TRACKNOSIS

Issue In: 6th July 2026

Tracknosis Government Edition

White Paper

Forensic Observability, Threat Detection and Regulatory Compliance for Government and the Public Sector

Making the Unknown Known

Tracknosis Ltd © 2026

Making the Unknown Known

Executive Summary

Government bodies and public sector organisations operate the digital backbone of national life — tax and benefits systems, citizen identity records, healthcare and welfare services, defence and critical national infrastructure. They are prime targets for nation-state actors, ransomware syndicates, and hacktivists, while remaining accountable to citizens, parliaments, and auditors for the security of the data they hold. At the same time, regulations and mandates including NIS2, CIRCIA, GDPR, the UK Cyber Assessment Framework (CAF), and FISMA / FedRAMP now require public bodies 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 government organisations to detect threats early, perform rapid root cause analysis, and produce regulatory-ready incident reports — without relying on scarce and costly external forensic specialists.

The Government Cybersecurity Challenge

Central and local government, agencies, and arms-length bodies face a uniquely demanding threat environment: legacy systems alongside modern cloud services, complex supply chains, large distributed workforces, and some of the most sensitive data in the nation. Conventional monitoring tools generate alerts — but rarely answer the question investigators and accountable officers need most: what actually happened, and what data was affected?

Nation-State Attacks - Advanced persistent threats target ministries and agencies for espionage, disruption, and data theft.

Ransomware - Attacks on councils, hospitals, and agencies disrupt essential citizen services and emergency response.

Supply Chain Risk - Compromise of contractors and managed service providers grants attackers a route into government networks.

Insider Threats - Civil servants, contractors, and cleared staff with legitimate access present data theft and tampering risk.

Legacy & Sprawl - Ageing systems and fragmented estates create blind spots that signature-based tools fail to cover.

Accountability Gap- Without forensic evidence, meeting NIS2, CIRCIA, GDPR, CAF, and FISMA 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 — including the stealthy, low-and-slow tradecraft characteristic of nation-state intrusions.

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 citizen records or classified data were affected
- Produce an evidence timeline for regulators, auditors, and counsel

Threat Detection

- Ransomware: mass file modification, extension changes, shadow copy deletion
- Insider threat: bulk data access or copying outside normal duty patterns
- Nation-state: new persistence artifacts and lateral movement 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 government 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, CIRCIA, GDPR, CAF and FISMA

Public bodies 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 Government	Key Obligation	Tracknosis Support
NIS2 (EU)	Public administration entities and essential service operators in EU member states	Early warning within 24 hrs; full notification within 72 hrs; senior accountability	Forensic timeline, evidence preservation, and structured regulatory report within hours
CIRCIA (US)	Federal agencies and critical infrastructure operated by government bodies	Report significant incidents to CISA within 72 hrs; ransomware payments within 24 hrs	Tamper-evident artifact preservation, incident documentation, and response records
GDPR / UK GDPR	All public bodies processing citizen 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
UK Cyber Assessment Framework (CAF)	UK central government, NHS, local authorities, and critical national infrastructure	Demonstrate security outcomes for detection, response, and resilience under the NCSC CAF	Continuous forensic monitoring and audit-ready evidence mapped to CAF objectives and outcomes
FISMA / FedRAMP	US federal agencies and the cloud services they consume	Continuous monitoring, incident reporting, and demonstrable security controls (NIST 800-53)	Forensic audit trail, control evidence, and incident records aligned to NIST control families

Government and Public Sector Use Cases

Ransomware Response

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

Citizen Data Breach

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

Nation-State Intrusion

Detect stealthy persistence and lateral movement; reconstruct the espionage timeline for national authorities

Insider Threat Investigation

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

Supply Chain Compromise

Detect tampering introduced via contractors and managed service providers across the estate

Critical Service Continuity

Identify anomalies affecting tax, benefits, healthcare, or emergency systems before citizen-facing disruption

Regulatory Audit Readiness

Detect unauthorised modification of statutory records, case files, or system configurations

Post-Incident Analysis

Reconstruct the complete attack chain; quantify impact for ministers, auditors, and public inquiry purposes

Value to CIOs, CISOs, and Accountable Officers

For government organisations balancing public service delivery with national security obligations, Tracknosis delivers measurable operational assurance. It provides early warning of threats and anomalies, accelerates forensic investigation, supports regulatory and parliamentary reporting, and helps maintain uninterrupted citizen services — 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 scarce external forensic specialists.
- Improved uptime and reliability across citizen-facing digital services.
- Regulatory reporting compliance — forensic evidence packages ready within hours, not days.
- Evidence-based forensic reporting for ministers, audit committees, and public inquiries.
- Enhanced collaboration between security, governance, legal, and operational leadership.
- Strengthened public trust in the stewardship of citizen data and essential services.
- 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 — supporting on-premises, sovereign, and air-gapped government deployments.

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
Data Sovereignty	On-premises, sovereign, and air-gapped deployment; full retention and residency controls
SIEM Integration	Splunk, Elastic, Datadog, Cisco XDR, Microsoft Sentinel — extends existing investments
Access Control	Granular RBAC and immutable audit logs; clearance-aligned segregation of duties

Why Tracknosis for Government

Government organisations cannot afford prolonged investigations, regulatory penalties, or the erosion of public trust that follows 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, auditors, and citizens demand.

Forensic Observability	Regulatory Compliance	Academic Protection
▸ Continuous disk-level evidence ▸ Delta analysis across every endpoint ▸ AI-assisted investigation ▸ Evidence independent of log tampering	▸ NIS2 · CIRCIA · GDPR · CAF · FISMA ▸ Reports generated within hours ▸ Structured evidence for regulators ▸ Minister and audit-ready outputs	▸ Nation-state intrusion detection ▸ Insider threat attribution ▸ Citizen data breach forensics ▸ Critical service protection.

Tracknosis Ltd © 2026 | Making the Unknown Known