



record.



replay.



relax.™

WHITE PAPER

Architectural Overview

Solera Networks' deep packet capture and storage appliances are capable of capturing, streaming, and archiving all traffic on any network up to 10 Gb. Captured traffic is written to a scalable, disk-based cache system and presented as a virtual file system, accessible to any security, forensic, compliance, analytics or network management application. Applications can then perform their analysis on either live or stored data, with the ability to throttle or accelerate traffic speeds and filter playback based on any number of variables, including source/destination, protocol, time period and other criteria.

Solera DS appliances are rack-mountable and scale to support very large storage partitions, up to 576 TB. They sit passively and invisibly on the network and can be attached via a SPAN port or network tap. A carefully tuned and proprietary file system ensures security and chain of custody, while web-based administration, open architecture, and preconfigured hardware or virtual appliance options provide simple plug-and-play deployment.



See everything. Know everything.™

Overview

The Solera Networks DS appliance is a deep packet capture and storage appliance. In simple terms, owning a Solera DS appliance is like having a digital video recorder (DVR) for your network. However, instead of recording just one or two channels at a time, it can record every channel, every program, all the time, and then make it all available for search and analysis, either immediately or at your convenience.

Solera Networks DS appliances can record all of the data in motion on your network—all the time—without losing a single network packet of data. It doesn't matter what type of data you want to capture, because DS appliances can capture packets from the Data Link layer on up (layers 2-7).

Connect a DS appliance to your network via a network tap or switched port analyzer (SPAN), and the DS appliance captures a copy of all network traffic flowing through the tap or port analyzer and saves it to storage. Figure 1 illustrates a sample deployment. The captured traffic is available for playback and analysis within 1 millisecond, giving you near real-time viewing and analysis capability, without the risks of performing the analysis on a live network.

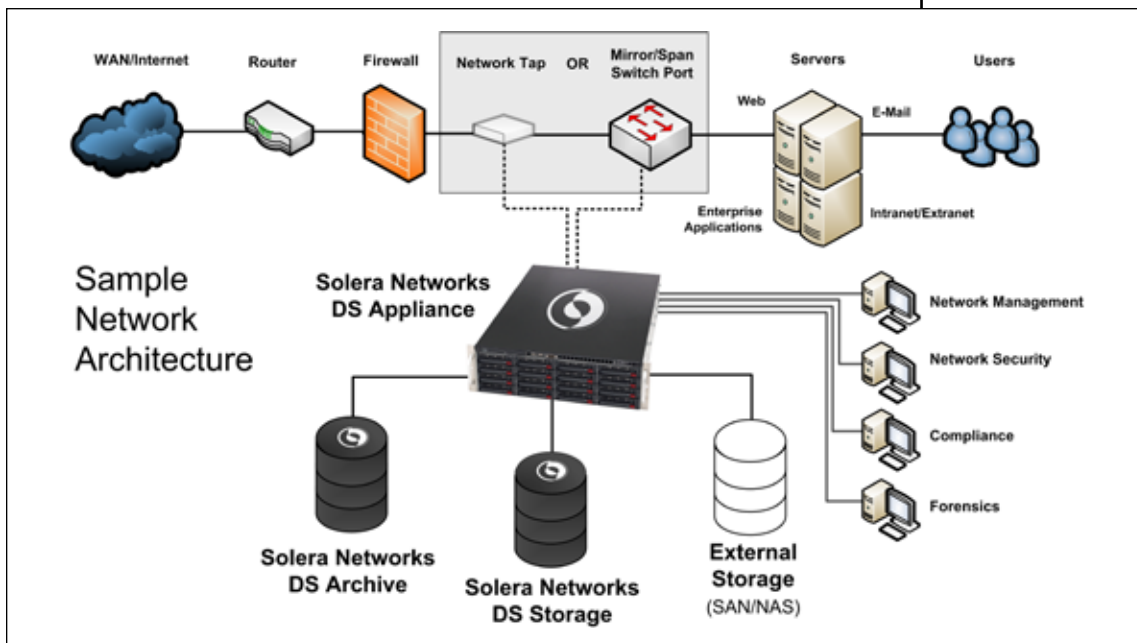


Figure 1

The DS appliance sits passively on the network and does not require a protocol stack (e.g. TCP/IP) on the data capture port. This renders the DS appliance effectively invisible to, and not addressable from, the targeted (captured) network segment. Appliance management occurs through a separate port that is not available on the targeted network segment.

You have complete control over the type of traffic that the DS appliance captures. You can filter network traffic, either during capture or when replaying captured traffic after the fact. Once captured, you can access stored network packets available in three ways:

- Generate Snapshot files, using industry-standard PCAP format
- View captured network traffic flows through Virtual Network Interfaces (VNI)
- Replay captured network traffic flows to a physical Ethernet segment for review by external applications and devices

You can review network traffic at variable speeds, merge multiple network data streams, or replay the same data stream to multiple applications and locations. Through these flexible delivery options, a DS appliance allows existing network monitoring, data analysis and forensic applications to view a comprehensive record of network traffic (including payload contents), rather than a mere sampling of packets, or a review of packet headers only.

With the capabilities of a DS appliance, you can analyze captured network traffic using any protocol analyzer, forensic tool or network management solution that you choose, with zero integration effort.

Solera DeepSee™ lets IT or business professionals locate and reconstruct specific communication flows or network activities from within a complete historical record of all network traffic that crosses their organization. Unlike complex analysis and forensic tools that require extensive knowledge of networking protocols and packet analysis methods, Solera DeepSee provides browser-like simplicity so anyone can search, locate and view actual network communications in the way they were originally delivered, eliminating the need for IT intervention.

To understand how Solera Networks devices contribute to effective packet analysis and network management, it's important to understand the component technologies that are part of every DS appliance. Therefore, the remainder of this document is organized into the following sections:

- Software Architecture
- Hardware Platform
- Packet Filtering
- Analysis
- DeepSee
- Virtual Appliance

Software Architecture

The software subsystems of the DS appliance are specialized and optimized specifically for the rigors and mission-critical nature of network traffic capture and storage. At its most basic level, a DS appliance consists of software, which reads data to memory, then streams that data to storage in a proprietary format, which permits extremely high speed and accuracy, as well as very flexible methods to access the captured data. Because the Solera Networks solutions are software-based and require no proprietary hardware, there is extensive flexibility in both portability and integration with existing infrastructure and toolkits.

Solera Networks' file system is powerful and flexible enough to handle networks at today's highest speeds (up to 10Gb as verified by Miercom), and for addressing very large storage partitions (up to 576 TBs). As those speeds increase and

"We verified that the DS 5100 was capable of capturing data at a faster rate than any other product we have seen in our lab.."

- Miercom Report



storage capabilities expand in the future, the Solera Networks solution can scale to take advantage of those improvements. As an additional security measure, once data is written to disk, it is kept in a proprietary format, preventing any unauthorized changes to the data and ensuring chain of custody. Furthermore, once stored on disk, the DS appliance restricts data access to only authorized applications, processes or agents.

The core of the Solera DS operating system is the DS File System (DSFS), a collection of loadable modules on a carefully tuned Linux kernel. These loadable modules implement proprietary disk management, a virtual file system (VFS), virtual network interfaces (Ethernet), and services for regenerating packets to external network segments, among other things.

The DS appliance architecture is superior to, and much more flexible than, more traditional “sniffer” and “network trigger” models that require users and network investigators to create elaborate event monitors to look for specific anomalies on a network. Since the DS appliance allows you to capture all network traffic, you get a complete network traffic picture, and analysis is done by searching, reviewing, reconstructing and dissecting the historical traffic record. The DS appliance provides an unparalleled view of live network traffic and flow dynamics at manageable speeds that IDS systems or other tools can handle.

The DS appliance software includes the following major subsystems:

- DS File System
- Virtual Network Interface
- Traffic Regeneration

DS File System

The DSFS includes a proprietary, high-performance file system, optimized for packet capture and sequential disk writes, and a virtual file system (VFS) to expose captured traffic. It can address volumes up to 576 TB, so maximum total storage capacity is limited only by the amount of external storage available.

DSFS utilizes an innovative storage architecture to manage limited memory disk resources. This also reduces CPU overhead when transferring packets to memory. When a disk approaches capacity, DSFS reallocates storage space to receive new packets, thus maintaining a scale or continuous time window of captured packets for playback and analysis. External storage can be added to increase the size of the sliding window.

The VFS provides access to packets captured and stored in the DSFS. The VFS offers the following features and benefits:

- Registers as a device-based file system and mounts as a standard Linux file system.
- Adds a PCAP header dynamically to each packet requested through the VFS, so any application that supports PCAP files (e.g. LIBPCAP or Tcpcap) can easily access or import captured packets. This also makes it easy for an analyst to export captured packets to a local workstation for analysis.

- Exposes captured network traffic so you can easily write to external devices (tapes, CDs, DVDs) for long-term storage.
- Exposes DSFS for remote access via NFS, Samba*, Intermezzo*, or any other remote file system access methods supported by Linux.
- Operates as a read-only file system from the user space, but supports the Linux *chmod* and *chown* commands to assign specific file permissions to system users. This allows the DS appliance administrator to provide access to the DSFS file system on an individual basis.
- Restricts data writes and modification to the DS appliance's capture engine subsystem. DSFS prohibits alteration of the captured data by any user, including the system administrator. This ensures the integrity of the captured data and maintains a valid chain of custody should the captured data be used in criminal or legal proceedings.
- Flexible enough to work in any customer networking environment.

Total retention time for captured network traffic is a function of traffic volume and total disk capacity. An environment with high traffic volume and a low capacity DS appliance might begin to overwrite captured traffic in a matter of minutes, while a high capacity appliance can extend storage capacity to many months. Permanent storage options are also available.

Appliance configurations are available with 3 - 16TB of onboard storage. In addition to using a single appliance, you can extend network traffic capture using Solera DS Storage appliances to achieve virtually unlimited archives of network traffic. DS appliances integrate with multiple options for long-term storage of network traffic on a SAN.

Virtual Network Interface (Ethernet)

DS appliances offer a series of Virtual Network Interfaces (VNI) that you can map onto the DSFS. To the operating system, and any applications, the VNI appear as physical network devices, but instead of reading live network packets, applications read captured network traffic from the DS appliance.

This architecture allows you to configure, or shape, custom data streams for the particular application receiving the data by specifying the packet characteristics in which you are interested. Furthermore, you can configure multiple VNI's using the same, or different, data characteristics and have multiple applications analyzing the same data stream in different ways at the same time. This is a significant advantage over using an application to access a physical Ethernet device which, when opened by the application, is inaccessible to other applications. Using a VNI doesn't prevent other applications from accessing the same captured network traffic on the DS appliance.

The DS appliance provides three different types of VNI's to fit the needs of the application and the type of data you want to analyze:

- Replay a captured network traffic stream at the full data rate supported by the DS appliance.
- Replay a captured network traffic stream at the same rate at which it was captured so you can properly analyze or reconstruct timing-sensitive data.

- Replay multiple captured network traffic streams in a single merged output.

Effectively, the DS appliance provides a large network buffer that multiple applications (e.g. firewall, IDS/IPS, or DPI platforms) can leverage to analyze network traffic in near real-time without the potential data loss or performance impact on a congested network. Applications can provide alerts and near-real time (within a millisecond) network analysis because the DS appliance buffers and shapes the traffic the application receives so it can do its job effectively. Over 24 hours, all tools see all the traffic, instead of dropping packets at peak load periods.

Traffic Regeneration

Traffic regeneration allows you to playback network traffic on a physical network segment by regenerating the traffic through an Ethernet port on the DS appliance. External applications and devices that receive these packets from the DS appliance are completely unaware of the fact that they are regenerated. Since the DS appliance captures packets in a lossless manner, the regenerated packets exist as live traffic on their network segment to which they are regenerated. Thus, integration with existing tools is seamless and straightforward.

Traffic regeneration relies on the DS appliance's VNI infrastructure to access captured network traffic. To regenerate a given network data stream, you must first map a VNI to the desired data stream, and then map the VNI to the DS appliance's appropriate physical Ethernet port.

The DS appliance can regenerate captured network traffic, at full-line rate, within a millisecond of capture. This is particularly useful for analyzing data with an application that cannot keep up with network traffic delivered at full line rate. Traffic regeneration allows you to use the DS appliance as a virtual switch; deploying multiple

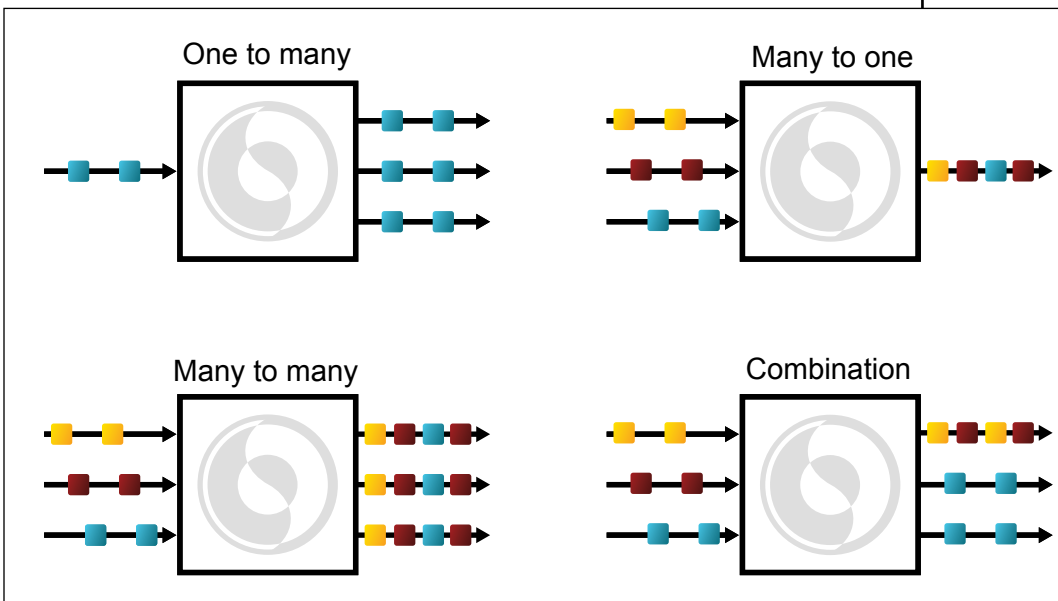


Figure 2

instances of the same tool and delivering segmented portions of the network traffic at a speed the tool can adequately handle. Examples of regeneration are represented in Figure 2.

Alternatively, you can buffer network traffic for a single instance of the application, which allows it to “catch up” during times of off-peak network traffic. For example, an IDS can’t handle intraday traffic spikes, but over 24 hours, sees all the data. Utilizing the Solera Networks appliance, network inspection and forensics tools are no longer a bottleneck for a secure network, optimal performance, or compliance with corporate or government regulations. Figure 3 represents buffering of network traffic to accommodate the limited speed of analysis tools.

Hardware Platform

The Solera Networks software architecture is so efficient that it is fully capable of

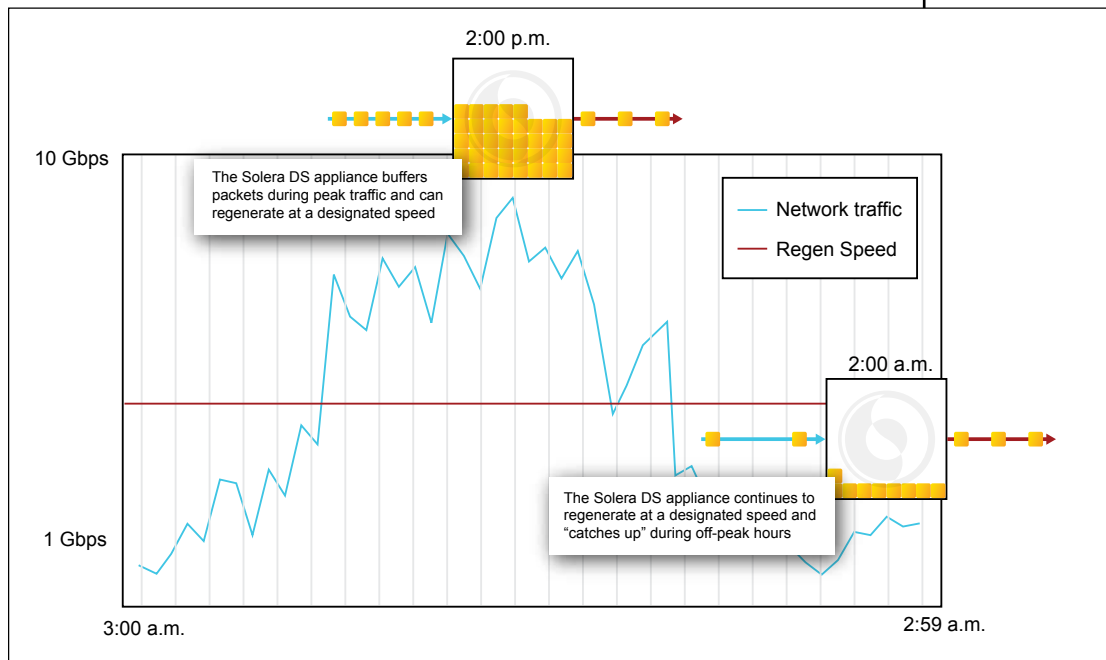


Figure 3

satürating even today’s most advanced data buses. The specialized architecture also eliminates the CPU as a potential bottleneck. It is important to recognize that overall performance is hardware constrained and not software constrained, and performance will continue to improve as hardware architectures evolve.

Without the bottleneck of the CPU and software, “speed to disk” (how fast you can get captured network traffic onto disk storage) is critical to the overall performance of the DS appliance. In support of this, Solera Networks carefully selects and optimizes hardware components for its rack-mountable 1U or 3U (depending on storage capacity) appliances.

The DS product line offers multiple network capture options that let you capture both copper and fiber Ethernet data streams on the same device. For example, you can configure the DS 3150 appliance with interface options including, 4 Gigabit copper 10/100/1000 interfaces and 4 1000 Base SX fiber interfaces or either 8 copper or 8 fiber interfaces.

These extreme traffic capture rates also demand rigorous disk performance. Solera DS appliances include SATA hot-swappable drives (7,200 RPM) in RAID 0/RAID 5 configurations from 1.5 TB up to 576 TB. Moreover, the DS appliance's operating system boots and runs independently of the disk drives used for traffic capture storage. Additional configurations are represented in Figure 4.

Packet Filtering

TECHNICAL SPECIFICATIONS						
	Size	Capture Rate	Storage Capacity	Standard Configuration	System Memory	External Storage Upgrade
Calea Appliance	1U	1.5 Gbps	1.5 TB	(1) 2-port copper GigE 10/100/1000	2 GB	No
DS 1150	3U	2.0 Gbps	3 TB	(1) 4-port copper GigE 10/100/1000 or (1) 4-port 1GB Fiber Card (optional)	8 GB	No
DS 3150	3U	5.0 Gbps	12 TB	(2) 4-port copper GigE 10/100/1000 or (2) 4-port 1GB Fiber Card (optional)	16 GB	Yes
DS 5150	3U	10 Gbps	16 TB	(1) 2-port 10GB Fiber Card and (1) 4-port copper GigE 10/100/1000 or (1) 4-port 1Gb Fibre Card	16 GB	Yes
DS Storage	4U	—	24 TB	Fibre Channel	—	—

Figure 4

To more efficiently analyze and review network traffic, you may want to specify the characteristics of the packets you want to capture. The DS appliance supports a robust filtering language and applies filters to captured network packets individually, one packet at a time. It sequentially evaluates each packet against the defined filter statements, one statement at a time. If the packet matches all policy statements, the packet is accepted. If the packet fails to match any filter statement, it is rejected.

The DS appliance allows you to filter captured network traffic in two ways:

INGRESS FILTERS: Restricts packets stored to the appliance based on your filter configuration. The DS appliance applies Ingress filters in memory, not at the point of capture. This means that the DS appliance still captures every packet on the network, but if a captured packet does not fit the Ingress filter, the DS appliance simply overwrites it with the next captured packet.

EGRESS FILTERS: Restricts packets retrieved from the appliance based on your filter configuration. You can apply Egress filters to both Snapshot file output and traffic replay to restrict the output to a subset of the packets stored in DSFS.

Both Ingress and Egress filters can include or exclude packets based on protocol type, MAC address, IP address, payload contents, a text string, or any other bit of information in the packet header or payload. Simple filtering is illustrated in Figure 5.

The Solera DS appliance's user interface and filter wizard allows you to quickly create specific filters to capture the desired traffic. This is all completed within the software framework, enabling complete and ongoing flexibility, providing the speed

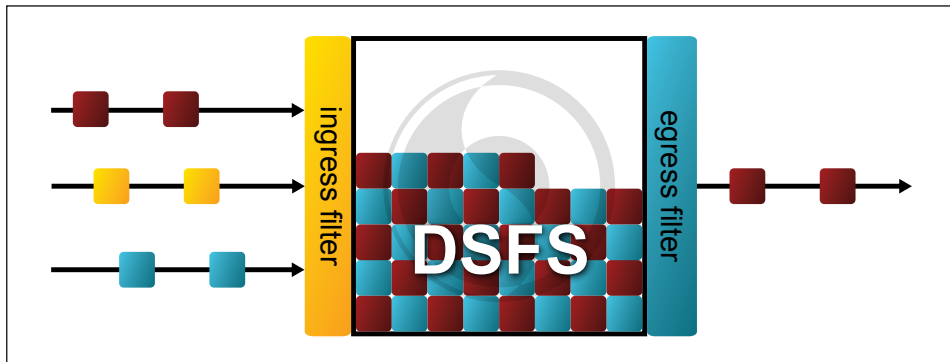


Figure 5

of hardware-based filtering without the complexity of hardware lock-in or fixed ASIC technology.

Once a network traffic stream is captured on the DS appliance, it is available almost immediately (within a millisecond) for replay without impacting network speed or interrupting network traffic. To do this, the DS appliance reloads the captured network traffic stream into another memory slot that you can review without impacting ongoing recording of the same network traffic stream. This capability delivers virtually instantaneous data availability for analysis or forensics with zero impact on the production network.

Analysis

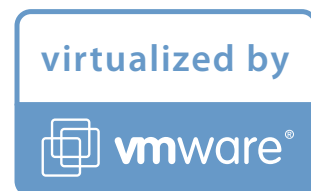
Any of the preceding data presentation methods can be consumed for analysis, data analytics, network security, forensics and network management using industry standard formats by commercial, custom or open source applications. The Solera Networks appliance exposes virtual interfaces, which seamlessly make the captured packets available to thousands of applications. Because you can access captured data via Snapshot files (using industry standard PCAP file format), it is accessible to any application using libpcap or WinPcap. APIs are also available based on REST (Representational State Transfer) and SOAP (Simple Object Access Protocol) for integration with third-party applications.

Solera Networks' proprietary file system makes the same captured data available to multiple applications (analysis, forensics, etc.) concurrently. Any number of read-only instances of a data set can be opened simultaneously without interrupting the real-time capture function. There is no need to stop capture in order to analyze data. Not only can a single time period be opened simultaneously for analysis, but overlapping time windows can also be concurrently inspected, all without interrupting the capture of live data on the network.

For a more extensive list of analysis tools with links to download sites, visit: www.soleranetworks.com/solutions/apps

DeepSee

Solera DeepSee™, available with Solera DS appliances, is the first and only solution that allows any authorized professional complete visibility into all network

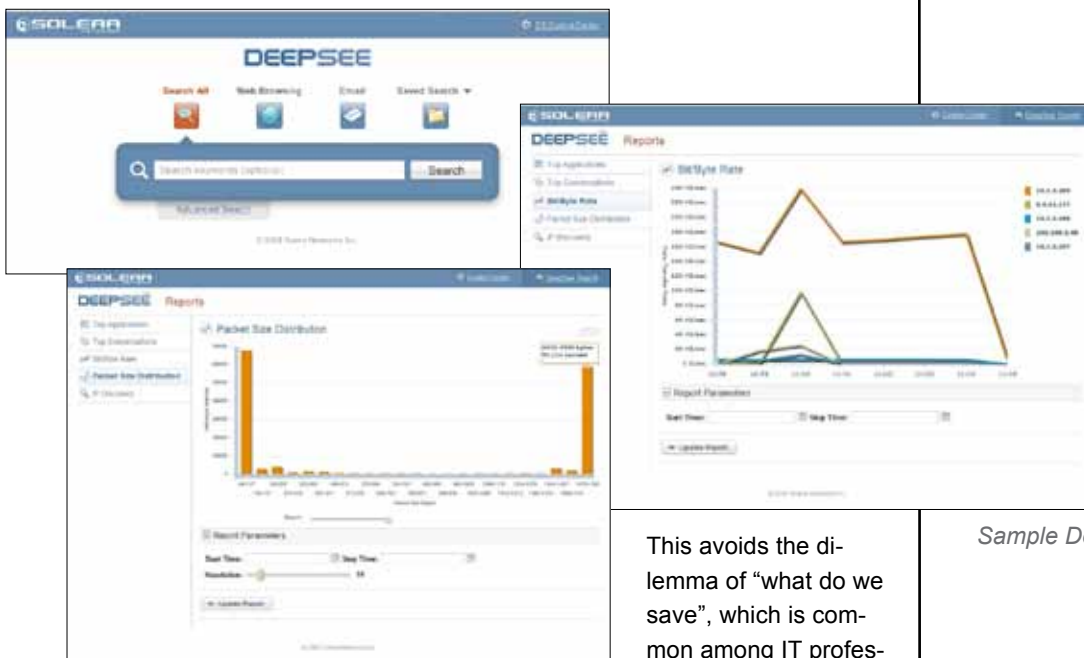


traffic, whether the traffic is an email, an IM, a browser session, an FTP session, or a communication, which contains an Excel spreadsheet or a Word document as an attachment.

Solera DeepSee lets IT and business professionals locate and reconstruct specific communication flows or network activities from within a complete historical record of all of their network's traffic. Unlike complex analysis and forensic tools that require extensive knowledge of networking protocols and packet analysis methods, Solera DeepSee provides web search-like simplicity so anyone can search, locate and view actual network communications in the way they were originally delivered.

Solera DeepSee indexes the complete historical record of network traffic, which is captured and stored by Solera DS appliances. It then identifies network flows that are meaningful conversations between users for examination by both IT and business users. DeepSee indexes based on any identified "artifact" – an email thread, word document, IM dialogue, browser session, VPN session, etc. – enabling guided search for both IT professionals and business users, delivering meaningful, intuitive results in the format of the original communication.

With the ever-increasing volume and complexity of data crossing networks, and the worldwide push toward increased data retention regulations, the capture and storage of all network traffic is swiftly becoming a best practice for all enterprises.



Sample DeepSee Screenshots

This avoids the dilemma of "what do we save", which is common among IT professionals. Instead, the

combination of Solera Networks' DS Appliance and DeepSee search engine eliminate the headache by making it easy to "save it all", knowing network information is readily available for any security, management, or compliance event.

Simple Deployment

An administrator versed in TCP/IP can install and deploy a Solera DS appliance and integrate it with existing monitoring, analysis and forensic tools in a matter of minutes. Solera DS appliances simply connect to a network via copper or SR fiber cables using either a switched port analyzer (SPAN) or a network tap. Using SPAN, the port is set to mirror (copy) packets from other selected ports of the router or switch to the SPAN configured port on the host router. With a tap or optical splitter, transmit (TX) and receive (RX) traffic feeds to the Ethernet adapters and flows through the device where data can be filtered or stored before retransmitting.

The implementation steps for preconfigured Solera DS appliances are:

1. Configuring the SPAN or tap
2. Powering up the device
3. Specifying the desired capture parameters

The DS appliance provides both a robust browser-based Web Console and a Command Line Interface that lets you configure capture and playback settings. Using one of these interfaces, you are able to:

- Select, start, and stop capture, replay and regeneration processes
- Create, edit, and load ingress and egress filters for captured packets
- Configure access to captured network traffic streams through both Snapshot files and traffic regeneration
- Configure a lawful intercept and forward data to a Law Enforcement Agency (LEA) collector
- Perform system configuration and management
- Issue console commands to the DS appliance
- Add and manage users and user access rights to the DS appliance
- View key system metrics and statistics in graphical or numeric form

Virtual Appliance

For those who want to implement a Solera Networks deep packet capture and storage appliance using existing hardware, Solera Networks offers the Solera Networks Virtual Appliance. The virtual appliance delivers the same architecture, functionality and performance of the DS appliance in a software-only solution. By installing the virtual appliance, you can convert any server into a network packet capture and storage appliance.

Solera Networks delivers the virtual appliance as a VMware® image that you can deploy on any hardware/operating system platform that supports VMware. This less expensive deployment option is ideal for remote offices or small businesses that don't need the additional performance and data storage options available in an optimized hardware appliance.

Figure 6 lists many of the popular open source analysis tools that can be used with a Solera Networks DS Appliance. For more information about the Solera Networks virtual appliance, see www.soleranetworks.com/products/virtual-appliance.php.

Summary

TOOL	DESCRIPTION
Wireshark/Ethereal	Network protocol analyzer
Snort	Network intrusion prevention and detection system
Tcpdump	Packet header capture
Tcptrace	TCP dumpfile analyzer
Tcpreplay	Tool suite for traffic replay
NeTraMet	Network traffic flow accounting meter
Fprobe	Collects traffic and emits as NetFlow (Cisco) stream
Ntop	Network traffic monitoring tool
Bro	Network intrusion detection system
Efftech	Mail, IM and HTTP monitoring
Etherboss	Conversation monitor and sniffer
HttpWatch	HTTP viewer and debugger
Nagios	Monitors for system and network outages
EtherPeek	Family of Ethernet network analyzers
CommView	Network monitor and analyzer
Nessus	Vulnerability scanner
Ettercap	Terminal-based network sniffer/interceptor/logger for Ethernet LANs

Figure 6

Having a comprehensive view of network traffic is critical for ensuring a more secure, effective and compliant network environment. The only way to do this is to have a complete record of all data in motion on a network. Solera Networks' deep packet capture and stream-to-storage appliances provide a complete packet capture solution with the flexibility today's organizations demand. The appliances are capable of capturing, recording and archiving 100% of the packets crossing a network at full-line rates, including fully saturated 10 Gb networks, with speed and accuracy unmatched by any other solution.

Captured data is available almost instantaneously for analysis using any application you choose, without affecting the integrity of the underlying data or the performance of the network. Additionally, you can shape the traffic, through filters and playback throttling, to permit complete analysis of all traffic crossing the network.

For more information about Solera Networks deep packet capture and stream-to-storage solutions, visit www.soleranetworks.com.

Contact

For more information on how you can use Solera Networks solutions for network security, network management, analytics or compliance, please visit our website at: www.soleranetworks.com or call us at 1 877-5SOLERA (877-576-5372) or 801-545-4100.

© 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.

Solera Networks Headquarters
 10713 S 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



See everything. Know everything.™