exterro®

www.exterro.com

A CLOSER LOOK AT THE NEW FEATURES

FTK Enterprise 7.4.2

Work from anywhere. Collect from anywhere.

The way we work has changed. Endpoints are no longer in a physical office. Employees are working from home, and often not connected to the VPN or company network. Data is increasingly being stored in online and cloud collaboration tools like Google Drive™ and Microsoft® Teams. How can you continue to respond to a data breach or perform an internal data collection as these challenges emerge?

FTK Enterprise 7.4.2 is the first forensic investigation tool that can perform off-network endpoint collection and collect from the most popular online and cloud data sources. Access every endpoint, no matter where the user is located.

Off network collections

Collect and analyze data from remote Windows® endpoints that are outside the corporate network with no VPN connectivity by using our Site Server Integration. Deploy the Exterro® remote agent to a Windows® OS endpoint, then configure a Public Site Server to manage collection activity initiated by these remote agents located outside the local network.

Collect data from sources in the cloud

Collect data from cloud data sources and easily review them in FTK Enterprise. FTK Enterprise is the first forensic collection tool in the industry to offer a suite of data connectors, including Network Shares, Microsoft Exchange®, Gmail™, One Drive™, Google Drive™, SharePoint®, and Microsoft Teams.

How does Public Site Server integration work?

1. **Set up an externally facing public site server.** This server connects and "talks to" your company network but sits outside the firewall, similar to a company website versus an intranet. The endpoint data is encrypted and collected into an AD1 file on the site server so you can be assured that it is forensically sound and defensible.
2. **Deploy the Exterro agent on endpoints.** The agent can be pre-installed per company standards or can be deployed covertly and remotely if connected to your network. Once installed, the Exterro agent will continue to communicate with the network whether the endpoint is connected to the network or not.
3. **Create a collection job in FTK Enterprise to collect from the off-network endpoint.** Configure and choose how to collect data and from what remote endpoints. Filter options are also presented in order to further triage and collect selective data.
4. **Perform specific collection.** Once the agent is installed, configured and filtered, the public site server will perform the collection, encrypt the data and collect it in to a forensically sound AD1 file.
5. **Retrieve the AD1 file.** The file can be brought back into the firewall and reviewed and analyzed with FTK Enterprise.

Why FTK Enterprise?

FTK Enterprise is still the reigning industry champion when it comes to digital forensic investigations.

With this release, you can choose from four different types of data collection with a single solution and access every endpoint, no matter *where* that user is located. FTK Enterprise offers:

- **In-network collections**
  Conduct forensically sound, remote, covert investigations and get visibility into all your endpoints, network shares and peripheral devices.
- **Off-network collections**
  Stay in control of your organization's data with the first forensic investigation tool that can perform off-network endpoint collections.
- **Superior Mac® collection**
  Mass deploy remote Mac agents to expand your forensic collection capabilities to endpoints running on a macOS operating system, up to macOS 10.15 (Catalina).
- **Cloud data source collection**
  Collect from cloud data sources for easy review. FTK Enterprise is the first forensic collection tool in the industry to offer a suite of data connectors.

In addition to the superior collection abilities of FTK Enterprise, we also allow you to conduct **live memory analysis** to locate traces of malware, gain insight into potential insider threats, and investigate unknown activity within temporary storage faster than ever before. And, with the AD API, you can **automate incident response** by seamlessly integrating with your cybersecurity platform to kick off a post-breach investigation from the first moments after an intrusion has been detected, initiating the immediate preservation of electronic evidence in an investigation.

Visit us online: www.exterro.com