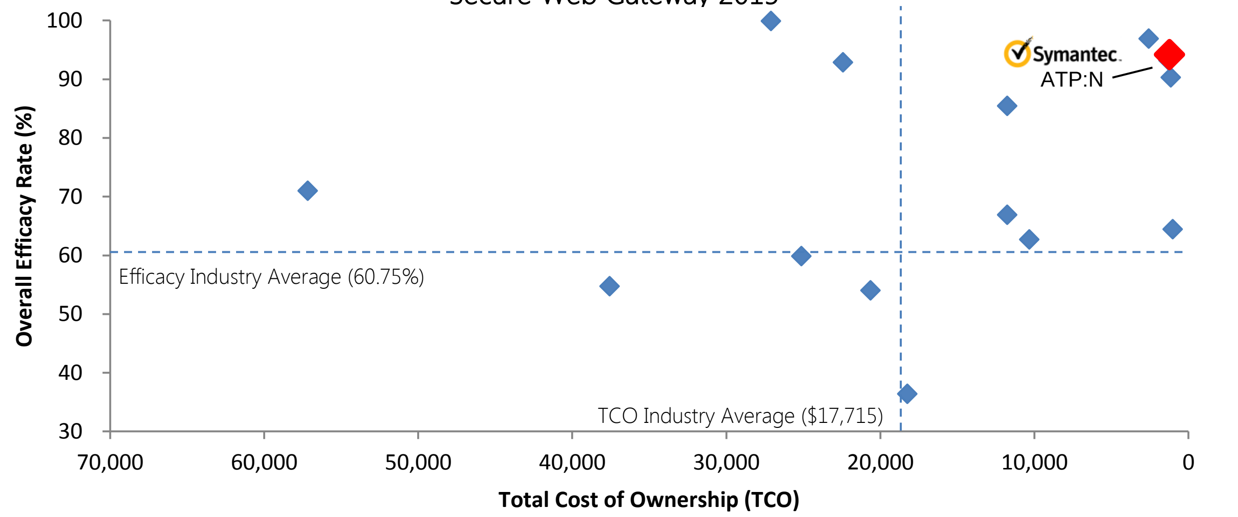
Symantec Advanced Threat Protection: Network

The Symantec Advanced Threat Protection: Network is a solution that detects malicious content within a network by utilizing its global intelligence to monitor threat activity in over 150 countries, and its intrusion detection system to notify of unauthorized or unusual access events. The Insight reputation-based security technology relies on advanced data mining to seek out mutating code and encryption to identify the latest threats. All threats are categorized to evaluate more accurate malware detection.

Impact Analysis Grid™
Secure Web Gateway 2015



Source Miercom Secure Web Gateway Industry Assessment 2015

Buyer Considerations

The Symantec Advanced Threat Protection: Network would be an investment for any company to consider. Its ability to block malware gave it a rating of 90.3% which is well above the industry average and the price of the product well below the average cost for products in its class.

Miercom Industry Assessment Impact Analysis Grid™ SWG 2015

Data collected from both individual product reports and comparative reports are used to create the Impact Analysis Grid™ for Miercom's 2015 Secure Web Gateway Industry Assessment.

The Impact Analysis Grid™ presents a visual evaluation of the relationship between effectiveness and value of security products over the course of one year. Each quadrant illustrates a characteristic based on the amount of effectiveness relative to cost projected of tested products, enabling enterprises to assess their purchase options based on their needs and budget.

Performance/Efficacy Score

The performance and efficacy score are averages formed by taking the total number of blocked malware sample sets and the total number of malware sets. This average shows the overall performance in SWG testing.

Total Cost of Ownership Evaluation

Using the Total Cost of Ownership (TCO), instead of the product purchase price, allows us to factor in the costs of managing and maintaining the product. Factors that were considered in the TCO were installation, maintenance, upkeep and tuning of the device. This information was used to calculate the cost of security over a one year licensed with 100 users. The benefits of this analysis are that within a given range of performance, additional insight is provided as to where the product falls within the average of its competitors.

What We Tested

Malicious software, or "malware", is any software used to disrupt computer or network operations, gather sensitive information, or gain access to computer systems. Legacy malware can be in circulation anywhere from a month to several years, while other malware utilizes techniques that adapt to networks or computers vulnerabilities.

Miercom used sample sets, developed in cooperation with numerous security professionals and experts, to create a realistic environment to test the security appliance.

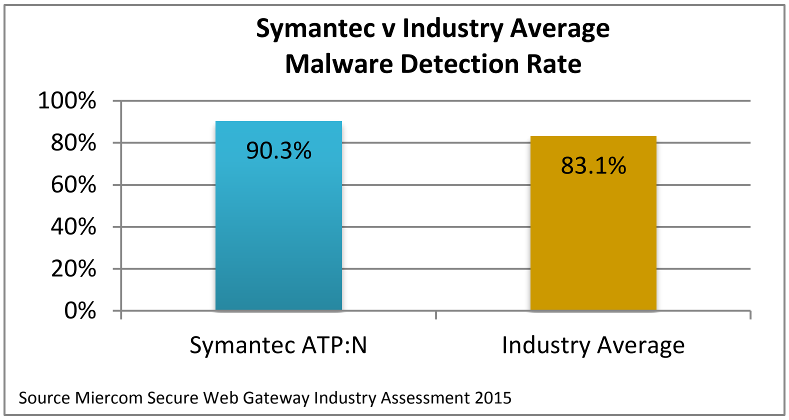
The Symantec ATP:N was significantly below the industry average in cost of products in the same class.

About the Sample Set

The threat samples were independently collected from various research sources, including threats validated and collected by and saved in a network of honeypots and malware analysis servers. Both automated and manual analysis of the samples was performed and only samples that achieved a consistent composite score of malicious rating across all the analysis methods were included in the test.

A significant amount of effort manually and automated processes went into the validation of the samples used. The manual verification was done using bare-metal server analysis. The samples were also tested utilizing several hundred combinations of user agent (UA) strings in an effort to verify consistent delivery of malware code and/or payloads.

Results v Industry Average



Symantec v Industry Average
Malware Detection Rate

Source Miercom Secure Web Gateway Industry Assessment 2015

The Symantec Advanced Threat Protection: Network Appliance was 7.2% better than the industry average in malware detection.