, e-commerce platforms, payment gateways, warehouses, and customer data lakes — often integrated with payment processors and a long tail of third-party suppliers. Conventional monitoring tools generate alerts, but rarely answer the question investigators and loss-prevention teams need most: what actually happened, and which customer and card records were affected?



Ransomware – Encryption of POS, e-commerce, and logistics systems halts sales and disrupts the supply chain.



Payment Card Theft – POS malware and digital skimming (Magecart) harvest cardholder data at the point of sale and checkout.



Customer Data Theft – Accounts, loyalty data, and personal records are prime targets for theft, extortion, and resale.



Third-Party Risk – Payment processors, suppliers, and MSPs with system access expand the attack surface.



Insider Threats – Store, warehouse, and head-office staff with access present fraud, theft, and tampering risk



Compliance Gap – Without forensic evidence, meeting PCI DSS, GDPR, NIS2, and CCPA 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 POS, back-office, and e-commerce 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 stealthy POS and skimming malware.

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 or card records were affected
- ▶ Produce an evidence timeline for regulators, acquirers, and counsel

Threat Detection

- ▶ Ransomware: mass file modification, extension changes, shadow copy deletion
- ▶ POS malware: new or modified executables on point-of-sale hosts between scans
- ▶ Skimming: unauthorised changes to e-commerce checkout files and scripts
- ▶ 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 retail 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: PCI DSS, GDPR, NIS2, CCPA and CIRCIA

Retailers 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 Retail	Key Obligation	Tracknosis Support
PCI DSS	Any retailer storing, processing, or transmitting cardholder data	Protect cardholder data; detect and respond to breaches; maintain audit trails	Forensic evidence of access to in-scope POS and cardholder data environments
GDPR / UK GDPR	All retailers processing EU/UK customer 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
NIS2 (EU)	Large retailers and digital marketplaces classified as essential or important entities	Early warning within 24 hrs; full notification within 72 hrs; board accountability	Forensic timeline, evidence preservation, and structured regulatory report within hours
CCPA / CPRA (US)	Retailers handling California consumer personal information	Safeguard consumer data; honour consumer rights; respond to and disclose breaches	Forensic identification of affected consumer records and user attribution for disclosures
CIRCIA (US)	Large retailers operating critical or high-impact infrastructure	Report significant incidents to CISA within 72 hrs; ransomware payments within 24 hrs	Tamper-evident artifact preservation, incident documentation, and response records

Retail and E-Commerce Use Cases



Ransomware Response

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



Digital Skimming (Magecart)

Detect unauthorised changes to e-commerce checkout files and scripts before card data is harvested



Insider & Fraud Investigation

Attribute file and system changes to specific store, warehouse, or head-office accounts



Peak-Season Continuity

Identify anomalies affecting POS and e-commerce platforms before disruption during peak trading



POS Malware Detection

Detect new or modified executables on point-of-sale hosts; reconstruct the compromise timeline



Customer Data Breach

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



Supply Chain & Vendor Risk

Detect compromise introduced via processors, suppliers, and managed service providers



Post-Incident Loss Analysis

Identify anomalies affecting POS and e-commerce platforms before disruption during peak trading

Value to CIOs, CISOs, and Loss-Prevention Leaders

For retailers balancing growth, margins, and customer trust, Tracknosis delivers measurable operational assurance. It provides early warning of threats and anomalies, accelerates forensic investigation, supports regulatory reporting, and protects the integrity of payment and e-commerce 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 POS, e-commerce, and supply-chain systems.

- ▶ Regulatory reporting compliance — forensic evidence packages ready within hours, not days.
- ▶ Evidence-based forensic reporting for boards, audit committees, and card acquirers.
- ▶ Enhanced collaboration between IT security, loss prevention, compliance, and operations.
- ▶ Strengthened customer trust and protection of the retail brand and reputation.
- ▶ Reduced cost and duration of cyber incident investigations and regulatory responses.

Benefits for Customers in Retail and E-Commerce

Forensic Observability does not only protect the business — it directly protects the customers who shop in store and online. When a retailer can detect, investigate, and contain incidents in hours rather than weeks, customers experience stronger protection of their payment and personal data, fewer disruptions, and clearer communication when an incident affects them.

Direct Benefits to the Customer

Payment Card Safety	Rapid detection of POS malware and skimming helps stop card data theft before customers are harmed
Data Privacy	Continuous evidence of who accessed personal and account data strengthens privacy safeguards
Faster Breach Notice	Precise identification of affected records enables prompt, accurate notification so customers can act
Shopping Continuity	Faster containment keeps checkout, online ordering, and loyalty services available with less disruption
Account Protection	Early detection of account tampering and fraud staging helps protect customer accounts and loyalty points
Confidence & Trust	Demonstrable forensic readiness reassures customers their data is protected when they shop

How Customers Experience the Difference

- ▶ Stronger protection of payment card and personal data in store and online.
- ▶ Fewer and shorter checkout, website, and loyalty service disruptions.
- ▶ Prompt, transparent communication when an incident affects their data.
- ▶ Quicker detection and intervention against account fraud and misuse.
- ▶ Greater confidence that the retailer can detect and respond to threats.

Deployment and Governance

Tracknosis deploys rapidly across Windows workstations, servers, POS hosts, and Citrix environments with no system reboot required. It integrates with existing IT management tooling and requires no dedicated database infrastructure — suited to distributed, multi-site retail estates.

Supported Platforms	Windows 11; Windows Server 2016–2025; POS 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
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 Retail and E-Commerce

Retailers cannot afford prolonged investigations, regulatory penalties, or the reputational damage of a poorly managed cyber incident — especially during peak trading. 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, card acquirers, and customers demand.

Forensic Observability

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

Regulatory Compliance

- ▶ PCI
DSS · GDPR · NIS2 · CCPA · C
IRCA
- ▶ Reports generated within hours
- ▶ Structured evidence for regulators
- ▶ Board and acquirer-ready outputs

Academic Protection

- ▶ POS malware and skimming detection
- ▶ Payment card and account safety
- ▶ Customer data privacy safeguards
- ▶ Peak-season continuity assurance.

TRACKNOSIS

