Advanced Threat Protection

DR151026D
December 2015

Miercom
www.miercom.com

Contents

Executive Summary

Miercom conducted an independent third party validation of the Symantec Advanced Threat Protection appliance, as well as the Cisco SourceFire and the FireEye 1310 products.

Security Effectiveness testing verified the detection and blocking of multiple malware threats including, legacy, Advanced Evasion Techniques, Advanced Persistent Threats, BotNet, RATs, active threats and malicious documents.

The Symantec ATP solution demonstrated its ability to detect the different types of malware threats. When compared to products of competing vendors, the Symantec ATP solution performed at least 18% better than both contenders, with well above average strengths in protection against six of the seven categories of malware.

Key Findings

- Malware detection rate of Symantec ATP was 18.5% higher than that of its competitors
- Scored 100% detection against Advanced Evasive Techniques, the most complex threats to date – identifying 95% more than competing vendors
- Reporting console has a timeline view for easy tracking of dated and categorized malicious events

We were pleased with the performance of the Symantec ATP solution for detecting malware, particularly its ability to effectively detect and remove not only the most common but even the unknown malware threats as well.

Robert Smithers
CEO
Miercom

Overview

Many of the security issues today are related to why and how malware manages to get through security defenses. One reason is that much of this malicious content is constantly changing in an attempt to evade signature-based antivirus and static security gateway and firewall technologies.

This report shows how the Symantec ATP solution performed when presented with some of the most sophisticated, currently active malware. The results outlined in this document represent the level of detection of several categories by Symantec ATP, Cisco SourceFire Intrusion Prevention System and FireEye Security Appliance for a competitive comparison.

Symantec ATP

This network security solution can be deployed using a hardware appliance or, in the case of this test, virtually using VMware ESXi 5.5. It is quickly deployed in an enterprise setting and provides protection against live threats using the following proprietary tools:

- Symantec Cynic, a malware analysis service that runs potentially malicious files through multiple layers of inspection to detect advanced threats and zero-day exploits
- Symantec Insight, a reputation-based technology to identify suspicious files based on history and prevalence
- Symantec Vantage, a technology to scan network traffic to detect exploits, malicious files, network attacks, and to identify actively infected endpoints in the environment
- Symantec DeepSight, an intelligence service which provides relevant information regarding observed events

Symantec ATP is intended to quickly gather suspicious file or URL data, categorize it, and offer visual investigations for security analysts to quickly remediate network vulnerabilities for a safer, more secure enterprise. These tools are used within the testing of this solution, and the results of real-world attacks in a simulated enterprise environment are provided here.

Methodology

The test approach of this threat detection assessment was based on the Miercom general security testing methodology for devices blocking malicious content from entering a network.

Security Functionality Assessment

The Symantec ATP product was evaluated for the following:

Function	Description	Rubric
Detection	Ability to identify known/legacy threats	Percentage

Products Tested

Symantec threat detection efficacy was part of a competitive study against the following security products:

Symantec **Advanced Threat Protection**	**Cisco Sourcefire** **Intrusion Prevention System**	**FireEye** **Security Appliance**
Version 2.0.0.58	Version 5.4	Version 7.5.1
• Symantec Cynic malware detonation and global intelligence to detect malicious content within a network • Symantec Vantage network intrusion detection • Symantec Insight reputation-based security technology to signal unknown and active threats • Symantec DeepSight inbound traffic scanner to detect endpoint vulnerability	• Continuous capabilities to monitor, store and recall malware that evades initial detection • Visibility of type, threat level, and behavior of malware attempting to enter • Investigations lead to enhanced intelligence for further improvements on system recovery for subsequent attacks	• Catches threats missed by firewalls, anti-virus, web gateways and intrusion prevention systems • Prevents data theft and botnets from outbound traffic • Applies several techniques for inbound, multi-phase inspections • Equipped with false-positive analysis for real-time processing, continuously expanding database of active threats and prevents phishing via email

Security Threat Samples

Malicious software, or malware, is any software used to disrupt computer or network operations, gather sensitive information, or gain access to computer systems. These samples were obtained from Miercom's honeypot, consisting of real and intricate malware developed for the purpose of this test. Although legacy samples were included in the set, the focus was on the detection of the most recent and advanced samples.

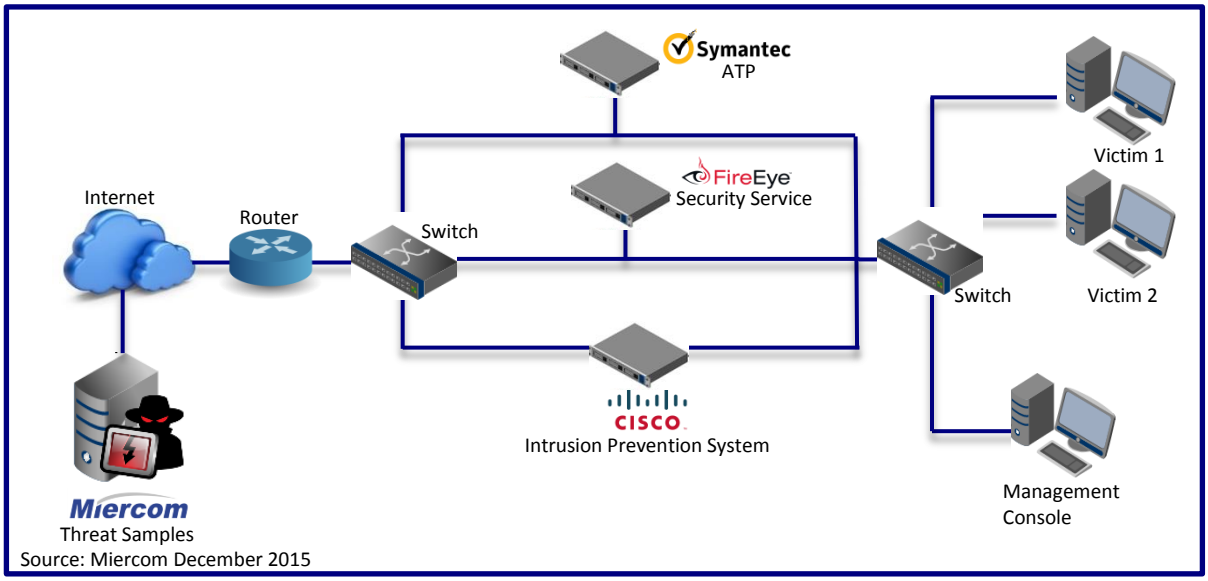
Active Threats	A constantly changing, unknown malware from external resources and private honeypots. These custom crafted, undetected samples and APTs have undergone AV evasion techniques such as encryption, black packaging, and payloads using normal traffic.
Advanced Evasive Techniques (AETs)	A network attack combining several known evasion methods to create a new attack delivered simultaneously over several layers. Its code is not necessarily malicious, but the danger the elusive attack whose access is undetectable. Currently, there are about 200 known evasion techniques recognized by vendor products. An AET can create millions of new evasion techniques from just a few combinations.
Advanced Persistent Threats (APTs)	A set of stealthy and continuous computer hacking processes, often orchestrated by humans targeting a specific entity. This malware usually attacks organizations or nations for business or political motives. An APT may consist of a staged payload that, when activated, allows an attacker to obtain shell access remotely via command line. These payloads are masked with randomization and evasion techniques to bypass AVs. The known APT samples used in our testing were sourced from multiple sources.
BotNet	A collection of interconnected, communicating programs which use a technique known as Command and Control. An intermediary receives orders or command attacker and are then forwarded to all infected hosts. Botnets are commonly used in spamming and DDoS operations. Variants of the Zeus and Citadel botnets were collected from high-interaction honeypots and used in this test.
Legacy	Samples included several hundred variants of known malware that have been in circulation for 30 days or more. The malware classifications primarily consist of viruses and worms.
Malicious Documents	These samples were a mix of Microsoft Office documents (Word, PowerPoint and Excel files) that held known macro viruses, and PDF files containing a variety of viruses, APTs and worms.
RATs	Remote Access Threats (RATs) are malicious code disguised as something normal or usable, often masquerading inside other legitimate software. When activated in a victim host, they provide full remote control over that victim.

Test Tools

Miercom used a proprietary blend of industry leading test tools, scripts, and databases to provide a robust, comprehensive, and realistic testing environment. Samples from our Advanced Threat Detection Industry Study were also tested by Symantec and its competitors.

Test Partners

Test Bed Diagram



Malware was delivered from the raw internet via multiple external sources in order to simulate a real world environment. These methods included http, https and FTP file initialization from within the protected network behind the Symantec ATP and other DUTs. Malicious Samples were delivered directly to the DUT through a typical layer 3 network router and thoroughly inspected before it could be delivered to the local LAN. The test bed consisted of a FireEye 1310, a Cisco Source Fire and the Symantec ATP which was a preconfigured Virtual machine hosted on an ESXI 5.5 server. The DUTs were then connected to a layer 2 network switch consisting of the victim machines.

Test Bed Configuration

The appliances were configured to detect every security related category available within its administrative console and to use all available defenses. All products were configured with default settings.

Product Deployment

Symantec Advanced Threat Protection	Cisco Sourcefire Intrusion Prevention System	FireEye Security Appliance
TAP mode deployment	**In-line deployment**	**TAP mode deployment**
• Monitor inbound and outbound packet information • No real-time protection • Traffic and malicious data passively monitored by management console • No response unless attack already occurred	• System sits on network's data path to analyze traffic • Real-time protection • Traffic that does not comply to standards of non-malicious traffic is recorded • Determines whether traffic is forwarded to original destination or quarantined	• Monitor packet information in inbound and outbound traffic • No real-time protection • Traffic and malicious data passively monitored by management console • No response unless attack had already occurred

Symantec ATP was deployed in TAP mode, a passive approach to monitoring traffic in comparison to in-line deployment which places the sensor directly in the network path for traffic inspection. TAP mode did not enable real-time protection and does not trigger a response unless the attack already occurred.

Victim Environment

Virtual machines, hosted on VMware ESXi release 5.5, acted as protected victim computers during tests. These VMs were subjected to attacks from a malicious server. Following the attempted transfer of samples from server to victim, security-product log files are then reviewed. Log files were intended to show if a sample was detected, how long it took to detect it from time of initial request to download, and what post-detection remediation steps, if any, were taken by the security product.

Results Summary

Security effectiveness testing validated each unit's ability to detect real world threats with accuracy, speed and clarity. Considering the wide variety of security products on the market, a product's mitigation techniques and ease of implementation within an enterprise are valuable as its detection rate.

	Symantec
Detection	92.1 %

Detection

Symantec ATP displayed a malware detection rate of 92.1%, at least 18.5% higher than its competitors. Its best detected malware categories were AETs, APTs, botnets, legacy, and RATs. The most meaningful scores were the 100% detection of AETs and APTs which are the advanced evasive and persistent malware that are considered the most relevant and complex threats today. Its competitors scored significantly lower in the AET category.

Forensic Reporting

The reporting interface was user friendly and offered an automated list of all threats, parsed by time, name, source and destination. A timeline feature on the dashboard gave a straightforward visual of the flood of detected threats by date and time of their occurrence allowing for easy tracking of attacks.

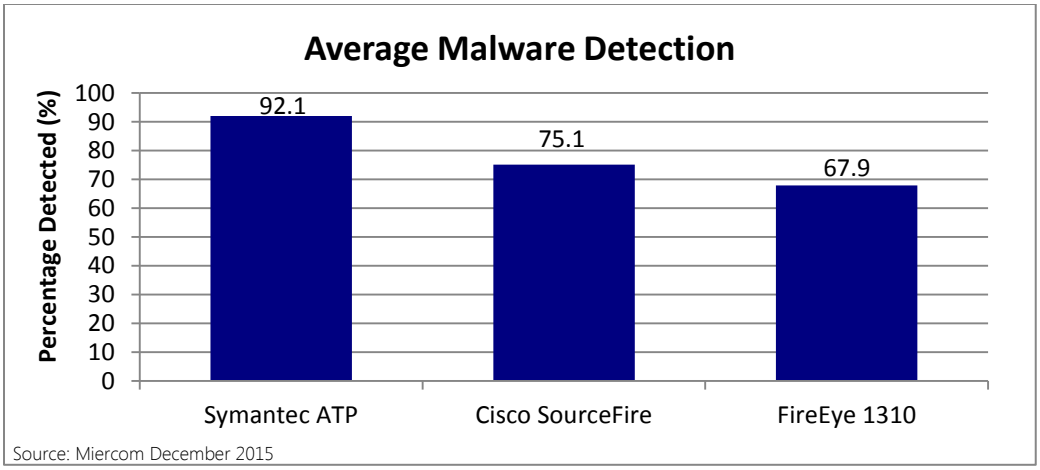
Competitive Malware Detection

Description

Malware detection was determined by how accurately the security product was at alerting the presence of malicious software samples in a mixed set of malicious and non-malicious samples.

Competitive Results

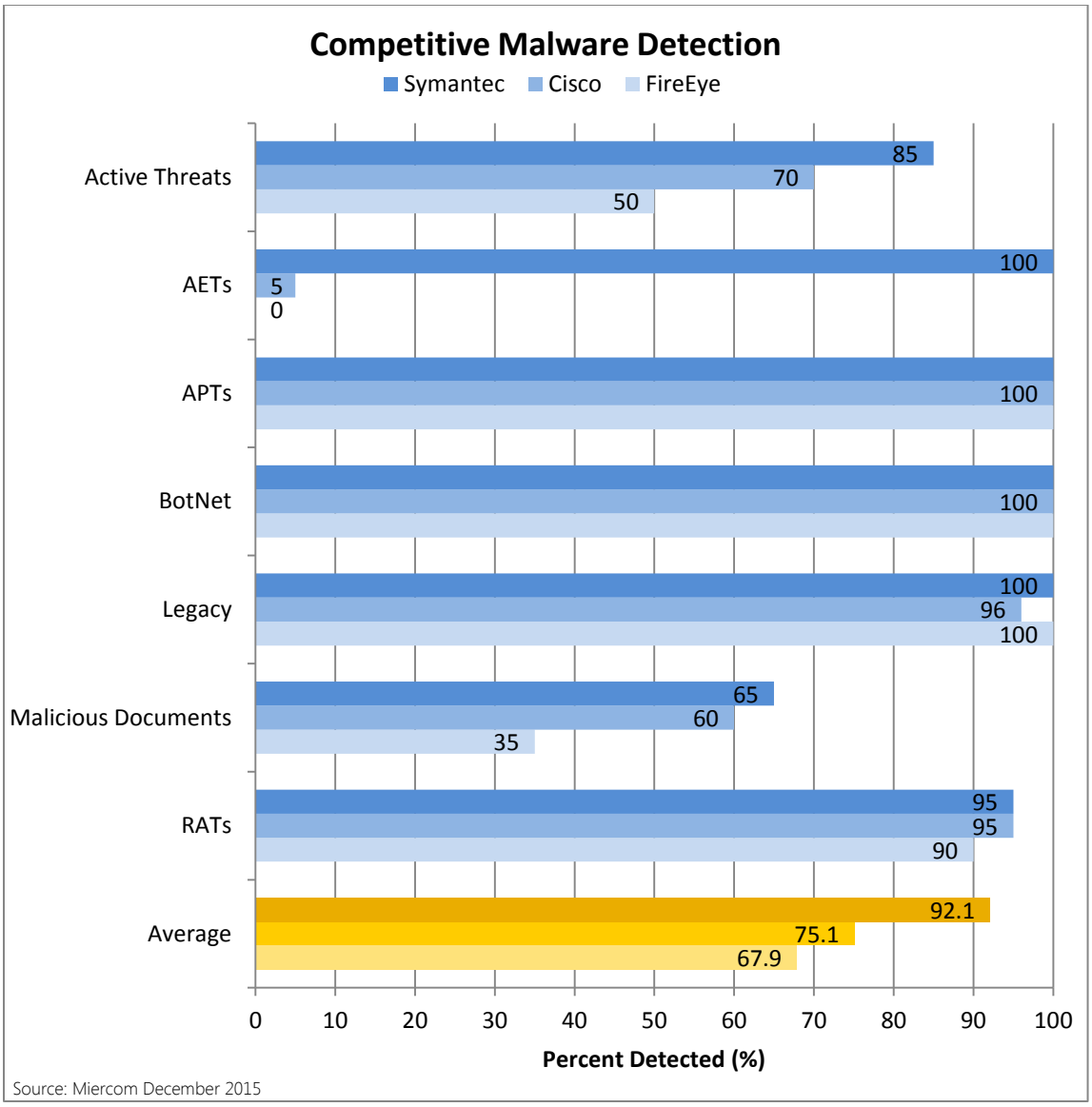
Each bar represents the average percentage of samples detected for each category of malware from the sample set. Detection is defined as the number of samples identified from the sample set mixed with clean traffic.



Symantec had a higher average detection of malware by over 18% than Cisco SourceFire and more than 26% higher than FireEye.

These malware detection results are broken down by category and compared to see the particular strengths each product has regarding certain types of malware. Some malware is considered to be a greater threat, such as Active Threats, AETs and APTs. These are the worst malware for an enterprise because of their complex, evasive and persistent nature.

The chart on the following page displays the percentages detected, and the averages for competitive comparison.



Symantec had the highest level of detection when sent traffic mixed with various categories of malware, with highest detection for the most complex threats – Active threats, AETs, and APTs – identifying at least 95% more AETs than Cisco or FireEye. The average detection rate of Symantec was at least 18.5% more than its competition.

In tap mode, detected samples could be reviewed in the console of each product. Symantec was observed to have the highest detection rate for every category of malware, scoring full detection against AETs and APTs.

Forensic Reporting

Description

Threat analysis is crucial for future preventative action. Being able to track, quantify and analyze collected data allows the user, and the enterprise, to be more prepared for the latest and most pervasive threats attempting to breach a network. This reporting interface is evaluated for its level of detail and its ease of use.

Results

The source and destination of the malicious file or URL was displayed to allow the user to easily distinguish between a web-based and filed-based threat. The threats were parsed to create a list by type and name while providing file path and possibly other attached malicious incidents associated with the threat. The timeline feature helps the user visually track when a threat has occurred, and also provides additional context such as global and local prevalence, as well as DeepSight information about the source of the attack.

Fair Test Notification

All vendors with products featured in this report were afforded the opportunity before, during, and after testing was complete to comment on the results and demonstrate the performance of their product(s). Any vendor with a product tested by Miercom in one of our published studies that disagrees with our findings is extended an opportunity for a retest and to demonstrate the performance of the product(s) at no charge to the vendor.

All vendors are welcome to demonstrate their performance on their own to Miercom. Miercom will update these results if new data presents itself.

About Miercom

Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed.

Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable™, Certified Reliable™, Certified Secure™ and Certified Green™. Products may also be evaluated under the Performance Verified™ program, the industry's most thorough and trusted assessment for product usability and performance.

Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.