BLUE COAT®

Security Empowers Business

DATASHEET

EXTEND THREAT MITIGATION TO VIRTUAL ENVIRONMENTS – ANYWHERE

Blue Coat Security Analytics Virtual Appliance

The virtualization of IT resources – from data centers and mission-critical systems to applications – has reduced capital expenses and increased utilization rates. Unfortunately, virtualization can carry a hidden cost. Advanced malware and targeted attacks now threaten virtualized assets wherever they reside. The Blue Coat Security Analytics Virtual Appliance deepens your defenses. As part of the Blue Coat Advanced Threat Protection Lifecycle Defense, it provides complete visibility into all network traffic, including traffic between applications running in the virtual network, and delivers unified security analytics, threat intelligence, and security visibility. So you can better protect your virtual assets anywhere, empowering your workforce and your business.

Real Protection for Virtual Assets

To mitigate the risks of advanced threats in virtual environments, organizations must achieve full security visibility and situational awareness into next-generation malware and targeted attacks. Security analytics solutions can provide these capabilities, allowing enterprises to detect advanced threats and enable swift incident response and mitigation. However, enterprises must also find a solution that:

- Works with both physical and virtual network environments
- Is easily deployed in remote or branch offices and any existing virtual environment
- Integrates with existing security tools to deliver greater context and leverage security processes, workflow, and threat intelligence
- Scales with continued growth in virtual data centers, servers, applications and network traffic

The Blue Coat Security Analytics Virtual Appliance includes the same advanced security analytics technology found in the high-performance, pre-configured Blue Coat Security Analytics Appliances, but also provides complete visibility into virtual networks and private and hosted clouds. As a virtual appliance, this solution delivers a cost-effective option for branch, small and medium enterprise deployments. Key capabilities include:

- **Unified security analytics, threat intelligence, and security visibility** – enabling superior advanced threat protection. Combined with Blue Coat ThreatBLADES, the Security Analytics Virtual Appliance leverages Security Analytics Software, which captures and classifies every packet of network traffic – from Layer 2 through Layer 7 – to provide comprehensive intelligence and analytics. The result is real-time situational awareness, continuous monitoring, advanced malware detection, incident response and resolution, data loss monitoring and analysis, organization policy compliance, and security assurance.
- **Application Classification** – Comprehensive deep-packet inspection (DPI) classifies more than 1,800 applications and supplies

AT A GLANCE

Description

The Security Analytics Virtual Appliance is the industry's only patented security intelligence and analytics appliance available as a virtual machine.

Capabilities

- Easy, flexible deployment on a laptop, desktop, or enterprise server anywhere in an enterprise network – from branch offices to data centers
- Deep-packet inspection (DPI) classifies more than 1,800 applications and supplies thousands of descriptive metadata details
- Real-time threat Intelligence via integration with Blue Coat ThreatBLADES and the Blue Coat Global Intelligence Network of more than 75 million users
- Context-aware security for full-payload detail of security events before, during and after the alert, with root-cause analysis for reduce time-to-resolution

Key Benefits

- Gain full security visibility into threats and 100% situational awareness of any network activity
- Capture and port all virtual traffic to physical security tools for comprehensive analysis
- Easily deploy anywhere in stand-alone or distributed networks for on-demand incident response
- Improve the performance of next-generation malware analysis and sandboxing
- Add full context to any alert via integration with leading security solutions

BLUE COAT®

Security Empowers Business

DATASHEET

thousands of descriptive metadata details. This feature efficiently provides descriptive information about a network session, including application, identity, geographic location and more.

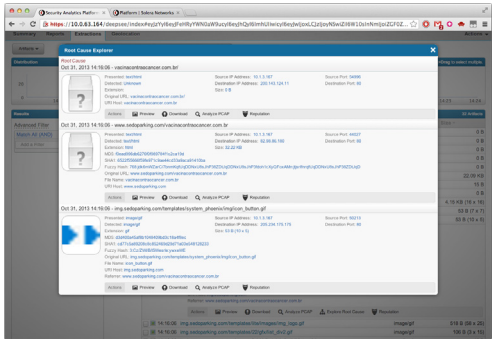
- **Real-time Threat Intelligence** – ThreatBLADES integrate directly with the Security Analytics Virtual Appliance and leverage the Blue Coat Global Intelligence Network, providing instant, actionable intelligence on web, file, or email threats.
- **Context-Aware Security** – The Security Analytics Virtual Appliance 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. You can leverage leading technologies such as Dell SonicWALL™, FireEye™, HP ArcSight™, McAfee®, Palo Alto Networks™, Sourcefire®, Splunk®, and many other security applications.
- **Root Cause Explorer** – Using extracted network objects, this 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

Benefits

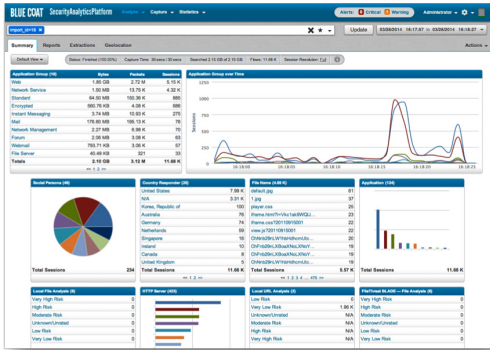
- **Full security visibility** into threats and 100% situational awareness of any network activity
- **Comprehensive analysis** of advanced threats through capturing and porting all virtual traffic to security tools in your physical network
- **Reduction of IT footprint**, saving valuable resources with minimal capital expenditure
- **Easy deployment** and management in stand-alone or distributed networks
- **On-demand incident response** through remote deployment anywhere in the network
- **Full context** for security incidents through integration with leading security solutions
- **Scalability** to support rapid growth in virtual data centers, servers, applications, and network traffic

Features

- Fully featured security analytics solution in a flexible virtual appliance
- Complete network capture (Layers 2-7), indexing, classification, storage and replay
- Performance and scalability to support any cloud or virtual network infrastructure
- Virtualized central management to gain enterprise-wide visibility
- Support for all leading enterprise virtual environments and infrastructures
- Seamless integration with Blue Coat ThreatBLADES
- Integration with industry's leading network security tools



Root Cause Explorer: Quickly determine the root source of any threat



Customized dashboard view for quick analysis

DATASHEET

SECURITY ANALYTICS VIRTUAL APPLIANCE

ARCHITECTURE	64-bit
BROWSER	Microsoft IE 8+, Firefox 18+, Safari 5+, Chrome 24+

VIRTUAL ENVIRONMENTS

ESXI	VMware ESXi 5 server (ESXi 5.5 is recommended for Security Analytics Platform 7.0+)
WORKSTATION	Workstation 9, Fusion 5, Player 6

APPLIANCE SIZING

	50G	500G	2T	5T	10T	CMC[1]	ESX TRIAL	WORKSTATION
CAPTURE	40 GB	0.4 TB	1.6 TB	3 x 1.34 TB	5 x 1.6 TB	40 GB	1.5 TB	100 GB[2]
INDEX	10 GB	0.1 TB	0.4 TB	1.0 TB	1.7 TB	10 GB	220 GB	20 GB[2]
SYSTEM	80 GB	0.1 TB	0.5 TB	0.75 TB	1 TB	30 GB	80 GB	80 GB
RAM (GB)	12	12	16	32	64	8	12	8
CPUS	8	8	8	4	8	2	8	4

[1] CMC sizing depends on factors such as the average capture rate and number of sensors that the CMC controls. Increase the size of the system disk as the capture speed and number of sensors increases. Refer to the table below as a general guideline.

[2] The size of capture and index virtual disks for the VMware workstation evaluation can be increased as long as the index disk is at least 20% the size of the capture disk.

CENTRAL MANAGER SIZING

AVG. CAPTURE RATE (GBPS)	RAM	CPUS
<0.5	8 GB	8
0.5	8 GB	8
2	16 GB	16
5	32 GB	32

BLUE COAT®

Security Empowers Business

Blue Coat Systems Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA
+1.408.220.2200

EMEA Headquarters
Hampshire, UK
+44.1252.554600

APAC Headquarters
Singapore
+65.6826.7000