DeepSee™ SOFTWARE

SOLERA NETWORKS™

Solera DeepSee™ Software

DeepSee Software Takes Big Data Security Intelligence and Analytics Out of The Box

YOUR CHALLENGE

Today's organizations are often blind to the activities of attackers due to the fact that today's advanced malware and zero-day attacks fly under the radar of traditional, preventative-based security technologies. As a result, organizations large and small are accepting the inevitability of security beaches. Due to the inevitability of advanced malware and attacks, there is a shift toward a more modern defense-in-depth strategy—one that provides the intelligence, context and real-time situational awareness needed to see and detect today's malware and advanced targeted attacks. Yet, many organizations still do not have these critical big data security technologies in place.

As security landscapes evolve, organizations and IT security teams are looking for big data security intelligence and analytics solutions to help them prepare for the reality of security gaps, while delivering 20/20 visibility of everything going in and out of the network. To efficiently address the growing gap in their security framework, organizations are mandating simple, flexible and cost-effective security solutions. With Big Data Security Intelligence and Analytics solutions from Solera Networks, organizations can close the security gap, while overcoming the challenges of adopting best-of-breed security intelligence and analytics, including:

- Easily deploying a simple and flexible solution that works with their current tools
- Finding a cost effective solution that fits into stretched security budgets
- Scaling to meet organization growth and increasing network performance demands

OUR SOLUTION

Solera DeepSee is the leading big data Security Intelligence and Analytics (SIA) solution that levels the battlefield against advanced threats and gives security professionals clear and concise answers to the toughest security questions. This award-winning solution records and classifies every packet of network traffic—from layer 2 through layer 7—while indexing and storing the data to provide comprehensive intelligence and analytics on any security event. The result is clear, actionable evidence for **Real-time Situational Awareness, Security Incident Response, Cyber Threat Detection, Data Loss Monitoring and Analysis, Organization Policy Compliance and Security Assurance.**

SOLUTION DESCRIPTION

Revolutionary new Solera DeepSee Software solution un-boxes the power of Security Intelligence and Analytics, eliminating the need for costly, proprietary hardware and storage.

KEY CAPABILITIES

- Fully featured security intelligence and analytics software solution
- Same performance and scalability as integrated appliances
- Integration with industry's leading security solutions
- Flexible licensing options for organizations of all sizes
- De-coupled software from it's underlying hardware
- Certified and widely available hardware platforms

KEY BENEFITS

- Gain 20/20 visibility into threats and 100% situational awareness into the network
- DeepSee Software leverages the latest in computer power and storage
- Add full context to any alert from leading security solutions
- Easy-to-deploy software solution with perpetual, term and enterprise-wide licensing
- Cost-effective OpEx security model that avoids high-overhead capital investments
- Simple, fast and scalable for easy deployment to all corners of an organization

Solera DeepSee Software is the only solution that is flexible, cost-effective and hardware-independent — while meeting the demands for high-performance, big data security analytics:

- Flexible, software-only delivery options optimize TCO and minimize CapEx costs
- Certified 10Gbps performance
- A patented database supporting 2M+ input/output operations per second (IOPS)
- Scalable storage options for large deployments (200+ terabytes)
- Solera DeepSee classification, search and real-time file extraction for instant delivery of recognizable evidence of a security breach or malware attack
- Direct integration with best-of-breed IPS, DLP, SIEM, log management, next-generation firewalls and malware detonation products

85%
of breaches took **weeks or more to discover (+6%)**
- VzB, 2012

1/3
of malware is **customized** (no signature available at time of exploit) - VzB, 2012

91%
of organizations believe that **exploits are bypassing their IDS and AV systems**
- VzB, 2012

KEY FEATURES

Flexible Deployment – Solera DeepSee Software provides the flexibility that no other solution can deliver. The industry's only software solution for security intelligence and analytics offers flexible and easy deployment on industry-standard hardware. Deploy DeepSee Software anywhere in an enterprise network from branch office to data center.

Application Classification – Solera DeepSee uncovers the true identity of any application trying to hide within your network. Comprehensive deep packet inspection (DPI) digs deep to classify over 900 applications and thousands of descriptive metadata details. This feature not only efficiently identifies applications but also provides descriptive information about a network session including application, personal identity, intended actions, content types, file names and more.

Real Time Intelligence – Real-Time Extractor is a security game changer. This innovative technology automatically extracts and analyzes any file—including the most prevalent and malicious file types. This enables immediate, automatic identification and alerting of advanced and zero-day threats.

Layer 2 to 7 Analytics – DeepSee Software provides a variety of analytics to strengthen security incident response with comprehensive and conclusive analysis. Some of the security-related analytics are: session reconstruction, reputation look up, media panel, root cause explorer and artifacts.

Context-aware security – Solera DeepSee integrates with best-of-breed network security technologies to pivot directly from any alert or log and obtain full-payload detail of the event before, during and after the alert. The open, web services REST API adds complete context to any security tool and lets you leverage leading technologies like HP ArcSight™, Dell™ SonicWALL™, FireEye™, McAfee®, Palo Alto Networks™, Splunk®, Sourcefire® or any other application.

Root Cause Explorer – Root Cause Explorer is the Incident Responder "Easy Button." Using extracted network objects, the tool reconstructs a timeline of suspect web sessions, emails and chat conversations. By automatically enumerating these events, Root Cause Explorer helps the analyst quickly identify the source of an infection or compromise and reduce time-to-resolution.

About Solera Networks

Solera Networks is the industry's leading advanced Security Intelligence and Analytics provider. Its award-winning DeepSee Software and Appliances are powered by next-generation deep-packet inspection and indexing technologies, network security analytics and intelligence capabilities. Global 2000 enterprises, cloud service providers and government agencies rely on Solera to see everything and know everything on their network—allowing them to gain total visibility and situational awareness, respond quickly and intelligently to advanced threats and malware, protect critical information assets, minimize exposure and loss and reduce business risk.

DeepSee™ SOFTWARE

DeepSee™ APPLIANCE

DeepSee™ VIRTUAL APPLIANCE

Solera Networks Headquarters
10713 South Jordan Gateway
Suite 100
South Jordan, Utah 84095

www.soleranetworks.com
info@soleranetworks.com
877-5SOLERA or 877-576-5372
801-545-4100

SOLERA NETWORKS™