# Content Analysis

## Block Known Threats with Advanced Threat Protection at the Gateway

**With the Blue Coat ProxySG appliance and Symantec Content Analysis, you can 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 business can move beyond fear and start focusing on possibilities. With the Symantec Advanced Threat Protection solution you can:**

- **Block known web threats**
- **Allow known good files**
- **Block known bad files**
- **Analyze unknown threats**
- **Update the Global Intelligence Network to protect against future attacks**

## A New Approach for Advanced Threat Protection

A new breed of hackers – including cybercriminals, 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 prevention with more effective attack detection, preparedness, and response.

Today, enterprises 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. The new strategic imperative for enterprises demands an integrated approach that can analyze advanced targeted attacks, zero-day threats, and unknown malware and provide that intelligence back to continually strengthen prevention defenses. The advantage for enterprises is immediate inoculation against all new threats.

## Symantec: Bridging the Incident Containment Gap

The Content Analysis combined with the Symantec Malware Analysis are critical components of the Symantec Advanced Threat Protection solution. This combination, together with the ProxySG appliance, offers the most complete ATP solution in the marketplace for blocking known threats and analyzing day-zero and other advanced threats.

As part of ongoing security operations, ProxySG and Content Analysis (with malware scanning and whitelisting) can block all known threats, sources and signatures and centrally analyze unknown content. The threat intelligence is shared locally between ProxySG and the Content Analysis as well as globally through the Global Intelligence Network to continuously fortify the security infrastructure.

Zero-day threats are automatically escalated and brokered by Content Analysis to Malware Analysis with dynamic sandboxing technology. This offers a unique hybrid analysis solution 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 the problem of 'false-positive' identification of malware, and improves sandbox efficiency by reducing the number of files sent for analysis by 37%.

Symantec™

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, which provides a network effect of valuable threat data from our customers, including over 70% of the Fortune Global 500. The discovery of new malware, threats or malicious files is shared locally within your infrastructure and out through this global community for faster protection against advanced targeted attacks and zero-day malware.

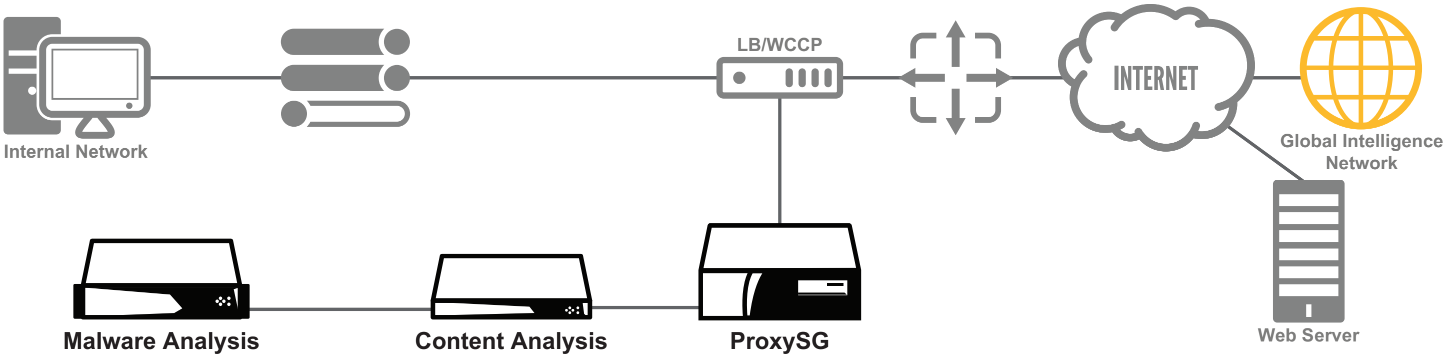
Symantec delivers advanced threat protection at the web gateway with the following products:

- **Blue Coat ProxySG**: The industry-leading web security gateway provides complete control over all your web traffic.
- **Symantec Content Analysis**: This flexible system provides real-time malware scanning with up to two malware signature databases and file whitelisting. It also acts as a broker for Symantec and third-party sandboxing engines.
- **Symantec Malware Analysis**: This highly customizable malware analysis solution 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.
- **Symantec Global Intelligence Network**: A collaborative defense that collects and analyzes over a billion previously uncategorized new web requests a day and shares that analysis with our 15,000 customers and their millions of users.

## Summary: Benefits and Advantages

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

| | |
|---|---|
| **Scalable, effective defense against advanced targeted attacks, APTs and zero-day malware** | New threat intelligence is shared locally across the security infrastructure and globally our 15,000 enterprise customers and their millions of users to turn unknown threats into known threats and shift protection to the gateway. |
| **Defense in-depth against advanced threats** | At the web gateway, combine real-time blocking and malware scanning, with application whitelisting and dynamic malware analysis |
| **More comprehensive 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. |




Symantec Content Analysis bridges the gap between prevention and incident containment.

## 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.