

SOLUTION BRIEF

NEXT-GENERATION FIREWALL MEETS ACTIVE NETWORK FORENSICS

SUMMARY:

What: Active network forensics appliances from Solera Networks add full context to any security event identified by the Palo Alto Networks next-generation firewall platform

For: Replay and reconstruction of any network event to support:

- Incident Response
- Situational Awareness
- Network Security Assurance



Like a police force, network security products cannot prevent every criminal act. There are simply too many vulnerabilities and clever perpetrators to expect that your organization can forever avoid a security breach. Astute organizations understand the need to shift resources from a simple “prevention” mode to a complete detection and remediation system. After all, the worst attacks are the ones you never know about. A next-generation firewall combined with active network forensics levels the playing field by allowing network administrators to “see” attacks, uncover their root cause, configure the network to prevent their recurrence, and mitigate further risk.

PALO ALTO NETWORKS/SOLERA NETWORKS SOLUTION COMPONENTS

Palo Alto Networks offers real innovation in the firewall, enabling unprecedented visibility and control of all applications and content – by user, not just IP address – at up to 10Gbps with no performance



UNIQUE PALO ALTO NETWORKS TECHNOLOGIES

App-ID™: Patent pending traffic classification technology that uses as many as four different mechanisms to accurately identify exactly which applications are running on the network, irrespective of port, protocol, SSL encryption, or evasive tactic employed.

User-ID: Seamless integration with enterprise directory services (Active Directory, eDirectory, LDAP, and Citrix) enables administrators to view and control application usage based on individual users and groups of users, as opposed to just IP addresses.

Content-ID: A stream-based scanning engine uses a uniform signature format to block a wide range of threats and limit the transfer of unauthorized files and sensitive data, while a comprehensive URL database controls web surfing.

Purpose-built Platform: Multi-Gbps throughput is enabled through function-specific processing for networking, security, threat prevention and management, which are tightly integrated with a single pass software engine to maximize throughput.

UNIQUE SOLERA NETWORKS TECHNOLOGIES

Solera DeepSee™ Forensics Suite: for automatic indexing, and easy, contextual search, navigation, replay, and reconstruction of all data in motion on the network.

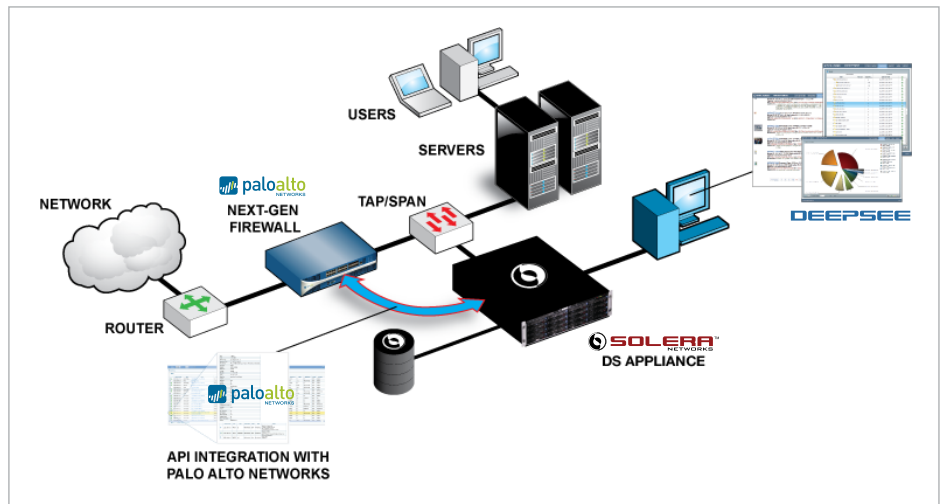
Solera DS™ Network Forensics Appliances: (DS 1150, DS 3150, DS 5150) DS Appliances enable active network forensics of all traffic (header and payload) up to 10Gbps with no network overhead. They work like a security camera for your network, recording everything and finding anything – fast.

Scalable Solera DS Storage™: Supporting up to 100TB of added storage. Extend the available storage to petabytes with DS SAN™ or DSFS file system licensing for NetApp™ to expand the forensics record to days, weeks, months or more.

Solera OS™: Patented operating system for virtual and physical appliances, and deployment across disparate networks. Available REST-based web services API allow custom access to captured network traffic for further analysis by virtually any network security or management tool.

SAMPLE IMPLEMENTATION

degradation. Based on patent-pending App-ID™ technology, these next-generation firewalls accurately identify applications – regardless of port, protocol, evasive tactic or SSL encryption – and scan content to stop threats and prevent data leakage. As a result, the firewall is once again able to function as a strategic point of network control. This enables enterprises to embrace the Web 2.0 world, while maintaining complete visibility and control, and significantly reducing total cost of ownership through device consolidation.



Network Forensics Appliances from Solera

Networks make all network traffic and 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. The Solera Networks open architecture seamlessly integrates with Palo Alto Networks next-generation firewalls, instantly providing full packet-level detail to any generated alert and specific details of what happened before and after an alert was triggered, including actual artifacts (documents, files, executables, etc.) recreated from raw network packets.

APPLYING ACTIVE NETWORK FORENSICS

Incident Response — Effective incident response starts with solid integration with the most popular security tools on the market. With the correct data, responding to an incident is instant, active, and efficient. Through the REST-based Web services API, Solera Networks appliances integrate directly to the Palo Alto Networks next-generation firewall to make all collected data available through standard PCAP format for sharing or analysis on a packet level.

Situational Awareness — Today, advanced, persistent, and targeted attacks are specifically designed to get around defenses that organizations have in place. Solera Networks appliances are like a time machine that can recreate and replay network traffic surrounding any event discovered by the Palo Alto Networks platform, providing situational awareness to defend networks against past, present, and future threats.

Network Security Assurance — Network security assurance verifies today that your network was not impacted by threats that were unknown yesterday. Because breaches can be transient and/or persistent—and signatures are typically written for initial exploits—there is no other way for historical incidents to be detected. With Solera Networks appliances you can replay traffic to your Palo Alto Networks next-generation firewall after it has been updated with the latest definitions. When a major new exploit is discovered, network security assurance can provide your organization the peace of mind that you are, and have been, secure against everything we know today.

LEARN MORE

For more information on the Palo Alto Networks/Solera Networks solution, contact:

Solera Networks

10713 South Jordan Gateway, Suite 100
South Jordan, UT 84095-3920
877-5SOLERA (877-576-5372)
1+ 801-545-4100
www.soleranetworks.com
Email: info@soleranetworks.com

Palo Alto Networks

232 East Java Drive
Sunnyvale, CA 94089-1318
866-320-4788
1+ 408-738-7700
www.paloaltonetworks.com
Email: info@paloaltonetworks.com

