SOLUTION BRIEF

Content Analysis

Block known threats with advanced threat protection at the gateway

A New Approach for Advanced Threat Protection

A new breed of hackers—including cyber criminals, nation states, hacktivists, and insiders—is perpetrating increasingly sophisticated, targeted, and effective exploits on enterprises. This shift in the threat landscape requires a new defense that combines threat prevention with more effective attack preparedness, detection, and response, across web, email and mobile devices.

Companies have a gap between their ongoing operations, where they detect and block known threats, and incident containment, where they analyze and mitigate zero-day threats and advanced or unknown malware. This gap exists because traditional malware analysis technologies cannot operationalize new threat intelligence discovered during incident containment across the security infrastructure.

This silo style of defense inhibits the ability of the organization to continually fortify its defenses. An integrated approach—analyzing advanced targeted attacks, zero-day threats, and unknown malware, then providing that intelligence back to threat intelligence networks continually strengthen defenses—is imperative. The advantage is immediate inoculation against all new threats.

Symantec: Bridging the Incident Containment Gap

Content Analysis, with it's multi-layer file inspection and sandboxing is a critical component of effective protection against advanced targeted attacks. Together with ProxySG or Symantec Messaging Gateway, it offers the most complete advanced threat protection in the marketplace for blocking known threats and analyzing zero-day and other advanced threats.

This solution blocks all known threats through inspection of sources and signatures and can centrally analyze unknown content locally and worldwide, leveraging Symantec's Global Intelligence Network. This community-watch effect constantly fortifies your security.

Zero-day threats are escalated automatically within Content Analysis to powerful, dual-detection sandboxing technology. This offers a unique hybrid analysis protocol, including the customizable IntelliVM virtualized sandbox to replicate production environments, and a bare-metal sandbox emulator for accurate analysis and detection of VM-evasive malware. File filtering by Content Analysis mitigates false positive identification of malware and it significantly improves sandbox efficiency by reducing the number of files unnecessarily sent for analysis.

Unlike other sandboxing solutions, information derived from the analysis of malware files is automatically shared with the ProxySG appliances and Content Analysis, so future instances of the malware will be blocked at the gateway.

The solution is powered by the Symantec Global Intelligence Network, informed threat data from more than 70 percent of the Fortune Global 500. The discovery of new malware, threats, or malicious files is shared both locally within your infrastructure, and out through this global community for faster protection against advanced malware and attacks targeting your web, email or mobile environment.

Symantec delivers advanced threat protection at the web and mail gateway with the following products:

- **Symantec ProxySG:** A web security gateway providing complete control over all your web traffic.
- **Symantec Messaging Gateway:** An advanced threat protection and antispam solution for on-premises messaging environments.

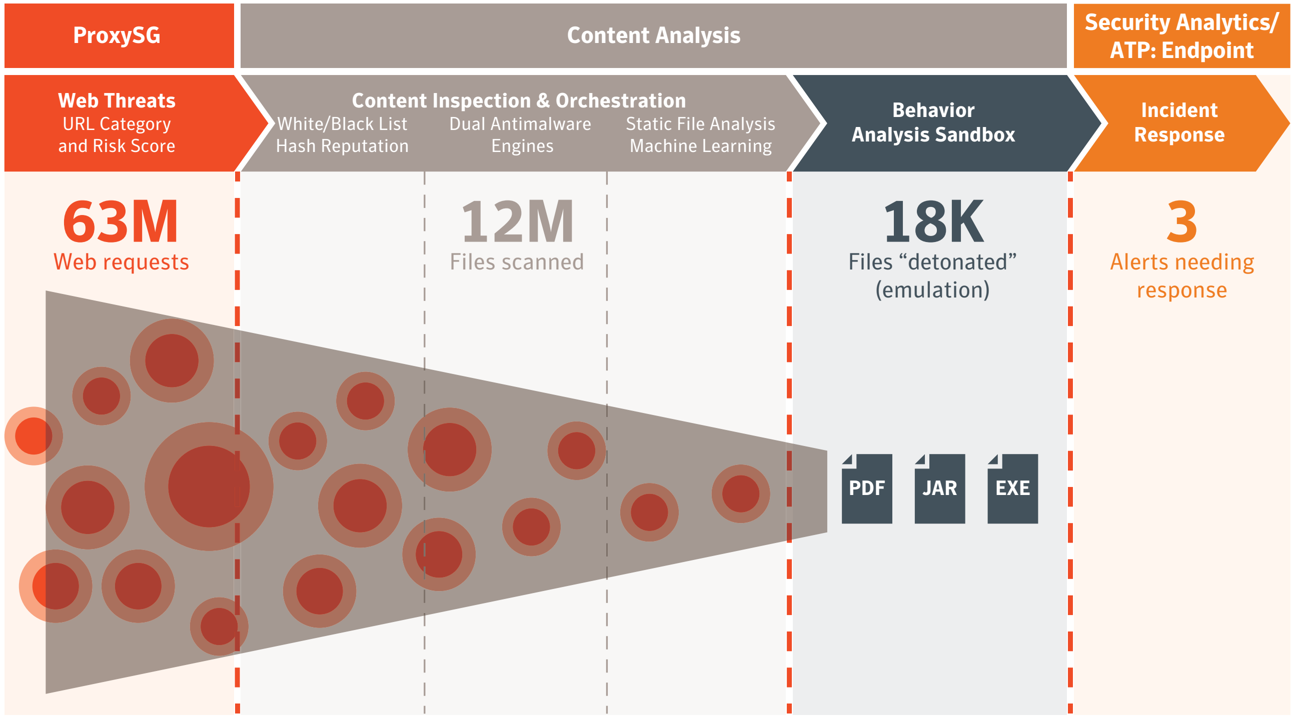
Symantec™ ProxySG and **Symantec Content Analysis** bridge the gap between real-time blocking of known threats and incident containment through the analysis and mitigation of unknown threats. The net result: your employees can access their data anywhere they are, fully confident that it's protected.

With the foundation of Symantec ProxySG and Content Analysis you can:

- Block known web and email threats
- Allow known good files
- Block known bad files
- Analyze unknown threats, even those targeting mobile devices
- Update the Global Intelligence Network to protect against future attacks

- **Symantec Content Analysis:** This flexible system provides real-time malware scanning with up to two malware signature databases and file whitelisting and blacklisting. It also acts as a broker for Symantec and third-party sandboxing engines.
- **Symantec Malware Analysis:** Now built directly into Content Analysis, this highly customizable sandboxing engine combines a virtualized environment and a bare-metal emulator to detect unknown malware and zero-day threats in an environment that replicates the systems on your network. This sandboxing can run on the same appliance as Content Analysis, as a stand-alone appliance or as a cloud service.
- **Symantec Global Intelligence Network:** A collaborative defense that turns 175 million endpoints and 50 million users into a global community watch against bad actors, processing eight billion security requests daily. Combined with the support of 1000 cyber warriors in nine centers around the world, it provides an ever-vigilant response.

Effectively Combating Advanced Threats


ProxySG
Content Analysis
Security Analytics/ ATP: Endpoint
Web Threats
URL Category and Risk Score
Content Inspection & Orchestration
White/Black List Hash Reputation
Dual Antimalware Engines
Static File Analysis Machine Learning
Behavior Analysis Sandbox
Incident Response
63M
Web requests
12M
Files scanned
18K
Files "detonated" (emulation)
3
Alerts needing response
PDF
JAR
EXE

Multiple-layered threat analysis and detection identifies and blocks more threats and reduces the number of files that need true sandbox analysis and ultimately the number of incidents that need actual response (example results from one day of an actual customer's web traffic).

Summary: Benefits and Advantages

Symantec brings together the full range of products, services, and technologies to deliver advanced threat protection at the web gateway. The table on the right summarizes its business advantages.

Benefit	Advantage
Scalable, effective defense against advanced targeted attacks, advanced persistent threats, and zero-day malware	Up-to-the-minute threat intelligence is collected from our millions of users to identify unknown threats and shift protection to the gateway.
Defense in depth against advanced threats	At the web and mail gateways, combine real-time blocking and malware scanning, with URL and file whitelisting/blacklisting, static code analysis, and dynamic malware detonation.
More complete detection of zero-day threats	A customizable IntelliVM virtualized sandbox and a bare metal sandbox emulator deliver more accurate analysis and detection of VM evasive malware.

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 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