exterro®

SOLUTION BRIEF

Exterro ARMOUR *for* FTK

Agentic AI for Remote Investigations

Resolve incidents and investigations faster.

Security tools can detect suspicious activity in seconds. Determining what happened, how far it spread, which systems were affected, and what evidence supports the response can still take hours or days.

Exterro ARMOUR for FTK connects AI reasoning to Exterro's live endpoint reach and proprietary forensic technology. Investigators describe what they need to establish in plain language. AI coordinates the supported workflow. Exterro performs the authorized forensic work. The investigator reviews the evidence and decides what happens next.

The AI coordinates.
Exterro executes.
The investigator decides.

AT A GLANCE

- Investigate available endpoints through natural-language conversation.
- Reach time-sensitive evidence without periodic polling delays.
- Connect approved AI models to Exterro forensic technology.
- Keep investigators in control of scope, evidence, and decisions.

Move Beyond the Alert

EDR and XDR platforms are designed to detect, alert, and contain. But an alert rarely answers what happened, which systems were affected, how far the activity spread, or what evidence supports the response.

Answering those questions often requires analysts to move between tools, construct specialized queries, collect endpoint data, review artifacts, and manually connect the findings. Exterro ARMOUR for FTK reduces the work between the initial alert or investigative question and the evidence needed to act.

From Question to Evidence

1. DEFINE THE OBJECTIVE
Ask the investigative question in plain language.

2. COORDINATE THE INVESTIGATION
The approved AI identifies supported actions and evidence sources.

3. EXECUTE THE WORK
Exterro agents and forensic technology perform the authorized work.

4. VALIDATE THE FINDINGS
The investigator reviews the evidence and determines what conclusions it defensibly supports.

Proof in Practice

HOURS OF ACTIVITY IDENTIFIED IN SECONDS
During a customer evaluation, Exterro identified a five-hour activity window in seconds — work that previously required hours of manual investigation.

5-60 MINUTES
of polling delays eliminated through persistent endpoint connections, removing repeated waits across multi-step investigations.

Results reflect a customer evaluation and representative workflows. Performance may vary by environment, configuration, endpoint availability, data volume, and investigative scope.

Investigate More. Wait Less.

Remote forensic depth, live endpoint reach, and human-controlled AI in one investigation workflow.

Remote Investigation Capabilities

- **Live Endpoint Inspection**
  Processes, users, network connections, ports, services, drivers, scheduled tasks, registry entries, startup activity, operating systems, and installed software
- **File, Memory, and Event Forensics**
  MFT and USN journal queries, targeted file search, system or process memory acquisition, Windows Event Logs, and supported Volatility, Sigma, Chainsaw, and YARA analysis
- **User and Browser Activity**
  Browser history, downloads, recent files, removable media activity, cloud synchronization, archives, and other artifacts relevant to employee and data-movement investigations
- **Targeted Collection and Job Management**
  Collect only the evidence needed to answer the question. Long-running operations continue as tracked background jobs while investigators keep working.

Built for Corporate Investigations

- **Incident Response**
  Establish what happened, assess scope, inspect affected endpoints, and collect time-sensitive evidence.
- **Compromised Endpoint and Malware**
  Examine processes, persistence, memory, logs, files, and network activity.
- **Insider Risk and Employee Matters**
  Investigate file access, removable media, browser behavior, cloud sync, archives, and recent documents.
- **Legal, Compliance, and Regulatory**
  Support targeted investigation, custodian evaluation, preservation planning, and reviewable documentation.

Why Exterro ARMOUR for FTK

AI Connected to Forensic Execution

Generic AI can reason and summarize. Exterro provides endpoint access, investigation infrastructure, and forensic technology to perform the work.

Thirty Years of Forensic Depth

Built on decades of FTK engineering - not a generic AI layer added to a security tool.

Live Endpoint Reach

Persistent connections provide immediate access to supported remote forensic functions without waiting for the next agent check-in.

Model Flexibility Through MCP

Connect supported AI models that align with security, sovereignty, commercial, and governance requirements. The AI never connects directly to endpoint agents.

Evidence-Grounded Results

The AI helps plan, query, organize, and summarize. Findings come from Exterro technology and endpoint data, not unsupported AI conclusions.

Human Control and Accountability

Role-based controls govern access. Authorized actions are documented, and consequential decisions remain with the investigator.

Resolve investigations while the evidence still matters.

Move from alert, suspicion, or business question to evidence-supported findings faster.
Learn more at exterro.com or contact your Exterro representative.

exterro®

ABOUT EXTERRO

Exterro empowers organizations to manage data risks with a complete platform for e-discovery, data privacy, cybersecurity and governance, and digital forensics. Unlike any other software provider, Exterro makes it easy for organizations to understand their data and take swift action. Exterro's AI-driven solutions provide accurate, actionable insights, enabling businesses to ensure compliance, reduce risks, and streamline operations while lowering costs. With Exterro, organizations gain the clarity and confidence needed to address their most critical data challenges. For more information, visit exterro.com.