THOR

Find the traces.
Reveal the compromise.
Zero blind spots.

Your defenses are in place. What got through? THOR examines the system itself, not the alert, for the advanced persistent threats (APTs) and hacking activity that AV and EDR have missed. With forensic precision. In IT and OT.

DETECTION CONTENT INCLUDED

30,000+
handcrafted YARA signatures

4,000+
handcrafted Sigma rules

Thousands of IOCs and anomaly checks included, Sigma applied to the live system state. You get the detection knowledge, not just a rule engine.

Beyond known malware

Files · Processes · Memory · Registry · Event logs · Services · Autoruns · Scheduled tasks · ShimCache / Amcache · Archives

Hack tools
Offensive frameworks, renamed tools and dual-use tooling.

Web shells
Static and obfuscated server-side backdoors.

Obfuscation
Encoded, packed or deliberately distorted content.

Malicious scripts
PowerShell, batch, Python, JavaScript and more.

Attacker artifacts
Exfiltration traces, tool output, dumps and helper files.

Backdoors & anomalies
Suspicious persistence, services, tasks and settings.

Incident response
Know which of thousands of systems are affected, and verify them after remediation.

Continuous assessment
See only what changed since the last scan. Recurring scans, baselined in Analysis Cockpit.

Forensic analysis
Start every image with prioritized leads, not a blank timeline. Today's detections applied to earlier traces.

nextron systems

We detect hackers.

500+ customers · 30+ countries · scanning tools recommended by security agencies

THOR

Choose how THOR runs.

The detection stays. The deployment changes.

A THOR

Portable scans

Run on live systems, manually or via existing tooling. No permanent Nextron agent. HTML or structured reports.

B THOR CLOUD

THOR Cloud

Share a launcher. Scan locally; review results in the cloud. No permanent Nextron agent or on-prem management server.

C MANAGEMENT CENTER

Management Center

Lightweight agents stay installed. THOR runs on demand or on a schedule; evidence collection and response from the same console.

THOR Included detection rules in every workflow. Findings are flagged, never blocked.

Scan your endpoints

Windows · Linux · macOS · AIX

Native support, including AIX.

THOR Legacy
Older operating systems with version-specific support.

THOR Thunderstorm
Collect files from appliances, hypervisors, embedded, ICS and IoT systems. Scan on the service host; coverage follows accessible files.

FILES COLLECTED FROM

vmware · android · IBM · hp UX

Investigate your way

Forensic Lab License
Scan mounted images, files, logs and backups offline. Multi-threaded, intensive scans on forensic-workstation resources. Evidence stays local.

Backup scanning before restore
Scan accessible backup contents via the Veeam integration or mounted backups. Choose a clean restore point, not the attacker's foothold.

Custom IOCs & YARA rules
Add indicators and signatures from threat feeds, investigations and threat reports.

System reliability first
Respect CPU limits, monitor free memory and throttle scans to maintain system stability.

Audit Trail · THOR v11 More data does not mean more alerts. It means more context. Keep the observations behind the findings. See the THOR v11 Tech Preview fact sheet.

See THOR in action.

Trusted by 500+ customers.

Technical demo · Compromise assessment · Strategic conversation

info@nextron-systems.com
nextron-systems.com/thor