

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

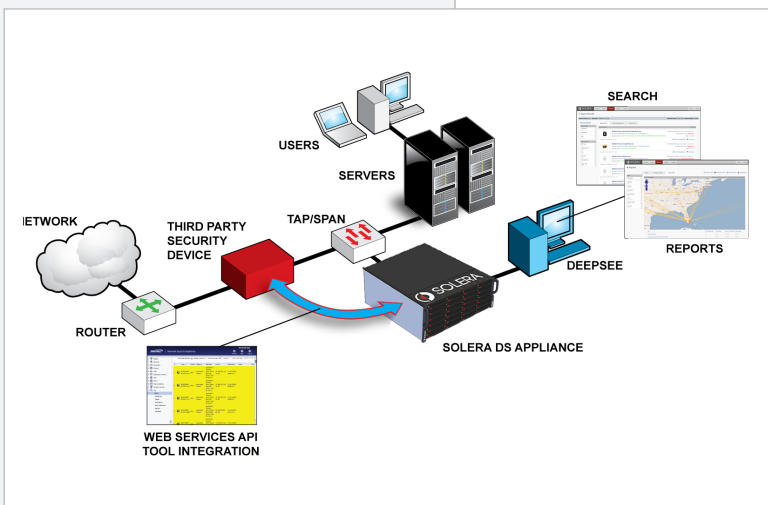
You can’t stop what you can’t detect. That’s why you need active network forensics. Network forensics makes all network data flows instantly visible and replayable, empowering you to detect advanced threats and insider misuse. Combining high-speed data capture, indexed storage, and comprehensive analysis tools, active network forensics is analogous to putting a security camera on your network.

More than 80% of corporate security officers expect a major network security event in the next three years* . A majority (52%) believes they do not have the tools and skills to prevent and respond to the attack. Active network forensics dramatically reduces the cost of network security incidents to organizations 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 line deploys anywhere on your network: at the perimeter or the core; 10 Gb backbones, remote links, or even within virtual hosts, enabling you to record and analyze everything and protect against targeted, persistent threats. DS Appliances integrate capture, indexing, and analysis into a single platform, eliminating the need for complex multi-box solutions.

The Solera DS line of appliances include options to expand storage capacity beyond onboard drives to external direct connect or storage area network devices. 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.



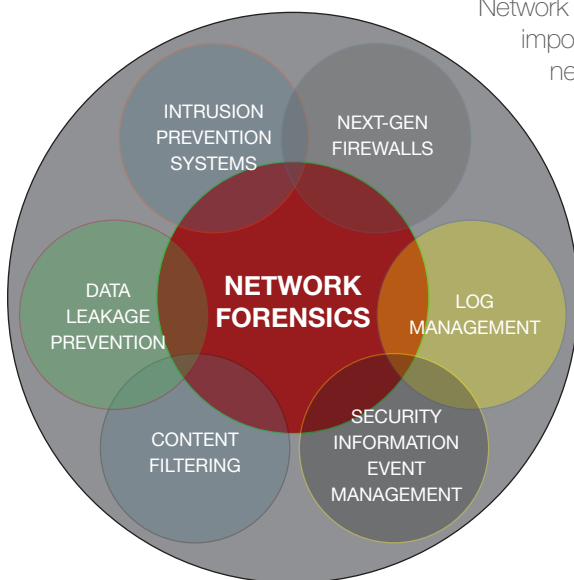
DeepSee™ Forensics Suite

The Solera DeepSee suite of analysis applications 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, IM conversations, images, and more. 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 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.

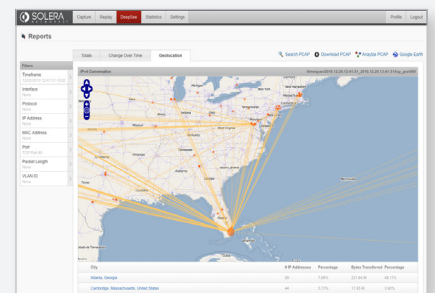
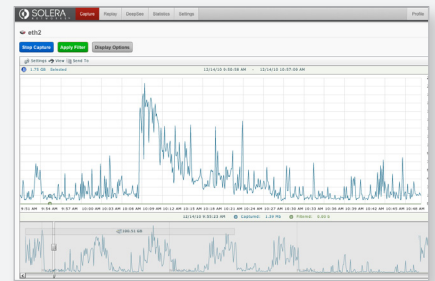
Network Security Landscape



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

*2010 Network Forensics Market Survey – Conducted by Trusted Strategies for Solera Networks

Quickly identify the complete scope of any network event



IP Address	File Name	File Type	File Size	Date
192.168.1.1	Artifact from auto-soft-2.pandora.com	Presented File Type: application/javascript	1024 bytes	11/11/10
192.168.1.1	Artifact from comcast.net	Presented File Type: application/javascript	1024 bytes	11/11/10
192.168.1.1	Artifact from msn.com	Presented File Type: application/javascript	1024 bytes	11/11/10
192.168.1.1	Artifact from 217.147.81.2	Presented File Type: application/javascript	1024 bytes	11/11/10

Hex	ASCII
41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50	A B C D E F G H I J K L M N O P
51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60	Q R S T U V W X Y Z [\] ^ _ `

Contact Us

Contact Solera Networks to give your network a memory. For more information, visit us online at www.soleranetworks.com or call us at 1-877-5SOLERA.

Solera Networks Headquarters
10713 South Jordan Gateway, Suite 100
South Jordan, Utah 84095
1 877-5SOLERA (877-576-5372)
1 801-545-4100 • 1 801-545-4040 fax
Email: info@soleranetworks.com

Solera Networks Japan, Inc.
Shinjuku Park Tower N30F
3-7-1, Nishi-Shinjuku
Shinjuku-ku, Tokyo 163-1030
+1 81-3-5326-3367 • +1 81-3-5326-3001 fax
Email: info@soleranetworks.co.jp



© 2011 Solera Networks. All rights reserved. Solera Networks, Solera DS Appliance, DeepSee, DS 1200, DS 3200, DS 5200, DS H200, DS Storage and See everything. Know everything. are trademarks of Solera Networks. All other company names, brand names and product names are the property and/or trademarks of their respective companies.