PRODUCT BRIEF

Content Analysis

Advanced, Multi-Layer Threat Protection

AT A GLANCE

- Multi-layered security for effective defense against known and unknown threats, and a critical component of a complete Secure Access Service Edge (SASE) solution
- A key component of Symantec Web Protection for deep file inspection
  - Quickly analyzes suspicious files and URLs, interacts with running malware to reveal its complete behavior, and exposes 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 must address
- Deployed on the same hardware as Symantec Edge SWG, as a VM, or in the cloud for improved ROI and flexibility
- Integrates with Symantec and partner ecosystem

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

Enterprises are 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 is a critical component that is included with Symantec Web Protection. Content Analysis uses a comprehensive approach to security that offers unequaled protection against known, unknown, and targeted attacks. Paired with Symantec Secure Web Gateway (SWG), Secure Messaging Gateway, Symantec Endpoint Security, Security Analytics, or other third party tools, Content Analysis takes a layered approach to threats targeting network, mail, or endpoint traffic. Content Analysis uses Symantec multi-layered detection for allow list/block list and file reputation services, antimalware detection, 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. Content Analysis is designed to protect organizations 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 Symantec SWG and Secure Messaging Gateway, Content Analysis provides the following services:

- Blocks known malicious URLs and emails at the gateway
- Leverages Symantec File Reputation Services (FRS) and conducts extensive allow list and block list scanning
- Analyzes unknown files through advanced machine learning and static code file analysis
- Scans content with the Symantec multi-layered inspection engine for greater detection accuracy
- Detonates unknown files through sophisticated sandboxing
- Integrates with many security tools including Symantec Endpoint Security to provide endpoint visibility, protection, and response

ENDPOINT INTEGRATION

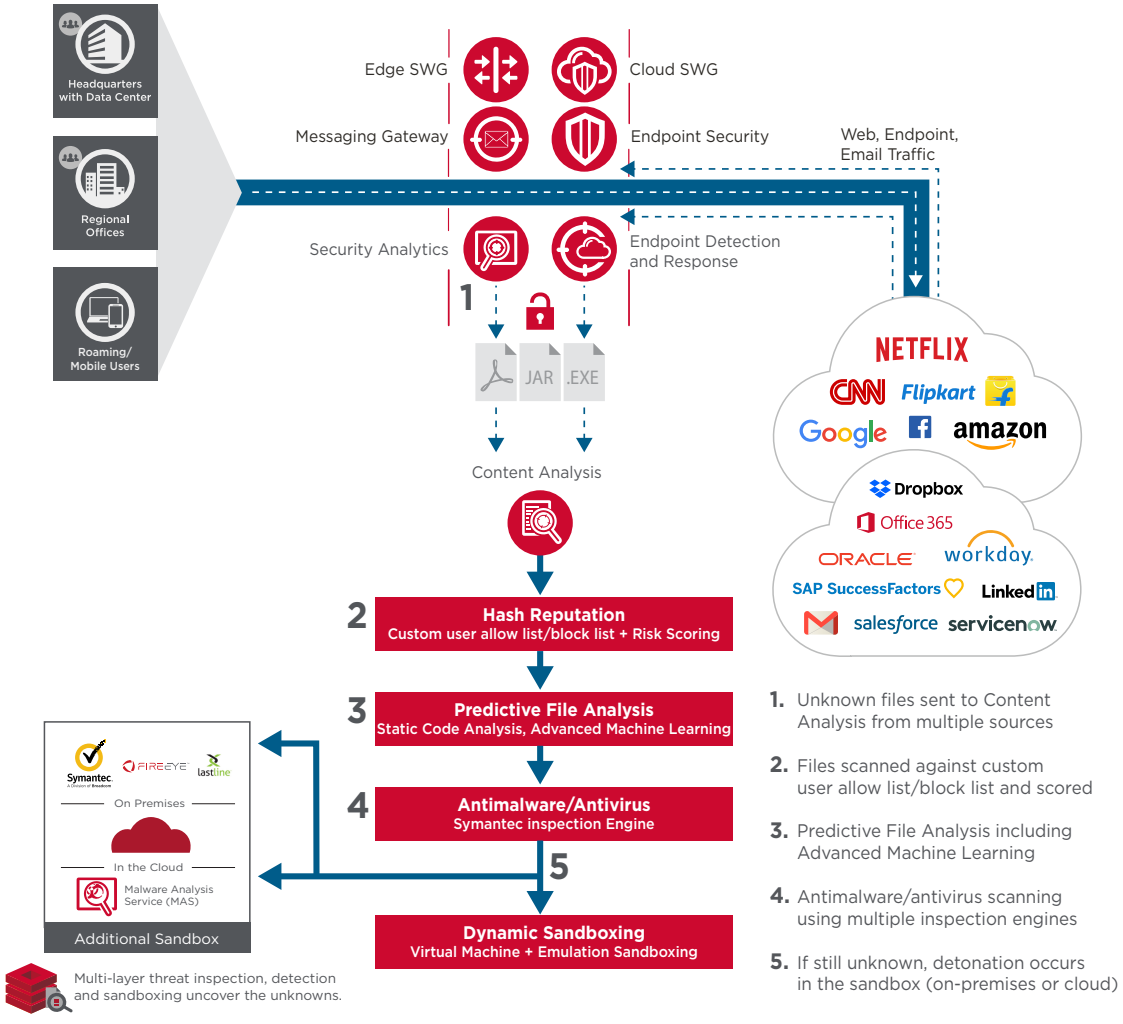
Content Analysis integrates with Symantec Endpoint Security and other endpoint solutions. When sandbox analysis determines a file is malicious, Content Analysis queries the endpoint manager to determine if any workstations in the network have been infected. That information is then included in the report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

Multi-layer Threat Inspection Architecture

Content Analysis architecture allows Broadcom to partner with technology vendors to offer enhanced protection. Leading antimalware engines 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 these integrated features:

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

Figure 1: After Edge or Cloud SWG 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 the Symantec multi-layered inspection engine. Any remaining unknown files are sent on to dynamic sandboxing.



SYMANTEC FILE REPUTATION SERVICES

Content Analysis generates hashes for each file it processes. These hashes are then compared with the Symantec 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 antivirus 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.

Flexible Configuration Options

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 as part of Symantec Web Protection at no additional charge, with the following deployment options:

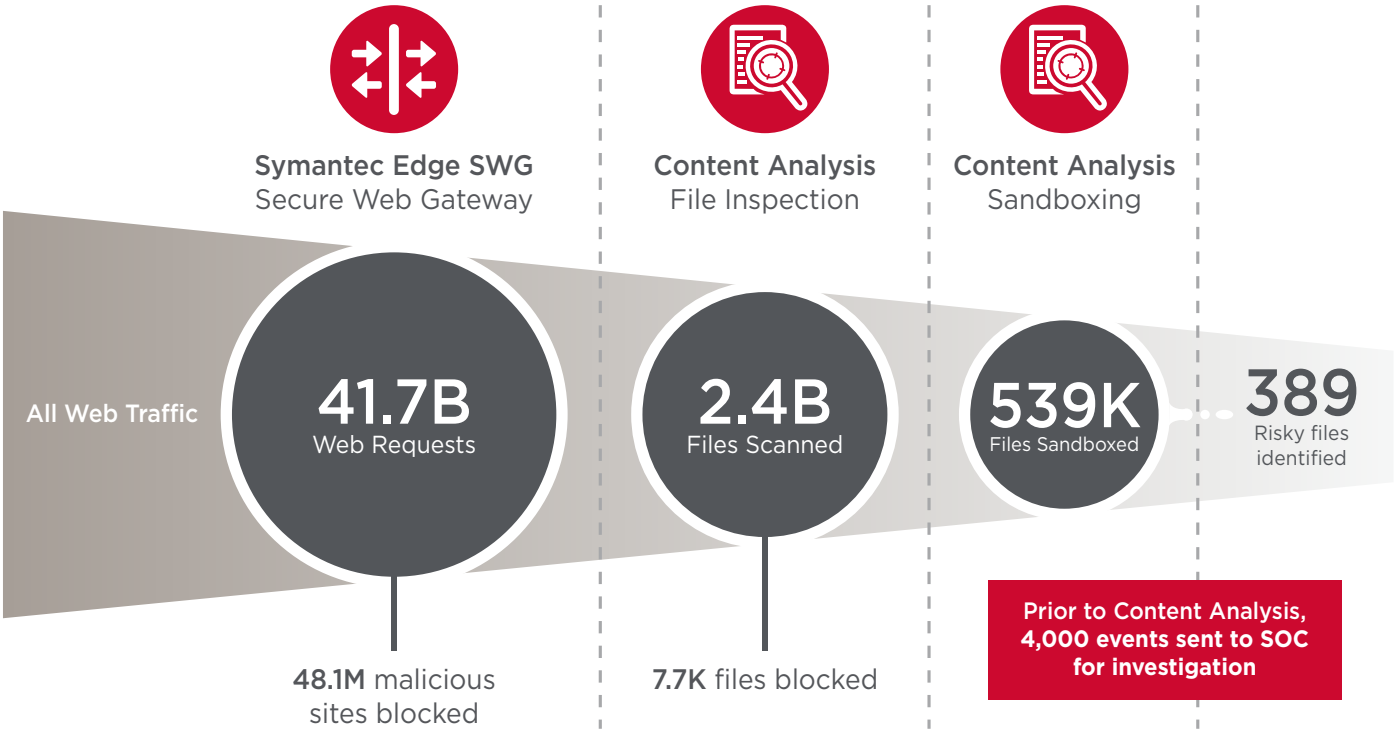
- High-performance hardware to meet the demanding needs of the largest networks
- Optimized virtual appliances to reduce hardware expense, support branch offices, or for deployments in cloud environments like AWS
- Cloud-hosted Secure Web Gateway and Deep File Inspection (Sandboxing) Services that deliver 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. 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.

Thirty Days of Actual Traffic at a Fortune 20 Customer

Figure 2: In this example from a real customer, Symantec Edge SWG 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.



Content Analysis Physical Appliance Options

Content Analysis can be deployed on the same Secure Web Gateway appliances as Symantec Proxy.

Secure Web Gateway Appliances	SSP-S210-10	SSP-S410-20B	SSP-S410-40B
Platform Specifications			
System			
CPU	*1 x 16 core 2.0 GHz C3958 Atom*	*2 x 10 core 2.2 GHz 4210 Cascade Lake*	*2 x 20 core 2.1 GHz 6230 Cascade Lake*
Memory	*64 GB (DDR4 SDRAM)*	*96 GB (DDR4 SDRAM)*	*384 GB (DDR4 SDRAM)*
Storage SSD	*2 x 960 GB*	*2 x 960 GB*	*2 x 1.9 TB*
Boot Drive (SATA)	*2 x 64 GB*	*2 x 64 GB*	*2 x 64 GB*
Power Supply	*2 x 300W*	*2 x 1200W*	*2 x 1200W*
Network Interface - Data	*4-port 1GbE Copper*	*2 X 2-port 10GbE Copper*	*2 X 2-port 10GbE Copper*
Network Interface - Management	*1GbE Copper*	*1GbE Copper*	*1GbE Copper*
Optional Network Interface Cards	*Quad Port 10GbE Copper (with bypass capability), Quad Port 1GbE Copper (with bypass capability), Quad Port 10GbE Fiber (LC, with bypass capability), Dual Port 10/25GbE Copper*		
Rack Specifications			
Shipping Dimensions and Weight			
Width	*580 mm/22.83 in.*	*610 mm/24.01 in.*	*610 mm/24.01 in.*
Overall Depth	*925 mm/36.42 in.*	*995 mm/39.17 in.*	*995 mm/39.17 in.*
Height (on Pallet)	*245 mm/9.65 in.*	*290 mm/11.41 in.*	*290 mm/11.41 in.*
Shipping Weight (Approximate)	*17.8 kg/38.14 lb*	*26 kg/57 lb*	*26 kg/57 lb*
Appliance Dimensions and Weight			
Width	*438 mm/17.24 in.*	*483 mm/19.01 in.*	*483 mm/19.01 in.*
Overall Depth	*471 mm/18.55 in.*	*826.8 mm/32.55 in.*	*826.8 mm/32.55 in.*
Height (One Rack Unit (RU) with Casters)	*43.5 mm/1.71 in.*	*43.5 mm/1.71 in.*	*43.5 mm/1.71 in.*
Appliance Weight (Approximate)	*9.02 kg/19.88 lb*	*22 kg/48.5 lb*	*22 kg/48.5 lb*
Operating Environment			
Main Input Power - PDU	*Dual 100–240 VAC, ~/4A, 50 to 60 Hz*	*Dual 100 to 240 VAC, 7.08A, 47 Hz to 63 Hz*	*Dual 100 to 240 VAC, 7.08A, 47 Hz to 63 Hz*
Facility Power Interface	*Type B, 5-15R, 120 VAC*	*Type B, 5-15R, 120 VAC*	*Type B, 5-15R, 120 VAC*
Power	*300W (Max.)*	*1200W (Max.)*	*1200W (Max.)*
Thermal Rating (Maximum)	*1025 BTU*	*4096 BTU*	*4096 BTU*
Operating Temperature	*0°C to 40°C/32°F to 104°F*	*0°C to 40°C/32°F to 104°F*	*0°C to 40°C/32°F to 104°F*
Non-operating Temperature	*–20°C to 70°C/–4°F to 158°F*	*–40°C to 70°C/–40°F to 158°F*	*–40°C to 70°C/–40°F to 158°F*
Operating Relative Humidity	*20% to 95% RH*	*20% to 85% RH*	*20% to 85% RH*
Non-operating Relative Humidity	*10% to 95% RH*	*10% to 85% RH*	*10% to 85% RH*
Operating Altitude	*3,000m*	*3,000m*	*3,000m*
Non-operating Altitude	*12,000m*	*12,000m*	*12,000m*

Content Analysis Physical Appliance Options (cont.)

Secure Web Gateway Appliances		
Regulations	**Safety**	**Electromagnetic Comp**
International	*UL: UL 60950 1, 2nd Edition cUL: CAN/CSA C22.2 No. 60950 1 07, 2nd Edition CB: IEC 60950 1:2005 +A2:2013+ Summary with National Differences: EN 60950 1:2006+A2:2013*	*CISPR22:2008 Class A; CISPR32 Class A*
USA	*UL: UL 62368 1, 2nd Edition*	*FCC part 15, Class A /ANSI C63.4 2014*
Canada	*cUL: CAN/CSA C22.2 No. 62368 1 14, 2nd Edition*	*ICES-003, Issue 6 Class A / CAN/CSA CISPR 22 10*
European Union (CE)	*CB: IEC 62368 1:2014 (Second Edition) Summary with National Differences: EN 62368 1:2014+A11:2017*	*EN 55011, EN 61000 6 3, EN 55032, CISPR 32, Class A EN 61000 3 2 / EN 61000 3 3, EN 55024 / EN 61000 6 1, EN 61000 4 2 / EN 61000 4 3, EN 61000 4 4 / EN 61000 4 5, EN 61000 4 8 / EN 61000 4 11*
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-CISPR32, AN/NZS CISPR 32:2015 + C1:2016 ED.2.0*
Korea	—	*KC – RRA, Class A, KN32/KN35, KN61000 4 2 / KN61000 4 3, KN61000 4 4 / KN61000 4 5, KN61000 4 6 / KN61000 4 11*
Russia	*EAC - TP TC 004/2011*	*EAC - 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. Support contracts available for 24/7 software support with options for hardware.*	

BROADCOM®
connecting everything®

For more information, visit our website at: www.broadcom.com

SED-Cont-Analysis-PB104 April 3, 2024