

## The Certified Data Trail™

The Certified Data Trail™ (CDT) is a combination of hardened network appliance and Web portal that provide verifiable proof of electronic transactions. From an investigation perspective, it gives you the equivalent of a surveillance camera recording of every electronic interaction. From an auditing perspective, it gives you the equivalent of complete original documents for every electronic transaction. What makes the CDT different from other approaches is:

- The CDT provides incontrovertible proof of transaction details.
- The CDT works seamlessly with secure transactions.
- The CDT strongly guards the privacy of transaction data.

### Features and Benefits

Feature	Benefit
Passively records packets from SPAN port, mirror port, or network tap.	No effect on network traffic, application execution, or user behavior.
Can record and replay network traffic secured with SSL and TLS.	Don't have to try and work around security to achieve proof.
Signs electronic records with a tamper-resistant hardware security module.	Delivers "notarized" records that are provably authentic.
Signs over encrypted packets for secure network traffic.	Establishes a "chain-of-custody" back to the original transaction parties.
Only saves the ciphertext of secure network traffic.	Minimizes risk of private information disclosure.
Recovers session keys for secure traffic on original transaction servers.	Don't need to pass around copies of all private server keys.
Only recovers session keys for specifically selected transactions.	There is no "collateral damage" to privacy of non-targeted transactions.
Can restrict access to records based on the original application.	Can compartmentalize replay privileges on a "need-to-know" basis
Replays recorded transactions in their original form.	Easy for auditors and investigators to interpret electronic records.
Creates a secure log entry for each transaction replay.	Can audit usage of the replay capabilities to eliminate risk of abuse.

Electronic Evidence  
for Investigations

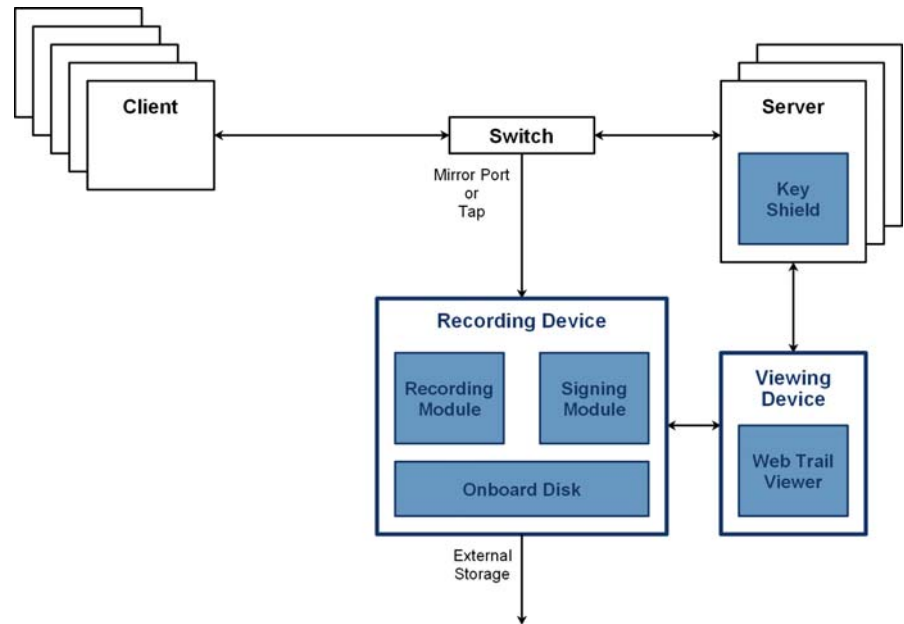
Electronic Proof  
for Auditing

Privacy Protections  
for Everyone

#### Unique Benefits

- Notarizes Records
- Chain-of-Custody
- Guards Privacy
- Shields Key Integrity
- Audits Usage

## Topology



### Components

- Recording Device
- Web Trail Viewer
- Key Shield

### Protocols

- SSLv3/TLS1.0
- HTTP 1.0+
- HTML 4.0+
- SOAP 1.0+

### Performance

- GigE Interfaces
- 300Mbps Sustained
- 600Mbps Burst

## Specifications

Recording Device	Web Trail Viewer	Key Shield
4U 19" Rackmount	Turnkey Appliance or Software Components	Daemon Running on Web and Application Servers
600GB - 1.2TB SCSI Disks	Java Web Interface using Servlets, Struts and Tiles	Windows XP and Windows Server 2003
3 GigE Network Interfaces	ANSI C Protocol Decoding Library on Unix	Linux, FreeBSD, and other Unix
FIPS 140 Level 3 Hardware Secure Module	SSLv3/TLS 1.0 Decryption	Supports PEM Key Files
Fedora Core 5 Linux	HTTP 1.0+ Decoding	Key Translation Toolkit
PostgreSQL 8.1 for Metadata Storage	HTML 4.0+ Replay	
Web and Command Line Configuration Interfaces	SOAP 1.0+ Replay	
SNMP Monitoring	Search Based on TCP/IP and Encryption. Properties	
300Mbps Sustained Recording	Access Restrictions Based on Recording Host-Port	
600Mbps Burst Recording	Built-In Administration	

#### Recording Device

- SPAN, Mirror, Tap
- Copies Packets
- Signs Packets
- Indexes Sessions
- Saves Sessions

#### Web Trail Viewer

- Searches Sessions
- Replays Sessions
- Restricts Access

#### Key Shield

- One on each Web or Application Server
- Uses Server's Private Key
- Recovers Individual Session Keys

## Overview of Execution

In modern networks, routers and switches connect the client and server machines that execute electronic transactions. Most enterprise-class switches provide "SPAN port" and "port mirroring" features where the switch sends copies of network packets to a monitoring device. In cases where these features are unavailable, a "network tap" can add the same packet copying capability as a standalone device. Therefore, an enterprise can be ready to record secure transaction by simply plugging in a CDT Recording Device.

Once an administrator has used the device's management interface to configure which packets it should record, the Recording Module begins saving them to the Onboard Disk. It also sends them to the Signing Module, which uses a tamper resistant hardware security module (HSM) to cryptographically sign them. Combining the original authentication handshake, original channel encryption, and new HSM signature creates unimpeachable evidence of the transaction. The Recording Device also creates an index that maps packets to sessions and permanently archives the sessions to the enterprise's storage network.

Replaying previously recorded traffic requires two additional CDT components. The Web Trail Viewer is a Web application that provides a search and replay interface along with associated administration and access restriction capabilities. Enterprises can deploy the Viewer as either a turnkey appliance or as a software-only component.

The other component required for replay is the Key Shield. Most passive capture approaches that support encrypted traffic require enterprises to make copies of the private encryption keys used by servers and then distribute them to the recording devices or viewing software. Because the secrecy of these keys guarantees that no machine can impersonate a legitimate server, distributing them degrades confidentiality and erodes the trustworthiness of the audit trails themselves—someone could falsely generate records using copies of private keys.

In contrast, the CDT's Key Shield ensures that a server's keys never leave its physical control. It uses this key within the server's trust boundary to recover the session key of each replayed transaction. Moreover, the Key Shield will only reveal this session key to the Signing Module. The Signing module then gives this information to the Viewer, but not before securely logging the replay. This "audit trail of the audit trail" ensures that there's no way to secretly conduct replays.

If defensible proof of electronic transactions is important to your enterprise, you need a solution designed from the ground up to guarantee completeness, authenticity, and privacy. You need the Certified Data Trail. Contact us now at 650-812-7700 or [info@networkresonance.com](mailto:info@networkresonance.com).