



Solera DeepSee™ Appliances

Turnkey, High-performing Big Data Security Intelligence and Analytics Appliances



YOUR CHALLENGE

Enterprises, service providers, government agencies and financial institutions are all under constant cyber attacks. Today's advanced threats, targeted attacks, and custom malware evade traditional security infrastructure. Lack of visibility and situational awareness further complicate the ability to discover and contain advanced threats and malware. To effectively defend and protect information assets, reputation and business viability, organizations need the full visibility only provided by Big Data Security Intelligence and Analytics.

Organizations have found it difficult to deploy a high-performance, scalable solution that enables security intelligence and analytics throughout the operational domain. An effective Security Intelligence and Analytics solution must:

- Scale to provide visibility throughout the organization—from the data center to remote offices
- Deliver high performance and sufficient storage capacity to meet growing network traffic demands
- Integrate with existing security infrastructure to leverage investments and established processes

OUR SOLUTION

Solera Networks is leading the explosion of Security Intelligence and Analytics (SIA). The Solera DeepSee Appliance is a turnkey solution that is pre-configured to deliver complete network visibility and situational awareness right out of the box. The award winning DeepSee Software, captures, indexes, classifies, and enriches all network traffic in real-time with threat intelligence data. Data is stored in a purpose-built, patented database and file system for rapid analysis, instant retrieval and complete reconstruction. DeepSee Appliances can be deployed anywhere in the network: at the perimeter or the core, 10 GbE backbones, or remote links to deliver clear, actionable intelligence for **Real-time Situational Awareness, Security Incident Response, Cyber Threat Detection, Data Loss Monitoring and Analysis, Organization Policy Compliance and Security Assurance.**

SOLUTION DESCRIPTION

Integrated and pre-installed with DeepSee Software, DeepSee Appliances are the industry's standard for delivering Big Data Security Intelligence and Analytics

KEY CAPABILITIES

- Scalable, easy and distributed management with DeepSee Central Manager
- Stand-alone operation with built-in DeepSee Dashboard
- High-performing integrated appliances with up to 10 Gbps packet capture rates
- Extremely expandable capacity for large capture windows, even years
- Turnkey deployment with pre-installed and pre-configured software
- Carrier class appliances – high availability and serviceability
- Integration with industry's leading security solutions

KEY BENEFITS

- Gain situational awareness and understand the full-context of security events
- Complete network traffic capture with full application visibility
- Collect and analyze traffic from a stand-alone appliance or across a distributed environment
- Evaluate any security event with real-time intelligence and analytics
- Speed threat identification, reduce incident response time, and shorten exposure windows
- Quick and easy deployment, even in resource constrained environments

DeepSee Appliances are the only completely integrated solution for big data security intelligence and analytics:

- Application Classification—Over 900 applications and thousands of descriptive, metadata attributes—including content types, file names and more are classified for easy analysis and recall
- Real Time Intelligence—Real-Time File Extractor is an industry first that enables policy-driven, instant reconstruction and analysis of files and network flows that may represent a threat
- Layer 2 to 7 Analytics—DeepSee Software provides a variety of analytics tools: complete session reconstruction, data visualization, root cause explorer, timeline analysis, file and object reconstruction, IP geo-location, trend analysis, and more
- Context-aware security—DeepSee integrates with best-of-breed security technologies to pivot directly from any alert or log and obtain full-payload detail of the event—before, during and after the breach
- Root Cause Explorer—This incident responder ‘Easy Button’ uses extracted network objects to reconstruct a timeline of suspect web sessions, emails, and chat conversations

Key Features

Turnkey Deployment: Pre-configured appliances allow easy deployment anywhere in the organization

Flexible Operation: Synchronous operation in a stand-alone mode or in a distributed environment

Central Management: Monitor thousands of network segments from a ‘single pane of glass’

High Performance: Multi-core processing for real-time capture and indexing with up to 10 Gbps lossless capture rates

Patented Database: Solera DB is an optimized database for big data security intelligence and analytics

On-board Analytics: Real-time packet capture, classification and indexing without any network overhead

Selective Recording: Configurable storage allocation for indexed metadata and full packet data

Enterprise Class: Appliances include long-life, redundant and field-replaceable components

Expandable Capacity: Supports 20 TB storage modules for add-on capacity to meet changing requirements

	Form Factor	Capture Rate (peak)	On-board Capacity	Expandable Capacity	Interfaces
 DeepSee 2G Appliance	1 RU	2 Gbps	6 TB	3 x 20 TB	3 x 1 GbE
 DeepSee 10G Appliance	2 RU	10 Gbps	20 TB	6 x 20 TB	7 x 1 GbE 2 x 10 GbE
 DeepSee Central Manager	1 RU	-Not Applicable-	3TB (not for capture)	-Not Applicable-	1 x 1 GbE
 DeepSee Storage Module	2 RU	-Not Applicable-	20 TB	-Not Applicable-	2 x SAS6

About Solera Networks

Solera Networks is the industry’s leading big data security intelligence and analytics company. Its award-winning DeepSee™ platform levels the battlefield against advanced targeted attacks and malware, and gives security professionals clear and concise answers to the toughest security questions. Solera DeepSee is powered by next-generation deep-packet inspection and indexing technologies, full-packet capture, malware analysis and real-time security intelligence and analytics capabilities. Global 2000 enterprises, cloud service providers and government agencies rely on Solera for real-time situational awareness, security incident response, cyber threat detection, data loss monitoring and analysis, organization policy compliance and security assurance—allowing them to respond quickly and intelligently to advanced threats and attacks, while protecting critical information assets, minimizing exposure and loss, and reducing business liabilities.

