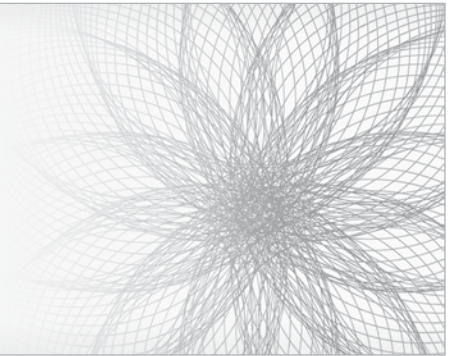


NETWORK FORENSICS



“You can only protect against threats you know, and you can’t know all of them. That’s why you need to be able to respond to breaches swiftly and effectively by doing root cause analysis.

It’s not enough to know that a machine is compromised; it’s vital to know how it was subverted so you can fix the network and prevent a recurrence.”

—John Bedrick, former senior security officer at Seagate, Microsoft, Intel



NETWORK FORENSICS

You can’t stop what you can’t find. That’s why you need network forensics. 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.

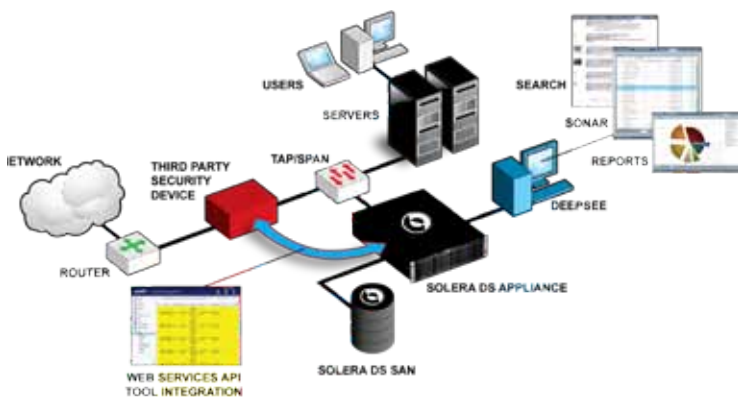
More than 85% of corporate security officers expect a major network security event in the next three years or had one in the past three years*. Half of the same group knows it will take two to 10 or more days to discover the full scope of the incident. Network forensics dramatically reduces the cost of network security incidents to corporations by slashing the time to remediate from days to hours, and eliminates the chance of follow-on attacks.

SOLERA DS™ APPLIANCES AND VIRTUAL APPLIANCE

The Solera DS series is a product line of network forensics appliances that capture and record at full-line rates, even on 10Gb networks. Using groundbreaking technology, Solera Networks’ devices capture, index, filter and regenerate network traffic data at unprecedented rates. Solera DS Appliances store critical data onto scalable, local storage or via storage area network (SAN), giving you a complete and accurate picture of network activity.

The Solera Networks Virtual Appliance is the industry’s first and only network forensics appliance available as a VMware™ image. It includes the same technology available in the DS series, but provides the flexibility to deploy on any hardware platform and has the ability to capture traffic crossing a virtual switch.

EXAMPLE NETWORK FORENSICS DEPLOYMENT



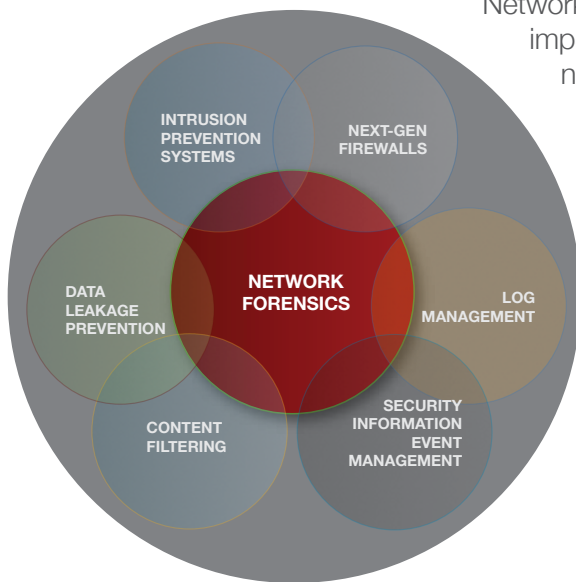
DEEPSEE™ FORENSICS SUITE

The Solera DeepSee Forensics Suite is the key to unlocking captured network traffic to find real answers. The suite of forensics software lets you search through your traffic like you search the web and navigate through it the same way you would navigate through the files on your computer. DeepSee reconstructs network traffic into meaningful flows, including network artifacts like web pages, Microsoft Office™ documents, PDF files, or images. DeepSee returns network artifacts to the user exactly as they appeared on the network at the time of the incident.

SECURITY WORKFLOW INTEGRATION

Solera Networks solutions improve the effectiveness of network security technologies such as Next-Generation Firewalls, IPS, DLP, SIEM and Log Management tools by recording all network traffic at full line rate. Then, through Solera Networks' open data access methods, these tools can access the complete recording of all network traffic, not just a sample, greatly increasing their results and the ability to determine the true scope of any network security event.

NETWORK SECURITY LANDSCAPE



Network forensics fills an important gap in today's network security landscape by capturing all data and providing full context and actionable evidence to stop a security incident.

*2009 Network Forensics Market Survey - Conducted by Trusted Strategies for Solera Networks



QUICKLY IDENTIFY THE COMPLETE SCOPE OF ANY NETWORK EVENT



ID	IP	Port	Action
1	192.168.1.100	80	HTTP GET
2	192.168.1.100	80	HTTP POST
3	192.168.1.100	80	HTTP GET
4	192.168.1.100	80	HTTP POST
5	192.168.1.100	80	HTTP GET
6	192.168.1.100	80	HTTP POST
7	192.168.1.100	80	HTTP GET
8	192.168.1.100	80	HTTP POST
9	192.168.1.100	80	HTTP GET
10	192.168.1.100	80	HTTP POST



© 2009 Solera Networks. All rights reserved. Solera Networks, Solera DS Series, DeepSee, Solera V2P Tap, DS 1150, DS 3150, DS 5150, and See everything. Know everything. are registered trademarks of Solera Networks. All other company names, brand names and product names are the property and/or trademarks of their respective companies.