

Closing the Proof Gap in Compliance

A Real Audit Trail for Electronic Transactions

The audit trails associated with electronic transactions are less useful and more vulnerable than their paper counterparts. When a transaction originates on paper, you have either the complete set of the original hardcopies or archives of their scanned images. Access to the originals provides a level of comfort that you have an uncontaminated record of the transaction details. Also, all the originals associated with a single transaction normally reside in a centralized location where a phone call or query results in reasonably fast retrieval. Because the original documents were intended for human consumption, they are relatively easy to decipher.

Contrast these features with those of the most common audit trails for electronically originated transactions: server logs. Each log entry represents a server's response to some data, not the data itself. Usually, no one log entry contains all the information associated with a transaction. Therefore, you must piece together many disjoint entries spanning multiple log files. The result is a subjective summary of the original transaction—one that is subject to interpretation. In addition, because software mechanistically generates the logs, you may require a technical expert to painstakingly 'translate' each log entry into plain English.

So, while it's much more efficient to process electronically originated transactions, you pay the price in dramatically increased auditing effort. The price can be even higher if external auditors, regulators, or courts do not accept your logs as satisfactory records. Just one serious case could have severe consequences.

Of course, it's not just the threat of outside review that's a problem. It's a fundamental question of adequate controls. If you want to verify the correct processing of transactions originated on paper, you can randomly select a group of original documents and trace their processing through the system to make sure they follow prescribed policies. With electronically originated transactions, you must rely on the testimony of your IT professionals to explain how the applications are supposed to work. Moreover, they have to explain why there are not any 'loopholes' that could produce spurious results.

The Certified Data Trail™ (CDT) is a hardened network appliance that eliminates the proof gap between paper and electronic transactions. It gives you the **equivalent** of complete, original documents and work seamlessly with secure electronic transactions. Auditing 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.

Paper Trails

- Complete
- Detailed
- Originals
- Short Retrieval Time
- Easy-to-Understand

Server Logs

- Disjoint
- Summarized
- Interpretations
- Long Retrieval Time
- Hard-to-Understand

Makes Electronic Transaction Auditing Easy

The Certified Data Trail (CDT) enhances auditor effectiveness. Auditing is about finding answers. That's why the CDT gives you the full story. You get to see the entire interaction in its original form. There's no guessing about what may have happened or whether some piece of software made an error.

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, then replay them on your screen. After a modicum of training, this process takes only a few minutes or even seconds.

But what good are answers if you can't prove they're right? With the CDT, you can prove to an external auditor, regulator, or 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 electronic transaction auditing. IT staff deploy, configure, and manage both the processing applications and the auditing infrastructure. You need their cooperation. For a solution to receive their blessing, it must respect infrastructure and policy constraints.

For example, your IT department would not endorse an auditing 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 effective business controls for electronic transactions are important to you, you need an auditing solution that will increase the productivity of your staff and deliver a level of proof that will satisfy the most demanding outside auditors and government regulators. You need the Certified Data Trail. Contact us now at 650-812-7700 or info@networkresonance.com.

Auditing Benefits

- Full Story
- Saves Time
- Defensible Proof
- Tracks Replays
- Easy to Learn

IT Benefits

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