

Solera Networks™ Announces Enhanced Integration with HP ArcSight™ ESM 5.0

Solera DeepSee™ enhances the ability to dig deep into network incidents to understand exactly what happened before, during, and after any security event

Washington, D.C. – HP Protect 2011 – Sept. 13, 2011 – [Solera Networks](#), the leading independent [Network Forensics and Security Analytics](#) platform provider, today announced its enhanced integration with the latest version of [HP ArcSight ESM](#), a leading Enterprise Threat and Risk Management platform, to provide visibility and context into network attacks, breaches, and insider threats. This integration allows security professionals to pivot directly from HP ArcSight ESM into a comprehensive packet-level record of any security event captured, indexed, and classified by Solera DS forensics appliances. Solera DeepSee delivers the evidence and artifacts required from every network packet to efficiently respond to today's advanced threats.

"Our strategy has always been to support integrations with best-of-breed network security solutions," said Steve Shillingford, President and CEO of Solera Networks. "Like a camera on the network, Solera DS Appliances provide a comprehensive record of what happened before, during, and after any event reported by HP ArcSight ESM. This enhanced integration gives incident response teams evidence to answer tough questions like, 'Who got into my network?', 'What did they see?', 'What did they take?', and 'What did they leave behind?'"

The award-winning Solera DS network forensics appliances include the powerful suite of DeepSee applications to deliver:

- Ultra-fast full packet capture, indexing and replay of all network traffic (layer 2-7)
- Active reporting to respond to incidents as they unfold
- Complete extractions and artifacts in their original format, recreated from the packet data
- Records of every image that crosses your network for acceptable use policy management
- Simplified root cause analysis workflow to speed the time to identify and minimize the scope of any breach

"We are responsible for securing very sensitive, classified information and rely on HP ArcSight ESM to make sense of countless network events related to a breach," said a Cyber Security Analyst at a major US government agency. "When responding to a targeted attack, the HP ArcSight solution is often our starting point for the investigation. Having the ability to pivot directly from the event into the full packet-level record on the Solera DS forensics appliance is huge. With Solera Networks we can respond with pinpoint accuracy."

About Solera Networks

[Solera Networks](#) is a pioneer in delivering Network Security Analytics – high-speed network monitoring, forensics, and analytics platform for complete network capture, classification, indexing, visualization, and reconstruction of any network event. Our systems record, classify, and index every packet, flow, and attribute, at line rates up to 10Gbps, on physical and virtual networks. Solera Networks appliances integrate into existing security workflows and support best-of-breed security tool environments, giving security professionals comprehensive network visibility. For more information on Solera Networks, visit www.soleranetworks.com.

###

Media Inquiries:

Alan Hall
Solera Networks
801.545.4060
ahall@soleranetworks.com

Suzanne M. Matick
Essem Communications
831.479.1888
suzanne@matick.net