Top Four Reasons To Migrate To The Content Analysis System

Step Up Advanced Threat Protection

Customers who purchased Blue Coat ProxyAV appliances received solid protection against web-based threats. But advanced threats continue to evolve and proliferate. Today more than 200,000 new malware samples are uncovered every day. CIO magazine reports that there are more than one million malicious and high-risk Android apps. Add to that the growing sophistication of targeted attacks and advanced persistent threats, and it is clear that traditional anti-malware alone is no longer enough.

What's needed is a deeper, more comprehensive defense that not only blocks the "known bad" but also protects against "unknown" zero-day threats and allows access to the "known good." Symantec Content Analysis delivers all of this critical functionality while also harnessing intelligence from millions of actual users. It gathers, analyzes, and shares actionable intelligence with Blue Coat ProxySG appliances, the Symantec Security Analytics solution for real-time threat profiling and remediation, and the Symantec Global Intelligence Network. The result is a new dimension of protection against advanced threats – and a new level of empowerment for your workforce and your business.

Four Great Reasons to Deploy the Content Analysis System

1 Get More Accurate, Complete Protection through Dual Anti-Malware Engines

Tests show that adding a second anti-malware engine results in a 12% increase in malware capture. The most complete coverage can be achieved with two engines on the perimeter and an engine from a third vendor on endpoint devices. That is why Symantec Content Analysis provides the option to use one or two anti-malware engines from anti-malware industry leaders (Kaspersky, Sophos, McAfee).

As a dedicated device, Content Analysis also scans all files at full throughput. Other solutions may claim high levels of anti-virus scanning throughput but ignore content they determine to be "safe" such as Facebook. Multi-purpose next generation firewall and unified threat management devices show a sharp drop in performance as anti-malware features are turned on.

2 Improve Control and Performance through File Whitelisting

Content Analysis provides "file whitelisting," which accelerates access to "known good" files and also boosts the performance of anti-malware scanning. Specifically, Content Analysis accesses a whitelist database of more than a billion files, and this database is updated continuously. When a user requests a file, Content Analysis checks against this database and delivers it to the requester if it's on the list. This increases the performance of anti-malware scanning and sandboxing by eliminating the need to analyze known good files. In fact, laboratory tests show that 29% of files entering Content Analysis will be classified as "good" by the whitelist. The whitelisting feature also provides the option to improve security even further by preventing users from downloading specific file datatypes of downloads that are not on the whitelist. A good example would be blocking any .exe files that are not known good files.

Symantec

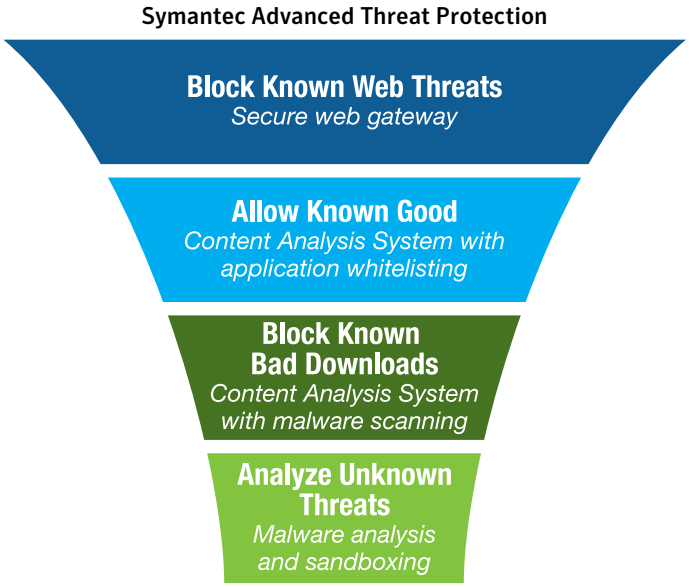
3 Boost Performance and Accuracy through Orchestrated Sandboxing

Content Analysis serves as a broker between multiple sandboxes, simultaneously sending unknown or suspicious files to the Symantec Malware Analysis sandbox and third-party sandboxes. And, laboratory tests show that with the implementation of dual anti-malware engines and file whitelisting, the number of files sent to the sandbox is reduced by 37%. As a result, there are fewer false-positives and improved sandbox performance as fewer files need to be processed. The sandbox orchestration capability allows you to optimize your existing investments while building modern, defense-in-depth protection against advanced and zero-day malware. Content Analysis provides the option to improve performance and accuracy even further by allowing the selection of file datatypes to be sent to the sandbox for analysis.

4 Protect Your Business and Your Investments with an Expandable Solution

The high-performance Content Analysis is built for expansion. It provides the performance and defense-in-depth you need for today's threat landscape without needlessly slowing the end-user experience. It handles the processing load needed for file scanning, protecting the ProxySG Secure Web Gateway from any impact due to spikes in new file downloads. The six current models, including a virtual model, have throughput ranging from 25Mbps to 1Gbps, letting you choose the right device for your network. It can scan files up to 5GB in size and analyze compressed archives up to 99 layers deep. When files are properly unpacked, Content Analysis gains the ability to reveal malicious content that may have been intentionally hidden, exposing intended behavior.

In addition, a best-of-breed strategy allows Symantec to partner with visionary security vendors to offer superior protection. Over time new features will be made available, including on-box and cloud-based sandboxing.



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