

DS 5150

COMPREHENSIVE NETWORK FORENSICS APPLIANCE



SOLERA DS 5150

The DS 5150 provides 10 Gbps capture rates, large onboard storage, and the DeepSee Forensics Suite™.



Easy-to-use browser-based management.



Visualize what data is crossing your network.

» SOLERA DS 5150

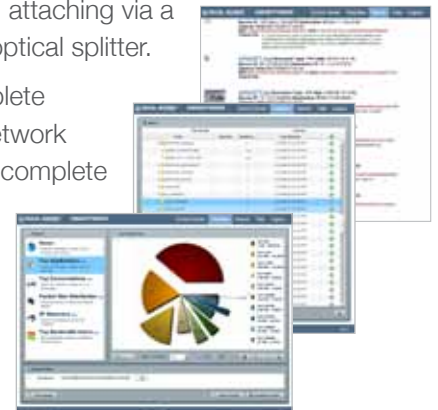
The Solera DS 5150 Network Forensics Appliance is for large enterprise or government agencies that require a complete picture of all network activity, even on the most demanding networks. Active network forensics makes all network data flows instantly visible and replayable, enabling administrators to detect the full source and scope of any network security event and protect the network against further attack. Combining high-speed data capture, indexed storage, and comprehensive analysis tools, active network forensics is analogous to putting a security camera on your network. Doing so instantly exposes any specific network event, making even the most sophisticated and targeted network attacks plainly visible.

NETWORK FORENSICS - DISCOVER THE SOURCE OF ANY NETWORK EVENT

The Solera DS 5150 is a 3U rack-mountable network forensics appliance with capture rates up to 10 Gbps. It has 16 TB of onboard storage and can connect to an external SAN to scale to any need. The Solera DS 5150 includes two 10 Gb capture interfaces to support today's high-speed traffic. Solera DS appliances use patented operating system technologies to ensure lossless traffic capture and storage. They are designed to “plug-and-play” into any Ethernet network, attaching via a mirror (SPAN port), network tap, or optical splitter.

Solera DS Appliances create a complete indexed and searchable record of network traffic (header and payload), provide complete filtering, regeneration and playback, and allow analysis using the included DeepSee Forensics Suite.

Having an exact record of all your data in motion is key to discovering the true source and scope of any event, and protecting your organization from further risk.



View reports, search and discover the source of any network event.

