ThreatRESPONDER® FORENSICS

DFIR IS BROKEN.

WE FIXED IT.

AI-powered forensic investigation for any Windows endpoint — live, offline, memory, or disk — at machine speed.

60+
Windows artifact types

20+
Event Log channels

3×
Detection engines

About NetSecurity Corporation

NetSecurity®
Leader in endpoint threat protection, vulnerability detection & computer forensics. Mission: predict, stop, and investigate advanced cyber attacks and data breaches.

About ThreatResponder® Platform

ThreatResponder Platform
Award-winning, AI-powered endpoint security platform — independently tested by AV-Comparatives — that detects, stops & forensically investigates cyber attacks.

This Product

ThreatResponder Forensics
The forensics & IR engine inside ThreatResponder Platform. Also available standalone for enterprise-grade DFIR without full platform deployment.

THE PROBLEM

Too Slow
Manual triage burns analyst hours

Too Manual
Disconnected tools never scale

Too Fragmented
Memory, disk & logs siloed

No Storyline
IoCs without attack context

THE SOLUTION

Investigative Synthesis at Machine Speed

ThreatResponder Forensics automatically correlates Windows artifacts — event logs, prefetch, registry, MFT, memory, network — into a coherent attack storyline with full timeline context. Stop switching between tools. One platform ingests live systems, memory dumps, disk images, and triage packages — linking everything together by process identity.

Full attack picture. One place. Already correlated.

One platform. One story.
From evidence to answer — at machine speed.

SCAN SOURCES

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

KEY BENEFITS

Built for Speed. Built for Depth.

Speed & Efficiency
Cuts investigation time from days or weeks to hours. Single platform: collect, analyze, correlate, report.

Powerful Detection
Sigma, YARA & AI/ML engines run in parallel. Catches threats signature-only tools miss.

Comprehensive Coverage
60+ artifact types across 8 evidence categories. 25+ Sysmon event types correlated.

Full Attack Storyline
Not just IoCs — auto-correlates memory, disk & live data. Visualizes lateral movement & process trees.

All-in-One Toolset
Memory forensics GUI, registry & filesystem explorer, PE analyzer, and a suite of artifact collectors and parsers.

ThreatResponder Platform — multiple AV-Comparatives awards · ThreatResponder Forensics available standalone or within the platform

netSecurity®

Under the Hood — Technical Depth

Detection stack, artifact coverage & evidence categories

ThreatRESPONDER® FORENSICS

DETECTION STACK

Multiple Engines. One Scan.

SIGMA	Normalized event log + registry rules. Hits carry process identity, pivotable into the broader case. Custom rules supported.
YARA	Memory, files, PE sections, extracted payloads. Feeds the memory injection detection pack. Custom rules at scan time.
AI / ML	LightGBM classifier for unsigned PE files. Behavioral detection beyond what signatures can reach.
REGISTRY	~100 persistence & tamper patterns: Run keys, services, WMI, COM hijacks, IFEO, AppInit_DLLs, silent exits.

CORE CAPABILITIES

Powerful Integrated Modules

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.

Memory Forensics Tool

Volatility-grade memory analysis in a modern GUI. Works with live RAM or imported dumps — no CLI needed.

Artifact Collectors and Parsers

Harvest and parse Windows artifacts from live systems, memory dumps, and disk images for forensic analysis.

ARTIFACT INTELLIGENCE

Every Evidence Category. No Tool-Switching.

FILE & ACCESS EVIDENCE

- MFT / USN / $LogFile
- ShellBags & LNK Files
- Prefetch Accessed Files
- ShimCache & AmCache
- Deleted Files & Recycle Bin
- Browser Downloads

PROCESS EXECUTION

- Running Processes (Live)
- SRUM & Windows BAM
- AV Detection Logs
- Prefetch Files
- UserAssist & Run MRU
- RDP Connections

NETWORK & PERSISTENCE

- Active Network Connections
- Task Scheduler Folder
- PowerShell Command History
- ARP Cache & DNS Cache
- Run / RunOnce Registry Keys
- WIFI & CertUtil History

SYSMON TELEMETRY

- Process Create / Terminate
- Registry Create/Delete/Set
- WMI Consumer / Filter
- Network Connection Events
- Create Remote Thread
- DNS Query Events

EVENT LOG CHANNELS ANALYZED (20+)

Application · Security · System · PowerShell · TaskScheduler · Windows Defender · Firewall · AppLocker · CodeIntegrity · BITS-Client · RDP RemoteConnectionMgr · LocalSessionMgr · RDPClient · WMI-Activity

IDEAL FOR: DFIR Leaders & IR Teams | MSSPs & MDR Providers | Forensics Investigators | Threat Intel Teams

ABOUT NETSECURITY CORPORATION

NetSecurity Corporation is a leader in endpoint threat protection, vulnerability detection, and computer forensics.

ABOUT THREATRESPONDER PLATFORM

ThreatResponder Forensics is the forensics & IR engine inside ThreatResponder Platform – an AI-powered endpoint security platform.

See it in action — Request a Live Demo

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

netSecurity®