BLUE COAT®

Security Empowers Business

HYBRID SANDBOXING FOR DETECTING AND ANALYZING ADVANCED AND UNKNOWN MALWARE

Malware Analysis Appliance

DATASHEET

The Blue Coat Malware Analysis Appliance is a key component of Blue Coat's Security and Policy Enforcement Center. Integrated with the Blue Coat Content Analysis System, it bridges the gap between blocking of known malware and detection and analysis of unknown and advanced malware.

The customizable appliance delivers comprehensive malware analysis and detonation with a dual detection approach that allows you to analyze suspicious files and reduce the impact posed by zero-day threats and unknown malware.

Dual Detection Approach: Best Way to Detect More Malicious Behavior

The Malware Analysis Appliance utilizes a powerful dual-detection approach that combines the benefits of code emulation with virtual machine introspection. This captures more malicious behavior across a wider range of custom environments than other solutions that typically rely on a single methodology. The dual detection approach includes:

- Sandbox® – A bare metal environment that emulates an actual system to detect malware that otherwise will not detonate in a virtualized environment.
- IntelliVM – Virtual machine profiles that replicate actual production environments, including custom applications, to quickly spot anomalies and differences in behavior that unveil anti-analysis and other advanced malware evasion techniques.

Simulated Systems: Detonation for Evasive Malware

The unique sandboxing technology simulates bare metal environments to detect evasive malware. The Malware Analysis Appliance uses malware detonation to execute files within the simulator as they would on a real system – without executing code on the targeted CPU, loading into real memory, or communicating with any other physical system components.

Working at the kernel level, the emulator exercises the malware, intercepting behavior and converting it into step-by-step forensic intelligence. Without ever putting actual systems at risk, the sandboxing technology provides a map of the damage the threat would cause if allowed to run on a real machine.

Custom Virtual Environments for Faster Anomaly Detection

With IntelliVM technology, the Malware Analysis Appliance uses virtual machine profiles to mirror different types of custom environments, so you can quickly detect anomalies and differences in behavior that unveil advanced malware evasion techniques. The Malware Analysis Appliance can monitor a wide range of system events for signs of malicious behavior in a safe, instrumented virtualized environment.

IntelliVM profiles can be customized to add flexibility when analyzing non-traditional malware, and to precisely mirror production environments to detect advanced malware and targeted attacks. Security analysts can analyze all types of threats, in any version of any application they choose. They are able to precisely match their organizations' desktop environments, gathering intelligence on malware targeting their specific organizations which may be looking to exploit specific application vulnerabilities.

Shared Threat Intelligence: Operationalize Learned Knowledge to Fortify Security Infrastructure

As unknown or advanced malware and zero-day threats are detonated, the new threat intelligence is shared locally across the security infrastructure, as well as with all of Blue Coat's 15,000 customers and 75 million users worldwide through a Global Intelligence Network. Turning unknown threats into known threats and sharing that information across the security infrastructure increases the scalability and effectiveness of the defense by moving protection to Blue Coat ProxySG secure web gateways.

BLUE COAT®

Security Empowers Business

DATASHEET

Malware Analysis Appliance Benefits

- **Superior analysis and accuracy** – Unique dual detection approach combines sandboxing with IntelliVM to deliver unrivaled malware and threat detection. Automatic sample classification and risk scoring by highest matched pattern along with support for existing malware analysis workflows allows you to flag detected system events based on potential malicious activity.
- **Ease of use and alerting** – Real-time incident reporting with detailed analysis of the event provides immediate notification to security analysts while a best-in-class, web-based user interface enables interaction with malware and the ability to click through installers. The web-based dashboard enables easy searches of the malware intelligence and collection database, store samples, reports, and events.
- **Scalable architecture and performance** – Process hundreds of thousands of files per day with parallel sample processing on up to 55 virtual machines per single Malware Analysis Appliance. Multiple VMs with Windows XP and Windows 7 OS's and unlimited software configurations can be supported.

MALWARE ANALYSIS APPLIANCE SERIES	MAA S400-10	MAA S500-10
PERFORMANCE		
Malware Samples	12,000 samples per day	50,000 samples per day
SYSTEM		
Disk Drives	2 x 500GB	6 x 1TB
RAM	32GB	96GB
Onboard Ports	(1) 1000Base-T Copper, System Management Port (1) 1000Base-T Copper, BMC Management Port	(1) 1000Base-T Copper, System Management Port (1) 1000Base-T Copper, BMC Management Port
Power Supplies	2	2

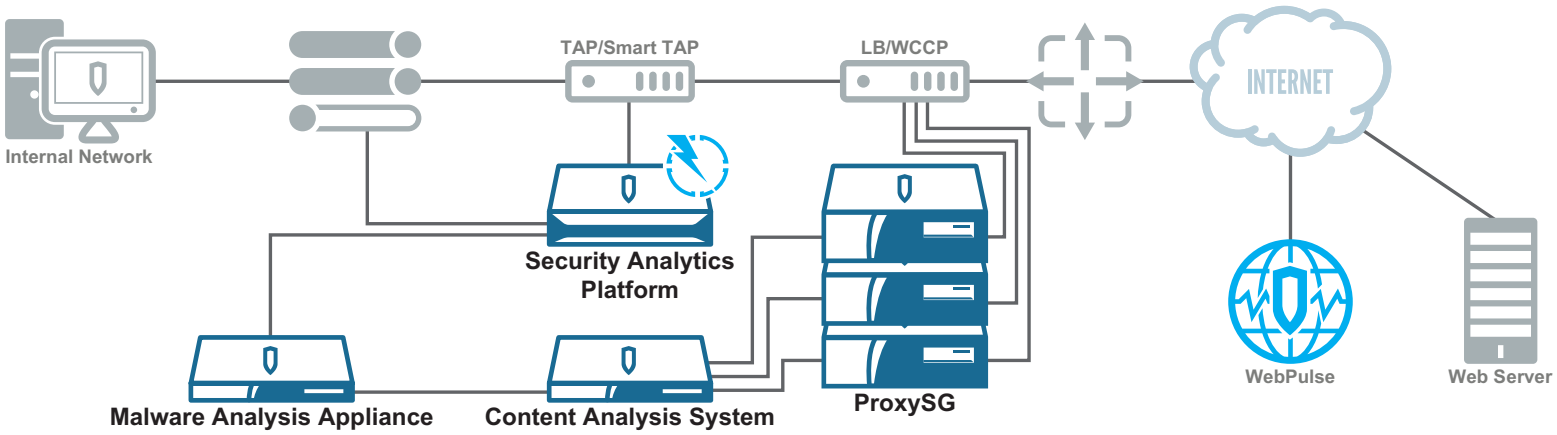
PHYSICAL PROPERTIES	MAA S400-10	MAA S500-10
DIMENSIONS AND WEIGHT		
Dimensions	572mm x 432.5mm x 42.9mm (22.5in x 17.03in x 1.69in) (chassis only) 643mm x 485.4mm x 42.9mm (25.3in x 19.11in x 1.69in) (chassis w/extensions) 1 RU height	710mm x 433.3mm x 87.2mm (27.95in x 17.05in x 3.43in) (chassis only) 812.8mm x 433.4mm x 87.2mm (32in x 17.06in x 3.43in) (chassis w/extensions) 2 RU height
Weight (maximum)	Approx. 12.8 kg (28 lbs) +/- 5%	Approx. 30kg (66.12 lbs) +/- 5%
OPERATING ENVIRONMENT		
Power	Dual redundant and hot swappable power supplies, AC power 100-127V @ 8A, 200-240V @ 4A, 47-63Hz (DC power available)	Dual redundant and hot swappable power supplies, AC power 100-240V, 50-60Hz, 12-5A (DC power available)
Maximum Power	450 Watts	1100 Watts
Thermal Rating	Typical 1086 BTU/Hr, Max 1381 BTU/Hr	Typical 2598.42 BTU/Hr, Max 3751 BTU/Hr
Temperature	5°C to 40°C (41°F to 104°F) at sea level	
Humidity	20 to 80% relative humidity, non-condensing	
Altitude	Up to 3048m (10,000ft)	

BLUE COAT®

Security Empowers Business

FOR ALL MALWARE ANALYSIS APPLIANCES

REGULATIONS	SAFETY	ELECTROMAGNETIC COMPLIANCE (EMC)
International	CB – IEC60950-1, Second Edition	CISPR22, Class A; CISPR24
USA	NRTL – UL60950-1, Second Edition	FCC part 15, Class A
Canada	SCC – CSA-22.2, No.60950-1, Second Edition	ICES-003, Class A
European Union (CE)	CE – EN60950-1, Second Edition	EN55022, Class A; EN55024; EN61000-3-2; EN61000-3-3
Japan	---	VCCI V-3, Class A
Mexico	NOM-019-SCFI by NRTL Declaration	---
Argentina	S Mark – IEC 60950-1	---
Taiwan	BSMI – CNS-14336-1	BSMI – CNS13438, Class A
China	CCC – GB4943.1	CCC – GB9254; GB17625
Australia/New Zealand	AS/NZS 60950-1, Second Edition	AS/ZNS-CISPR22
Korea	---	KC – RRA, Class A
Russia	CU – IEC 60950-1	GOST-R 51318.22, Class A; 51318.24; 51317.3.2; 51317.3.3
ENVIRONMENTAL	RoHS-Directive 2011/65/EU, REACH-Regulation No 1907/2006	
PRODUCT WARRANTY	Limited, non-transferable hardware warranty for a period of one (1) year from date of shipment. BlueTouch Support contracts available for 24/7 software support with options for hardware support.	
GOV'T CERTIFICATIONS	For further government certification information please contact Federal_Certifications@bluecoat.com	
MORE INFO	Contact regulatoryinfo@bluecoat.com for specific regulatory compliance certification questions and support	



Blue Coat Advanced Threat Protection Reference Architecture.

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