DeepSee™ VIRTUAL APPLIANCE

SOLERA NETWORKS™

Solera DeepSee™ Virtual Appliance

Big Data Security Intelligence and Analytics in Any Virtual Environment

YOUR CHALLENGE

There has been a major drive to virtualize IT assets and infrastructure. Enterprises in all industries have virtualized their data centers, applications and mission-critical systems. Virtualization has reduced capital expenses and IT footprint, resulting in great savings—but it's not without a cost. Unfortunately in recent years advanced malware and targeted attacks have evolved to infiltrate virtual environments and compromise mission-critical systems. IT organizations must gain complete enterprise-wide visibility to monitor, detect and analyze these advanced threats, even within virtual environments.

With the need to gain visibility into advanced threats that target virtual environments, organizations must meet the challenge to acquire sophisticated security that will fit into their existing virtual IT infrastructure. IT organizations need to gain visibility into their physical enterprise network as well as the activity within the virtual infrastructure, thereby achieving complete situational awareness into potential advanced malware and attacks. Big Data Security Intelligence and Analytics solutions enable enterprises to detect advanced threats and enable expedited mitigation.

Some of the challenges that enterprises face in adopting Security Intelligence and Analytics solutions are in finding a solution that:

- Fits into security budgets without incurring capital expenditures
- Is easily deployed into their existing virtual environment and that supports their existing security tool infrastructure
- Scales with the growth in their virtual data centers, servers, applications and network traffic

OUR SOLUTION

The DeepSee Virtual Appliance is the industry's first and only Big Data Security Intelligence and Analytics appliance available as a virtual machine. This patented appliance includes the same DeepSee technology as on a physical appliance, which provides complete visibility into virtual networks and private and hosted clouds—as well as a cost-effective option for branch, small and medium enterprises. The DeepSee Virtual Appliance furnishes complete visibility of network traffic—including traffic between applications running in the virtual network. With support for VMware™ ESX servers, Citrix XenServer, Windows Hyper-V Virtual and KVM

SOLUTION DESCRIPTION

Industry's first and only virtual appliance for Big Data Security Intelligence and Analytics, delivering unprecedented visibility and threat detection for any virtual environment

KEY CAPABILITIES

- Fully featured Big Data Security Intelligence and Analytics solution
- Complete network capture (layers 2-7), indexing, classification, storage and replay
- Performance and scalability to support physical, cloud or virtual network infrastructure
- Virtualized central management to gain enterprise-wide visibility
- Support for all leading enterprise virtual environments and infrastructures
- Integration with industry's leading network security vendor solutions

KEY BENEFITS

- 20/20 visibility into advanced malware, threats and attacks
- 100% situational awareness of enterprise virtual and cloud environments
- Minimal capital expenditure, reduced footprint and saved resources
- Ease of deployment, usage and management in standalone or distributed operation
- On-demand incident response with remote deployment
- A perfect complement to existing security controls with advanced threat detection

environments, the virtual appliance delivers the world's most comprehensive, flexible and cost-effective solution for security intelligence, analytics and advanced threat detection. DeepSee Virtual Appliance – Lab Edition is a no-cost version of the DeepSee Virtual Appliance that is easily deployed on desktops and laptops for simplicity and portability. The Lab Edition is ideal for threat researchers, security consultants, security analysts and incident responders.

Solera Networks is the leading Big Data Security Intelligence and Analytics (SIA) provider 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. The result is clear, actionable evidence for **Real-time Situational Awareness, Security Incident Response, Advanced Threat Detection, Data Loss Monitoring and Analysis, Organization Policy Compliance and Security Assurance.**

KEY FEATURES

Easy Deployment – Solera DeepSee Virtual Appliance offers the easiest way to implement and deploy Big Data SIA. Deploy the DeepSee Virtual Appliance on a laptop, desktop or enterprise server in VMware, Citrix, Windows or KVM virtual environments, anywhere in an enterprise network, from branch office to data center.

Application Classification – Comprehensive deep-packet inspection (DPI) digs deep to classify more than 900 applications and supply thousands of descriptive metadata details. This feature efficiently identifies applications and also provides descriptive information about a network session, including application, identity, geographic location and more.

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

Layers 2 through 7 Analytics – DeepSee Analytics provide a variety of features to strengthen security-incident response with comprehensive and conclusive analyses. Some of the security-related analytics are: session reconstruction, media panel, artifacts, packet analyzer and extensive filtering and search features.

Context-Aware Security – DeepSee integrates with best-of-breed network security technologies so that you can 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 existing investments.

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 listing these events, Root Cause Explorer helps the analysts reduce time-to-resolution.

SPECIFICATIONS

Interfaces
1—Virtual Management Interfaces
3—Virtual Capture or Replay Interfaces

Capacity
500GB, 2TB, 5TB or 10TB of usable storage

Minimum CPU & RAM
2-Core CPU with 8 GB RAM

Virtual Environments
VMware ESX servers, VMware Workstation, Citrix XenServer, Windows Hyper-V Virtual and KVM

Versions
DeepSee Virtual Appliance – Enterprise
DeepSee Virtual Appliance – 30-Day Trail (ESX)
DeepSee Virtual Appliance – Lab Edition (VMware Workstation, No-Cost Version)

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 Networks 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, reduce business risk and minimize exposure and loss.

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™