Malware Analysis S400/S500

Respond To Malicious Threats That Elude Traditional Defenses

At A Glance

Description

Detects and analyzes unknown, advanced, and targeted malware using a unique, dual-detection approach that safely detonates suspicious files and URLs, reveals malicious behavior, and exposes zero-day threats.

Capabilities

- Comprehensive, enterprise-class malware detonation in highly realistic sandbox environments
- Combines dynamic, static, and reputational analysis techniques for more thorough exposure of malware
- Scalable and customizable solution
- Detailed forensics and shared threat intelligence
- Seamless integration with Symantec Content Analysis, Symantec Mail Threat Defense or Symantec Security Analytics

Key Benefits

- Transforms malware exposure into continuous security improvement
- Superior detection, more accurate and relevant analysis
- Exceptional performance even on high-volume networks
- Helps prioritize and accelerate incident response

Symantec Malware Analysis is a key component of Symantec's Advanced Threat Protection solution. Integrated with Symantec Content Analysis, Symantec Mail Threat Defense or Symantec Security Analytics, it provides a highly scalable solution for detecting and analyzing unknown, advanced, and targeted malware. This adaptive and customizable sandbox solution delivers enterprise-class, comprehensive malware detonation and analysis using a unique, dual-detection approach to quickly analyze suspicious files and URLs, interact with running malware to reveal its complete behavior, and expose zero-day threats and unknown malware.

Expose More Malicious Behavior

Malware Analysis utilizes a powerful dual-detection approach that combines virtualization and emulation to capture more malicious behavior across a wider range of custom environments than typical consolidated single-sandbox solutions.

- Emulation Sandbox: An instrumented, fully controlled, replicated PC computing environment emulates Windows systems to detect malware that otherwise will not detonate within a virtualized environment
- Virtualization Sandbox: Custom analysis profiles replicate actual Windows production environments, down to the applications and versions in use, to quickly spot anomalies and behavioral differences that unveil anti-analysis, sleep, and other advanced evasion techniques. A virtualized Android sandbox detects and analyzes mobile threats traversing enterprise networks.

Multiple Detection Techniques

Malware Analysis uses a combination of static and dynamic analysis techniques that employ standard, custom, and open source YARA patterns to unmask cleverly disguised malware. It detects packed malware and VM-aware samples that alter their behavior in an artificial environment, plus malware that attempts to wait out any sandbox analysis using short or long sleeps.

Symantec

Defeat Anti-Analysis at Many Levels

Anti-analysis defeating tools – such as hook-based introspection, high-level and low-level event capture, and detection in both kernel and user modes – intercept and convert behavior into detailed forensic intelligence.

Interact with Running Malware

A flexible plug-in architecture extends detection and processing by interacting with running malware, clicking through dialog boxes and installers, and generating unique post-processing analysis artifacts.

Generate More Relevant Results

Virtual machine profiles replicate multiple custom production environments, allowing security analysts to analyze threats across a range of operating systems and applications. They can closely match their organizations' desktop environments, gathering intelligence on malware targeting their organizations directly or seeking to exploit specific application vulnerabilities.

Customize Detection and Risk Scoring

Detection criteria, analysis parameters, firewall settings, and risk scoring can all be customized to add flexibility, unique detection, and fast response capabilities when analyzing non-traditional and targeted malware in unique production environments.

Adaptive Intelligence for Changing Threats

Since Malware Analysis does not rely on static signatures, its flexible detection patterns are designed to detect polymorphic files, single-use targeted malware, and fast-changing website domains.

Detailed Forensics for Remediation

Symantec sandboxing technology provides security defenders a comprehensive map of the damage – including both host-based and network indicators of compromise – that any malicious file or URL would cause to equivalently configured production machines without putting actual computers or sensitive data at risk.

Share Threat Intelligence

As unknown, advanced, or targeted malware and zero-day threats are exposed, the previously unseen or uncategorized threats are shared across the security infrastructure with the Symantec Global Intelligent Network, a network effect of our 15,000 customers worldwide.

Inoculation for Forward Defenses

Malware Analysis turns unknown threats into known threats and shares threat data with others across the global network, improving the effectiveness of front-line defenses such as Blue Coat ProxySG secure web gateways by moving protection forward to the perimeter where blocking will take place for subsequent attacks.

Malware Analysis Features

- Dual-detection emulated and virtual sandbox analysis environments
- Customizable Windows 8/7/XP profiles closely match production systems
- Virtualized Android sandbox detects mobile threats
- Pattern-based detection exposes malicious files and URLs including polymorphic, unique, and targeted threats
- Supports any PC file format
- Clicks through dialogs and installers to expose interactive malware requiring user interaction
- Thwarts VM-aware malware, bypasses sleep calls, and detects generic exploits such as "heap sprays"
- Customizable pattern matching, analysis settings, and risk scores

- Automatic pattern updates for continuous protection against fast-evolving threats
- Generates relevant, granular verdicts plus a complete range of analysis artifacts
- Seamlessly integrates with Symantec Content Mail Threat Defense and Security Analytics
- Integrates with the Global Intelligence Network for continuous threat sharing among our 15,000 customers who include over 70% of the Fortune Global 500
- Supports centralized appliance management for enterprise provisioning and deployment
- Provides real-time sandboxing to block malicious files before delivery

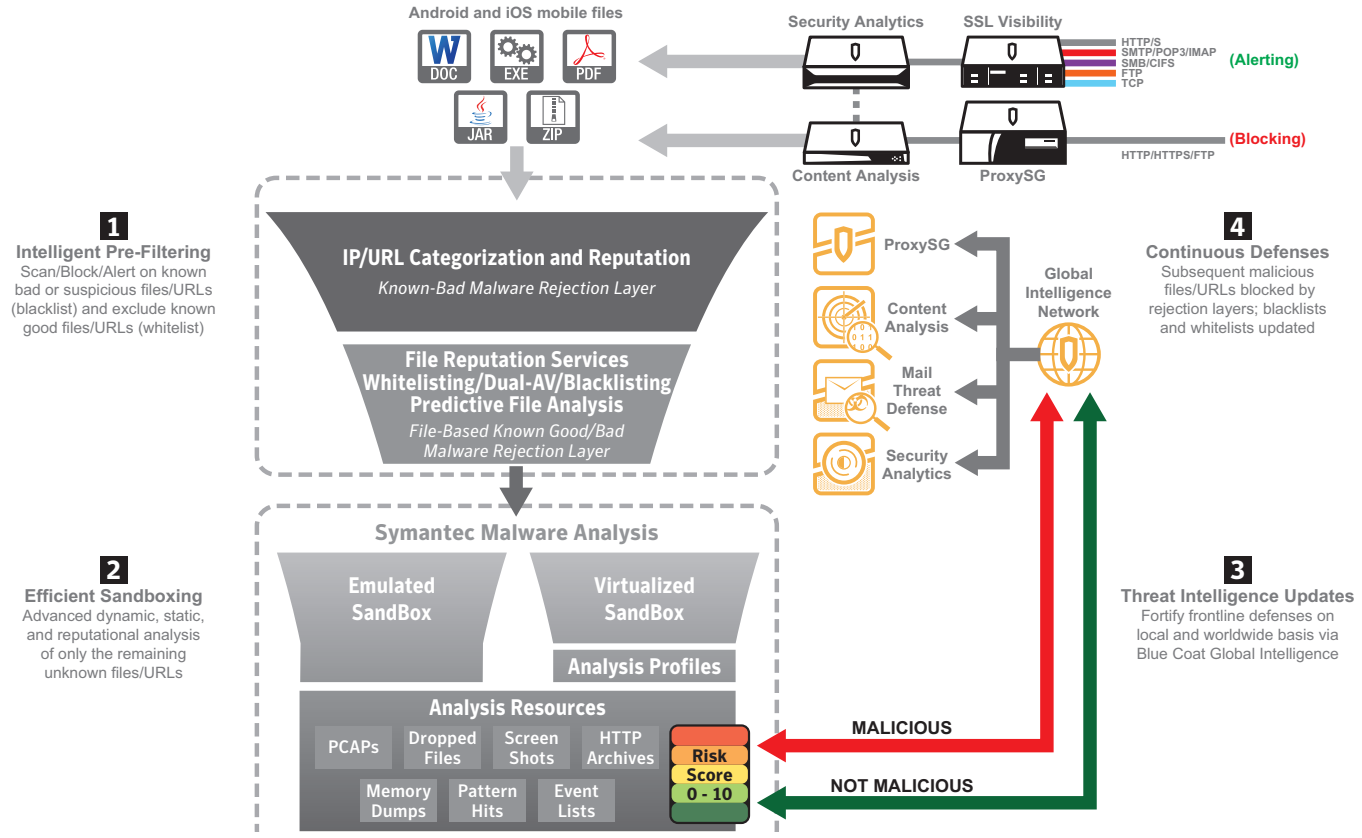
Malware Analysis Benefits

- Superior threat detection: Unique dual-detection approach combines emulation and virtual sandboxing, plus static and dynamic analysis techniques, to deliver unrivaled intelligence for unknown threats
- Accurate and relevant analysis: Customized virtual machine profiles running Windows XP, Windows 7, and Windows 8 closely replicate actual corporate gold images to detect targeted threats against actual production configurations
- Customizable analysis and risk scoring: Automatic sample classification and risk scoring – augmented by custom detection patterns, interactive analysis plugins, and risk scores – flag suspicious system events based on degree of potential malicious activity within your unique environment
- High throughput performance: Parallel sample processing on up to 55 virtual machines per single Malware Analysis appliance generates continuous enterprise-class performance on high volume, high threat networks
- Improved incident response: Helps prioritize and focus incident response, streamlining damage assessments and speeding remediation efforts
- Inoculates forward defenses: Shares threat intelligence with the Global Intelligence Network, providing rapid updates to inline forward defenses that quickly block newly exposed malware

MALWARE ANALYSIS 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, "Dirty Line" Connection Note: BMC ports have been disabled	(1) 1000Base-T Copper, System Management Port (1) 1000Base-T Copper, "Dirty Line" Connection Note: BMC ports have been disabled
Optional NIC		2x10Gb Base-T (Copper non-bypass)
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)	

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	



Malware Analysis Ecosystem

About Symantec

Symantec Corporation World Headquarters

350 Ellis Street Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

SYMC_ds_Malware_Analysis_S400_S500_EN_v2a