

Closing the Proof Gap in Investigations

Verifiable, Direct Evidence of Electronic Transactions

The ever-increasing volume of electronic transactions naturally results in an ever-increasing volume of electronic investigations. Just like their hardcopy counterparts, electronic transactions lead to incidents of fraudulent behavior, money laundering, insider breaches, legal discovery, and customer complaints. Because a large enterprise may pursue thousands of high-stakes inquiries each year, the ability to efficiently and effectively complete investigation is critical.

While there are a handful of tools on the market designed to detect suspicious patterns of electronic interaction, enterprise investigators lack the ability to subsequently review reliable evidence. While an automated system or external inquiry may initially raise a red flag, a human being must ultimately make a judgment call regarding the nature of the threat. In order to make an accurate call, an investigator must have access to the most detailed and reliable information possible. Moreover, he also needs a verifiable evidentiary trail to support his decision.

Databases and logs provide only indirect evidence of what happened during an electronic interaction. Both are vulnerable to server errors, data tampering, and human misinterpretation. Not every investigator has the technical acumen to download and correctly interpret a database's complex structure or a logfile's obscure entries. Although forensic network recorders eliminate the problem of server errors, they are still vulnerable to tampering and don't work well for encrypted transactions. None of these existing mechanisms provide any guarantee of authenticity.

What investigators actually require is a forensic datastore of record for electronic transactions. When a detection system or external inquiry flags a transaction, an investigator should be able to immediately retrieve its complete forensic record in an easily comprehensible format. This record must provide indisputable chain-of-custody and authenticity guarantees to support criminal prosecution, civil testimony, or personnel action. Such a solution would dramatically enhance investigator productivity, prove invaluable in bringing perpetrators to justice and help promote public trust in electronic transactions.

The Certified Data Trail™ (CDT) is a hardened network appliance that eliminates the proof gap in electronic investigations. It gives you the **equivalent** of a surveillance camera recording of every electronic interaction and works seamlessly with secure electronic transactions. Investigating a transaction is as easy as logging into a Web-based auditing portal, performing a search, and replaying the result in its original form. Advanced authenticity features mean that the CDT's records can withstand deep legal and technical scrutiny. Stringent confidentiality protections virtually eliminate privacy risk.

Types of Investigation

- Fraud
- Money Laundering
- Insider Breaches
- Legal Discovery
- Complaints

Evidence Problems

- Indirect
- Server Errors
- Altered Data
- No Authenticity
- Time Consuming

Makes Electronic Investigations Easy

The Certified Data Trail (CDT) makes investigating electronic transactions easy. Investigations are about uncovering the truth. That's why the CDT gives you a complete recording of each and every transaction in its original form. There's no guesswork about what might have happened.

Moreover, the CDT delivers this direct evidence much more quickly and affordably than having to painstakingly assemble 'clues' by hand. The CDT's search functionality can immediately retrieve and replay any desired transaction or set of transactions, the replay them on your screen. After a modicum of training, this process takes only a few minutes or even seconds.

But what good is evidence if you can't provide a chain-of-custody? With the CDT, you can prove to law enforcement or a court that the records faithfully represent transactions in their original form. The CDT even tracks auditing activities so you can provide the reasons and results behind every replay. Best of all, you can be up and running with the CDT in a matter of hours!

Works Smoothly with Existing IT Infrastructure and Policies

Clearly, the IT organization plays a critical role in investigating electronic transactions. IT staff deploy, configure, and manage the transaction processing applications in question. Their cooperation is critical to uncovering the truth. For a solution to receive blessing, it must respect infrastructure and policy constraints.

For example, your IT department would resist a new evidentiary solution that requires a painful reorganization of the network topology. Furthermore, they would protest any solution whose requirements to conflict with policies governing encryption key management or private data handling. By design, the CDT integrates seamlessly into typical IT environments. Turnkey recording devices plug into network switches. They have no appreciable impact on network performance, application execution, or user behavior. The Web-based auditing portal runs on standard Java server components. Everything about the CDT is easy to install and manage.

Moreover, the whole solution was designed specifically to work with encrypted network traffic while complying with stringent key management guidelines. The CDT never decodes an encrypted transaction unless specifically requested by an authorized auditor so it's secure against even physical theft.

If you face the challenge of keeping up with investigations of electronic transactions, you need an evidentiary solution that will increase the productivity of your staff and deliver a level of proof that will help law enforcement bring perpetrators to justice. You need the Certified Data Trail. Contact us now at 650-812-7700 or info@networkresonance.com.

Investigator Benefits

- Direct Evidence
- Saves Time
- Chain-of-Custody
- Tracks Replays
- Easy to Learn

IT Benefits

- Quick to Deploy
- Easy to Manage
- Unintrusive
- Works with SSL
- No Privacy Issues