

SonicWALL and Solera Networks Solution Brief

NETWORK SECURITY

Finding the Root Cause of Any Alert – Fast

A awareness of a network vulnerability often comes by a system monitoring alert, log file review or vendor press release. As a security administrator, your job is to quickly decide if it poses a real threat to your network, how to remedy that threat, and the priority for action. Your operational challenge is linking an alarm to actual network activity by specific users. The lack of specific data often forces security professionals to guess at the degree of exposure, or whether a breach actually occurred. Without sufficient network forensics data, your ability to identify the scope of a security event or verify compliance with security policy is ineffective.

A new appliance-based network forensics solution from SonicWALL® and Solera Networks™ allows you to quickly and precisely evaluate every alert, and know with confidence if and how an associated vulnerability was exploited on your network prior to detection or public announcement.

SonicWALL/Solera Networks Solution Components

This joint solution fulfills three requirements for security: (1) having the ability to perform deep packet inspection in real time without significantly impairing network throughput; (2) to record and store all network packet header and payload data; and (3) perform network forensic analysis in near real-time, linking any alert to its actual data on demand. SonicWALL and Solera Networks meet these requirements and provide integrated alert and forensic capabilities. With the components listed below, users can immediately deploy and tap the high-performance alerting and forensics features enabled by the joint solution.

Summary

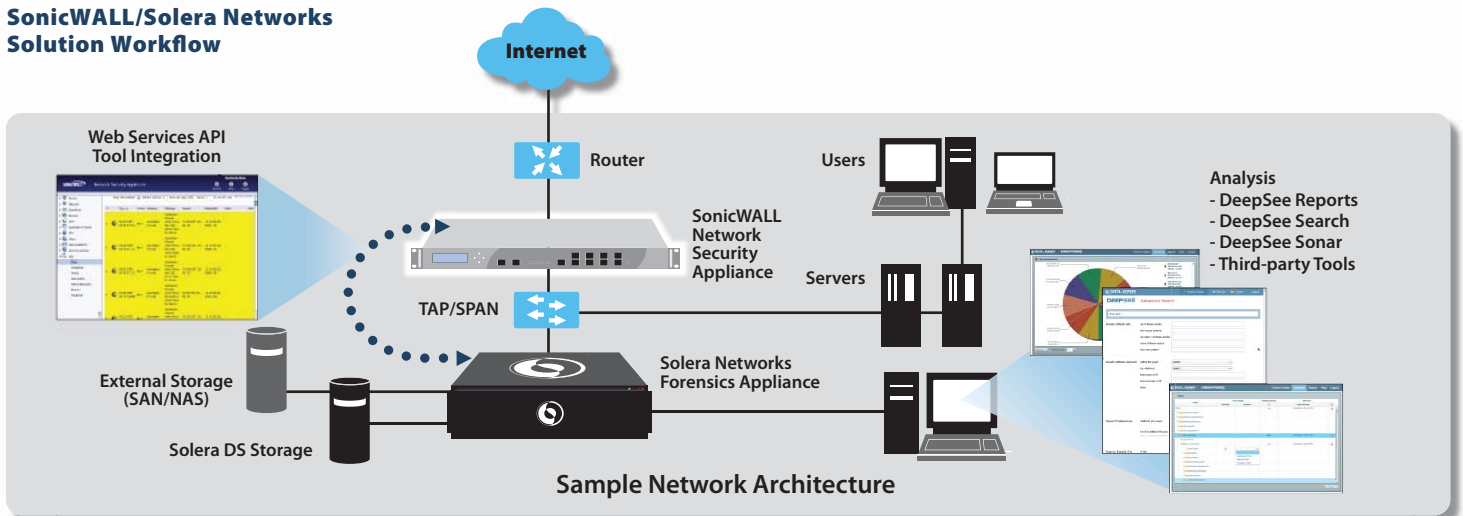
What: SonicWALL Deep Packet Inspection technology adds anomaly and attack discovery capabilities to the Solera Networks full packet capture, storage and analysis solution.

For: Instant total forensic insight on any event or anomaly occurring in your network.

SonicWALL	Solera Networks
Unified Threat Management appliance (E-Class NSA and NSA Series) engineered to support high-bandwidth enterprise networks, providing flexible controls for intrusion prevention, anti-virus, anti-spyware, application firewall and content filtering.	Network forensics appliance (Solera DS™ 1150, 3150, 5150) for passive capture of all traffic (header and payload) to disk at up to 10Gbps with no network overhead. It works like a security camera for your network, recording everything and finding anything – fast.
Multi-core Processing capability in SonicWALL UTM appliances exceeds the security and performance of traditional solutions by almost 3:1, while eliminating bottleneck and latencies introduced by security co-processing. It is essential for real-time scanning of headers and payloads of every packet in high-bandwidth networks. The architecture leverages up to 16 cores on a single processor.	Scalable Storage (Solera DS Storage™) supports up to 24TB per device, externally expandable to petabytes to extend the available traffic capture window to days, weeks, months or more. You may optionally attach to industry standard storage device such as NAS or SAN.
Deep Packet Inspection audits 100% of all traffic headers and payloads; traditional stateful packet inspection audits only about 2% of traffic.	Solera OS™ for virtual and physical appliances, and deployment across disparate networks. Available web services APIs allow custom access to captured network traffic for further analysis by virtually any network security or management tool.
Application Programming Interface to integrate SonicWALL alerts with forensics data and applications provided by Solera Networks.	Solera DeepSee™ Forensics Suite for automatic indexing, and easy, contextual search, navigation, and replay of all data in motion on the network.



SonicWALL/Solera Networks Solution Workflow



How the Solution Supports Security Compliance

Most regulations do not specify individual technologies for compliance. Some do, but usually it's the organization's auditors who drive specifications for security in combination with an IT security framework such as NIST SP 800-53 for U.S. federal agencies, or COBIT for business IT governance. For purposes of compliance, the jointly integrated functionality of the SonicWALL/Solera Networks solution usually falls under categories such as monitoring, testing, surveillance, logging, auditing, data retention, and protecting networks and systems. Here are two examples:

NIST SP 800-53

The U.S. National Institute of Standards and Technology's Special Publication 800-53 provides federal civilian agencies with guidance on purchasing security controls for networks and computer systems. It fulfills statutory requirements of the Federal Information Security Management Act (FISMA). The SonicWALL/Solera Networks solution fulfills requirements in the following sections of SP 800-53 (Rev. 3):

- **AU-2 Auditable Events.** Ensures that auditable events are adequate to support after-the-fact investigations of security incidents. Adjusts audit targets based on current threat information and ongoing assessments of risk. Includes varying levels of abstraction, including detail down to packet level as information traverses the network. This facilitates identification of root causes to problems.
- **AU-3 Content of Audit Records.** Records must contain sufficient information to establish what, when and where events occurred, sources of the events, and their outcomes.
- **AU-6 Audit Review, Analysis, and Reporting.** For indications of inappropriate or unusual activity, reporting and analysis – including adjustments for changes in risk or policy.

PCI DSS

The Payment Card Industry Data Security Standard provides technical and operational requirements for protecting cardholder data. Any organization that accepts payment cards, or stores, processes or transmits cardholder data must comply 100% with the standard. PCI DSS v1.2 requires many controls, such as firewall, IPS, antivirus, and access. In addition to these, the SonicWALL/Solera Networks solution is used for compliance with Section 10: Regularly Monitor and Test Networks, as follows:

- **10.6** Review logs for all system components at least daily. Testing procedures require follow-up to exceptions.
- **10.7** Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (e.g. online, archived, or restorable from back-up).

SonicWALL, Inc.
1143 Borregas Avenue
Sunnyvale CA 94089-1306
T +1 408.745.9600
F +1 408.745.9300
www.sonicwall.com

Solera Networks
10713 South Jordan Gateway, Suite 100
South Jordan, Utah 84095
T +877-5SOLERA (+877.576.5372) or +1 801.545.4100
F +1 801.545.4040
www.soleranetworks.com



About Sonicwall

- Global organization founded in 1991
- Recognized leader with millions of users worldwide
- Visionaries Quadrant, Gartner Magic Quadrant
- 15,000 partners worldwide
- www.sonicwall.com

About Solera Networks

- Leader in forensic solutions for physical and virtual networks
- Provides complete historical record of all network activity
- Architecture is open, extensible and scalable
- www.soleranetworks.com

Learn More

For more information on the SonicWALL/Solera Network solution, contact:

Jacob Bardin
Federal Territory Manager
SonicWALL, Inc.
+1 703.624.2438
jbardin@SonicWALL.com
www.sonicWALL.com

Dave Nish
Inside Sales Manager
Solera Networks
+1 801.545.4051
dnish@soleranetworks.com
www.soleranetworks.com