DATA SHEET

Content Analysis

Advanced, Multi-layer Threat Protection

At-a-glance

- Multi-layered security for effective defense against known and unknown threats
- Uses a unique, multi-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
- Filtered, on-prem or cloud sandbox analysis for efficient and thorough inspection of truly unknown files
- Prioritized analysis reduces the number of alerts SOC and incident response teams need to address
- Improved ROI by way of fewer appliances and less complexity
- Innovative layered approach to security
- Integration with Symantec and partner ecosystem
- No tradeoff between security and performance

Block, Detect and Analyze Threats with Automated, Advanced Threat Protection at the Gateway

Your enterprise is vulnerable to increasingly sophisticated exploits. Increased exposure requires a new defense that combines prevention with more effective attack detection, analysis, and response.

Symantec™ Content Analysis uses a comprehensive approach to security that offers unequaled protection against known, unknown, and targeted attacks. Paired with Symantec™ ProxySG, Secure Messaging Gateway, Symantec Endpoint Protection, Security Analytics or other third party tools, Content Analysis takes a layered approach to threats targeting network, mail or endpoint traffic. It uses both Symantec and other leading security vendors for whitelisting/blacklisting and file reputation services, dual antimalware engines, machine learning, and deep inspection and detonation through on-box or cloud sandboxing. Together, this fusion of content and malware analysis is the best protection against targeted malware attacks. Protect your organization from viruses, Trojans, worms, spyware, and other malicious content across the network, endpoints or targeting email.

Inline Threat Analysis

Sophisticated attacks come in many forms, designed to avoid detection by siloed, single-purpose blocking tools; no single technology effectively stops all threats. Content Analysis takes a different approach and offers a platform for multi-layered/multi-vendor threat detection and protection to dramatically reduce the number of alerts that SOC and Incident Response teams need to address. By incorporating ProxySG and Secure Messaging Gateway, Content Analysis:

- Blocks known malicious URLs and emails at the gateway
- Leverages Symantec's File Reputation Services (FRS) and conducts extensive whitelist and blacklist scanning
- Analyzes unknown files through advanced machine learning and static code file analysis
- Scans content with dual antimalware engines for greater detection accuracy
- Detonates unknown files via on-box sandboxing, dedicated sandboxes or cloud-based sandboxing
- Integrates with many security tools including Symantec Endpoint Protection to provide endpoint visibility, protection, and response

Symantec File Reputation Services

Content Analysis generates hashes for each file it processes. These hashes are then compared with Symantec's cloud-based File Reputation Services (FRS) classification to identify known files. The service uses reputation scores that indicate whether files are "known" trusted or malicious. Depending on the reputation score, files are then either blocked if malicious, passed to the user if safe, or further processed with anti-virus scanning and sandboxing. Symantec FRS enables crowd sourced security – any file that is detonated in a Content Analysis sandbox by one customer is shared with the FRS service and therefore blocked if that file shows up at another Symantec customer.

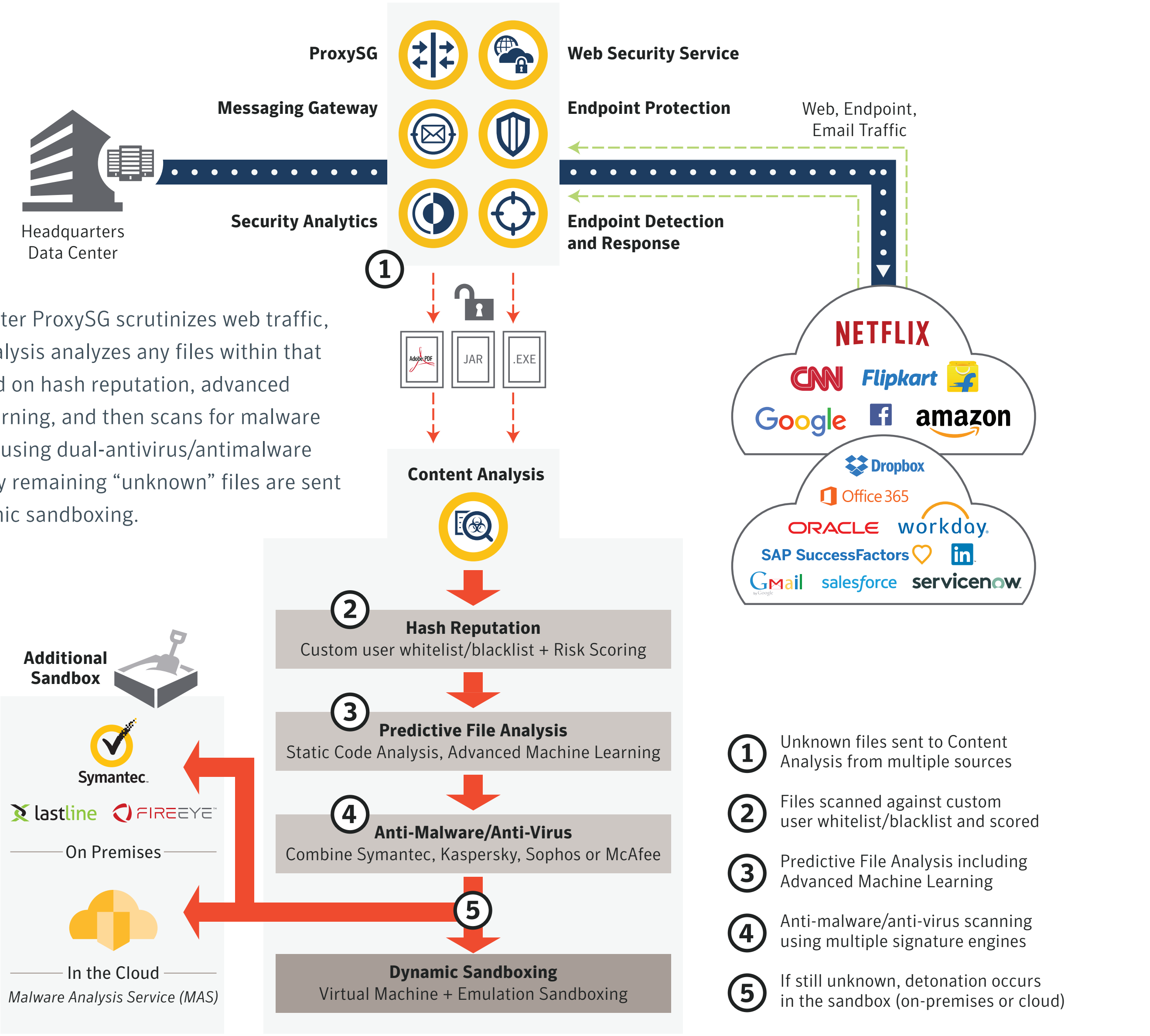


Figure 1: After ProxySG scrutinizes web traffic, Content Analysis analyzes any files within that traffic based on hash reputation, advanced machine learning, and then scans for malware and viruses using dual-antivirus/antimalware engines. Any remaining "unknown" files are sent on to dynamic sandboxing.

1. Unknown files sent to Content Analysis from multiple sources
2. Files scanned against custom user whitelist/blacklist and scored
3. Predictive File Analysis including Advanced Machine Learning
4. Anti-malware/anti-virus scanning using multiple signature engines
5. If still unknown, detonation occurs in the sandbox (on-premises or cloud)

Content Analysis architecture allows Symantec to partner with technology vendors to offer enhanced protection. Leading antimalware engines from Symantec, Kaspersky™, Sophos™, and McAfee® are supported with up-to-the-minute updates, providing better protection than desktop antimalware alone. Up to two antimalware engines can be employed simultaneously to improve detection and blocking. Threat detection engines include:

- Checksum signature matching for known threats
- Command and control behavioral analysis for preemptive detection
- Emulation mode for deep script and executable analysis

Flexible configuration allows both inbound and outbound traffic analysis and includes options such as set time-out duration, drop file if errors in detection occur, real-time sandboxing to prevent patient zeros, and defining trusted sites. Set policies for allow/deny lists, with extensions, along with file size and content type restrictions. Alerts and log files can also be customized. This powerful Advanced Threat Protection at the gateway is available in various deployments to meet the needs of any-sized organization. Options include:

- High-performance hardware to meet the demanding needs of the largest networks
- Optimized virtual appliances to reduce hardware expense, support branch offices, or for deployments in cloud environments like AWS
- Cloud-hosted Web Security and Malware Analysis (sandboxing) Services that deliver industry-leading threat protection

Effectively Combat Advanced Threats

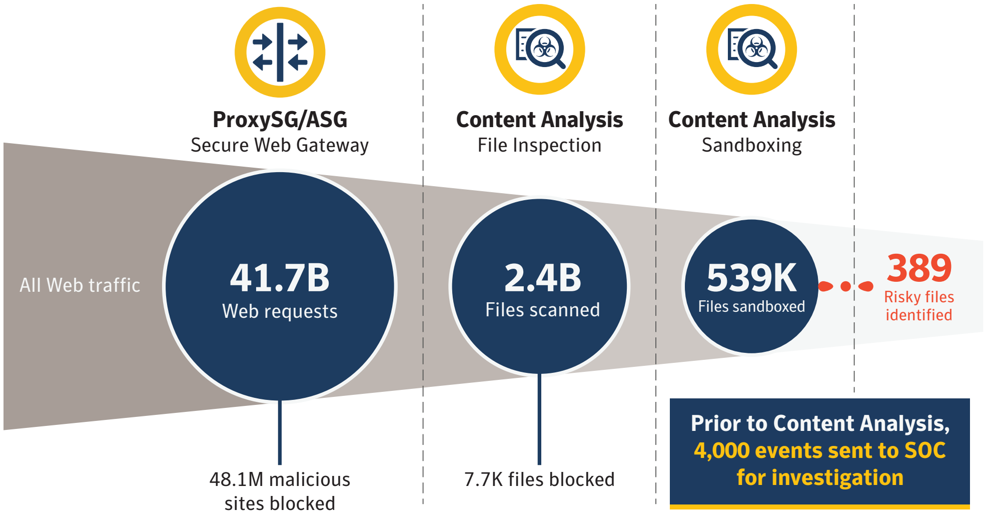
Content Analysis thwarts targeted attacks with threat intelligence from multiple sources, integrated with leading web proxy and email gateway architectures to block malicious web sessions and emails. Traffic is filtered through multiple levels of inspection to stop malware from entering your organization. You will detect and block more exploits, better manage threat analysis—even on the fastest of networks—and reduce false positives. The strongest protection available requires layered, orchestrated technology that only Symantec provides.

Endpoint Integration

Content Analysis integrates with Symantec Endpoint Protection and other endpoint solutions. When sandbox analysis determines a file is malicious, Content Analysis queries the endpoint manager to determine if any workstations in the network have been infected. That information is then included in the report to the administrator and provides the options to add the file hash to a blacklist or run a remediation policy to protect against further infection throughout the organization.

30 Days of actual traffic at Fortune 20 Customer

Figure 2: In this example, Symantec ProxySG and Content Analysis analyzed billions of web requests using a multi-stage process and filtered them down to only a handful of valid alerts that required further investigation by a security team.



Prior to Content Analysis, 4,000 events sent to SOC for investigation

Content Analysis Physical Appliance Options

	CAS S200-A1	CAS S400-A1	CAS S400-A2	CAS S400-A3	CAS S400-A4	CAS S500-A1
Performance						
Throughput*	25Mbps	50Mbps	100Mbps	250Mbps	500Mbps	1000Mbps
System						
Disk Drives	500GB (1 x 500GB)	1TB (2 x 500GB)	1TB (2 x 500GB)	1TB (2 x 500GB)	1TB (2 x 500GB)	6 x 1TB
RAM	6GB	16GB	16GB	32GB	32GB	128GB
Onboard Ports	(2) 1000Base-T Copper Ports (with bypass) (2) 1000Base-T Copper Ports (non-bypass) (1) 1000Base-T Copper, System Management Port (1) 1000Base-T Copper, BMC Management Port	(2) 1000Base-T Copper Ports (with bypass) (1) 1000Base-T Copper Ports (ICAP) (1) 1000Base-T Copper, System Management Port (1) 1000Base-T Copper, BMC Management Port				(2) 10GBase-T Copper Ports (without bypass) (1) 1000Base-T Copper, System Management Port (1) 1000Base-T Copper, BMC Management Port
Optional NICs	4x10/100/1000Base-T (Copper with bypass capability) 4x1GbE Fiber-SR (with bypass capability, full height slot only)	4x10/100/1000Base-T (Copper with bypass capability) 4x1GbE Fiber-SR (with bypass capability, full height slot only) 2x10Gb Base-T (Copper with bypass capability) 2x10Gb Base-T (Copper non-bypass) 2x10Gb Fiber (SR with bypass capability) 2x10Gb Fiber (LR with bypass capability)				
Available Slots	1 full height	1 full height/1 half height				2 full height/4 half height
Power Supplies	1	2 with optional DC Power supported				

*Throughput values are subject to change based on traffic mix, single or dual AV use.

Physical Properties	CAS S200	CAS S400	CAS S500
Dimensions and Weight			
Dimensions (L x W x H)	446.3mm x 440.0mm x 43.5mm (17.57in x 17.32in x 1.71in) (chassis only) 454.5mm x 482.6mm x 43.5mm (17.89in x 19.0in x 1.71in) (chassis with extensions) Note: 640mm L (25.81in L) with optional slide rails	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 with extensions)	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 with extensions)
Form Factor	1 RU height	1 RU height	2 RU height
Weight (max)	Approx. 7.4 kg (16.4 lbs) +/- 5%	Approx. 12.8 kg (28 lbs) +/- 5%	Approx. 30 kg (66.12 lbs) +/- 5%
Operating Environment			
AC Power	100-127VAC @ 6A 200-240V @ 3A, 47-63Hz	Dual redundant and hot swappable power supplies, AC power 100-127V @ 8A 200-240V @ 4A, 47-63Hz	Dual redundant and hot swappable power supplies, AC power 100-240V, 50-60Hz, 12-5A
Maximum Power	350 Watts	450 Watts	1100 Watts
Thermal Rating	Typical: 785 BTU/Hr Max: 1195 BTU/Hr	Typical: 1086 BTU/Hr Max: 1381 BTU/Hr	Typical: 2598.42 BTU/Hr Max: 3751 BTU/Hr
Optional DC Power	Not available	Input voltage range: 40.5V - 57V Input Max Current: 22A Total Output Power: 770W	Input voltage range: 40 - 72 VDC Input Max Current: 30A Total Output Power: 1100W
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 Content Analysis Physical Appliance Models		
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	TP TC 004/2011	TP TC 020/2011
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. Symantec Hardware Support contracts available for 24/7 software support with options for hardware support.	
Gov't Certifications	For further government certification information please contact DL-BC-GROUP-Federal_Certifications@symantec.com	
More Info	Contact regulatorycompliance@symantec.com for specific regulatory compliance certification questions and support	

Content Analysis Virtual Appliance Options

Model	CAS-VA-C4	CAS-VA-C8	CAS-VA-C16	CAS-VA-C32	CAS-VA-C64
Performance*	Up to 100 Mbps	Up to 200 Mbps	Up to 400 Mbps	Up to 800 Mbps	Up to 1600 Mbps
Virtual CPUs	4	8	16	32	64
Virtual Memory	8-16 GB	16-32 GB	32-64 GB	64-128 GB	128-256 GB
Virtual Storage	100GB	100GB	200GB	200GB	200GB
Sandbox Broker	Supported	Supported	Supported	Supported	Supported
On-box Sandboxing**	n/a	n/a	n/a	n/a	n/a
Cloud Sandboxing	Optional	Optional	Optional	Optional	Optional

*Throughput values are subject to change based on traffic mix, single or dual AV use, and the virtual host hardware.

**Content Analysis Virtual Appliances do not support on-box sandboxing. Customers choose to either use cloud sandboxing or deploy an on-premises Content Analysis Appliance with sandboxing license enabled.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, 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 and LifeLock product suites to protect their digital lives at home and across 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**, subscribe to our **blogs**, or connect with us on **Facebook**, **Twitter**, and **LinkedIn**.

Symantec

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