ThreatRESPONDER® FORENSICS

KEY CAPABILITIES

- Automated Investigative Analysis
- Attack Story Reconstruction
- Memory + Artifact + Disk Correlation
- Live Systems · Memory Dumps · Disk Images

ThreatResponder® Platform is an award-winning, AI-powered endpoint security platform — independently tested by AV-Comparatives — that detects, stops, and forensically investigates cyber attacks.

ThreatResponder Forensics is the forensics and incident response engine built into ThreatResponder Platform, enabling security, forensics, and IR practitioners to conduct legally defensible DFIR investigations on any Windows endpoint — offline, online, disk image, on-premises, or cloud — at speed and scale. For organizations that need enterprise-grade forensic investigation capabilities without deploying the full platform, ThreatResponder Forensics is also available as a standalone offering.

THE PROBLEM	Too Slow	Too Manual	Too Fragmented	No Storyline	DFIR IS BROKEN. WE FIXED IT.
	Manual triage burns analyst hours	Disconnected tools never scale	Memory, disk & logs siloed	IoCs without attack context	

SOLUTION OVERVIEW

Investigative Synthesis at Machine Speed

NetSecurity built ThreatResponder Forensics to move DFIR from artifact parsing to investigative synthesis. The platform automatically correlates Windows artifacts — event logs, prefetch, registry, MFT, memory, network — into a coherent attack storyline with full timeline context. Analysts stop stitching data across disconnected tools and start getting answers.

KEY BENEFITS

SPEED & EFFICIENCY

- Cuts investigation time from days or weeks to hours
- Eliminates manual artifact stitching across tools
- Single platform: collect, analyze, correlate, report

COMPREHENSIVE COVERAGE

- Parses 60+ Windows artifact types
- Analyzes 20+ Event Log channels simultaneously
- Correlates 25+ Sysmon event types for deep telemetry

POWERFUL DETECTION

- Sigma, YARA & AI/ML engines run in parallel
- Built-in + custom user-defined rules supported
- Catches threats signature-only tools miss

DEEPER INVESTIGATION

- Full attack storyline — not just a list of IoCs
- Auto-correlates memory, disk & live system data
- Visualizes lateral movement & process tree paths

FLEXIBLE SCAN SOURCES

- Live systems, memory dumps & disk images (VMDK, VHD)
- No separate tools needed per evidence type
- Forensic triage package ingestion supported

ALL-IN-ONE TOOLSET

- Memory forensics GUI — no CLI expertise needed
- Built-in Registry, Filesystem & Event Log tools
- PE Analyzer & CLI for automation pipelines

SCAN SOURCES

- Live Windows Systems
- Full Memory Dumps
- Forensic/Disk Images (E01, AD1, VMDK, VHD)
- Forensic Triage Packages/Folders

DETECTION ENGINES

Sigma · YARA · AI / ML

Internal + user-defined custom rules across all three engines.

ARTIFACT COVERAGE

60+ artifact types across 8 evidence categories

20+ Windows Event Log channels

25+ Sysmon event types correlated

IDEAL FOR

- DFIR Leaders & IR Teams
- MSSPs & MDR Providers
- Forensics Investigators
- Threat Intelligence Teams
- Red / Blue Team Operations

One evidence plane for *live, memory, disk & triage* — keyed by process identity, queried in one language

ThreatRESPONDER® FORENSICS

DFIR investigations at speed and scale

CORE CAPABILITIES

Forensics Analysis Engine
Comprehensive artifact scanning with Sigma, YARA & behavioral detection. Automated attack story reconstruction.

Attack Story Reconstruction
Auto-reconstructs attacker TTPs. Visualizes lateral movement and full process-tree timelines.

Event Log Analyzer
Fast visualization across 20+ log channels — Security, PowerShell, WMI, Defender, DNS — with Sigma.

Memory Forensics Tool
Volatility-grade memory analysis in a modern GUI. Works with live RAM or imported memory dumps.

Filesystem & Registry Explorer
Raw NTFS/FAT32 parsing, deleted file recovery, ADS, disk imaging, and offline registry hive analysis.

Collector, PE Analyzer & CLI
Collect all Windows artifacts or full memory dumps. Static PE analysis. CLI for automation pipelines.

ARTIFACT INTELLIGENCE — DEEP WINDOWS COVERAGE ACROSS EVERY EVIDENCE CATEGORY

ThreatResponder Forensics parses and cross-correlates the most comprehensive set of Windows forensic artifacts in a single platform. Across eight evidence categories — file access, process execution, network connections, user events, autoruns, applications, event logs, and Sysmon telemetry — every artifact is normalized and correlated to reconstruct a complete attack timeline. No tool-switching. No manual joins. One platform. One story.

FILE & ACCESS EVIDENCE
- MFT / USN / $LogFile
- System Volume Information
- Deleted Files & Recycle Bin
- ShimCache & AmCache
- ShellBags & LNK Files
- Recent Docs & MUICache
- IE History & Typed Paths
- Prefetch Accessed Files
- Mapped Network Drives
- Browser Downloads

PROCESS EXECUTION
- Running Processes (Live)
- Prefetch Files
- Processes in Event Logs
- SRUM
- Windows BAM
- Run MRU
- App Compatibility Cache
- UserAssist
- Antivirus Detection Logs
- RDP Connections

NETWORK & PERSISTENCE
- Active Network Connections
- Browser History & Cookies
- CertUtil History
- Typed URLs
- ARP Cache & DNS Cache
- WIFI History
- Task Scheduler Folder & Logs
- Run / RunOnce Registry Keys
- Startup Folder
- PowerShell Command History

SYSMON TELEMETRY
- Process Create / Terminate
- Creation Time Change
- Network Connection
- Driver / Image Loaded
- Create Remote Thread
- Registry Create/Delete/Set
- File Created / Deleted Log
- Pipe Event Create / Connect
- WMI Consumer / Filter
- DNS Query

EVENT LOG CHANNELS ANALYZED (20+)

Application · Security · System · PowerShell · TaskScheduler · Windows Defender · Firewall · AppLocker · CodeIntegrity · BITS-Client · RDP (RemoteConnectionManager / LocalSessionManager / RDPClient), Windows Installer, AppX Deployment, WMI-Activity, etc.

THREAT DETECTION STACK

Sigma — CUSTOM OK
Normalized event logs + registry rules. Hits carry process identity and are pivotable into the broader case.

YARA — CUSTOM AT SCAN
Memory, files, PE sections, extracted payloads. Feeds the memory injection pack.

LightGBM PE — SHIPPED
Learned classifier for unsigned PE. Toggle: `enable-pe-ml`. Scoped to PE — not a generic ML detector.

Registry rules — ~100 PATTERNS
Persistence & tamper catalog: Run keys, services, WMI, autoruns, IFEO, AppInit_DLLs, COM hijacks, silent process exits.

One evidence plane.
Live · memory · disk · triage —
one investigation.

ABOUT NETSECURITY CORPORATION

NetSecurity is a leader in endpoint threat protection, vulnerability detection, and computer forensics. Our mission is "*to predict, stop, and investigate advanced cyber attacks and data breaches.*"

12001 Sunrise Valley Drive, Suite 400, Reston, VA 20191
netsecurity.com | (703) 444-9009 | 911@netsecurity.com

netSecurity®