Intel Security Advanced Threat Defense
Threat Detection Testing

DR150724C
July 2015

Miercom
www.miercom.com

Contents

1.0 Executive Summary

Miercom was engaged by Intel Security to conduct a thorough threat detection and security efficacy analysis of Intel Security's Next Generation Firewall and Advanced Threat Defense products. The objectives of this analysis were to evaluate the successful threat detection rate and to determine the blocking capability.

The assessments of Intel Security's products were included in Miercom's ongoing industry average study, which compares metrics and performance of similar products to gauge each device's relative proficiency.

The malware samples used during this testing, as with Miercom testing of other products, were obtained by Miercom through its own resources. A set of malware samples were created by Miercom; no vendors provided any of the samples used in this testing.

Key Findings:

- The Advanced Threat Defense's detection performance was notably above industry average.
- With sandboxing enabled, the ATD was very efficient at analyzing malware files.
- The ATD detected 94% of the most destructive type of threats live on the internet today – Polymorphic threats – which constantly change by the second and remain the most difficult for security packages to identify.

Any pertinent observations and recommendations by our test team relating to the Intel Security, security solution's overall effectiveness have also been noted and included in this report.

Intel Security ATD distinguishes itself from other antivirus solutions by being implemented as an integral component of the network, not on an endpoint. One of its main purposes is to identify Polymorphic threats, colloquially referred to as "zero-day" threats, which have become increasingly aggressive in their attacks against networks. Intel Security effectively protects against these threats by their sandboxing method, to virtually run files without breaching security in its discernment of malicious and benign files.

The Intel Security Advanced Threat Defense is an effective security product, our testing showed, and Miercom appreciates the opportunity to have conducted this independent and confidential assessment of the latest Intel Security package.

Robert Smithers
CEO
Miercom

2.0 About Advanced Threat Detection

Advanced threat detection is the necessary combatant for attacks that are designed to overthrow, obscure, or avoid protective measures of a network security system.

Threats are ever increasingly complicated and intelligent. Polymorphic threats can change, adapt and infiltrate a system before security devices and methods have a chance to assess the situation.

Miercom's ongoing Advanced Threat Detection Study compares products with developed features for reducing vulnerabilities against advanced attacks, as well as legacy malware that continues to remain prevalent. All vendor products included in the statistics for this study were tested with their most current version available as of March 2015.

Products Tested

Intel Security Advanced Threat Defense (ATD) in conjunction with the Next Generation Firewall (NGFW) was the only product package officially evaluated in this testing. Its results were added to the Miercom Advanced Threat Detection Study for comparison to industry-wide detection rates for this particular protection arrangement.

Intel Security ATD is a multi-layered solution that involves various techniques and products. These include pattern matching (signature-based detection), global reputation, and static and dynamic threat analysis. Its blocking method is heavily reliant on sandboxing, in which it emulates potentially malicious files within a virtualized container, or sandbox, and executes portions of suspicious code in a tightly controlled environment. Without sacrificing network security, it can determine a verdict of whether the threat is harmful or harmless.

The product package as tested was a combination of two discrete Intel Security appliances:

- The Advanced Threat Defense (ATD) appliance – we tested the ATD-3000 appliance with pre-loaded software version3.4.8.71.50053
- The Next Generation Firewall (NGFW) appliance – we tested the NGFW 5206 appliance, running software version 5.9.0.13052

3.0 How We Did It

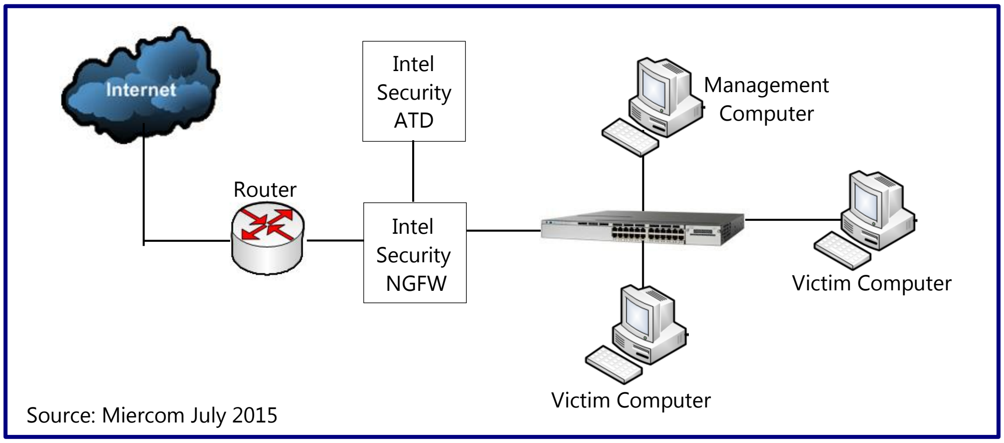
Miercom's security-efficacy analysis of Intel Security's ATD and NGFW package employed all the same test samples that Miercom has been using throughout its Advanced Threat Detection Study.

During this analysis, Miercom's engineers assessed the following security functionality:

- *Detection*: ability to identify known threats from test sample sets.
- *Emulation*: ability to emulate unknown but suspicious files
- *Sensitivity*: percentage of accuracy in its ability to discern between malicious and safe files, based on the outcome of threat emulation
- *Forensics*: level of detail offered in post-response reporting to an incident (Note: Forensic reporting is an important feature of products such as this one, but since it does not enhance upfront detection or threat remediation, it is not used in gauging the product's overall security efficacy.)

Known malware samples were obtained from Miercom's honeypot, which consists of both low- and high-interaction honeypot partitions. Legacy samples were used, but the focus was on younger samples. Known and noteworthy malware and variants of Zeus, Poison Ivy, Carberp, Cryptolocker and others were also used.

Test Bed Setup



Source: Miercom July 2015

The test bed is structured so the security package under test, in this case two appliances, acts as a logical intermediary between the victim and attacking machines.

One attacking machine is employed:

- *Malicious Web Server*: a Windows 7 computer with an online cloud server used to host malware samples utilized during web- and network-share propagation tests.

The Intel Security NGFW is set up to pass files through the ATD for analysis before reaching the victim network. After analysis, the file is passed as partially inspected from the NGFW to the ATD for completion.

The first victim computer will download the files, and after the ATD has analyzed all files, the second victim attempts to download them. The files passed through the first victim, which were determined to be malicious, are blacklisted based on their signature and not allowed to be downloaded by the second victim.

All file types and locations need to be defined in the Rules of the Intel Security NGFW in order to send them to the ATD. The victims consist of two Windows 7 hosts with common applications installed that are inherently vulnerable to malware attacks.

Attempts are made to deliver malware samples to each victim via HTTP traffic. (Samples downloaded to the host in their entirety are considered undetected.)

Following the attempted transfer of the samples from the server to each victim, security-product log files are then reviewed to see if a sample was detected, the time period until detection of the sample initially requested, and what post-detection remediation steps, if any, were taken by the security product.

The tests in this report are intended to be reproducible for customers who wish to recreate them with the appropriate test and measurement equipment. Contact Miercom Professional Services via reviews@miercom.com for assistance. Before making any product selection, Miercom encourages customers to conduct their own needs analysis study and to test specifically for the expected environment for product deployment. Miercom engineers are available to assist customers for their own custom analysis and specific product deployments on a consulting basis.

Malware Sample Set

The following types of malware were used in the sample set for evaluating detection and blocking efficacy.

Malware	Description
Advanced Evasive Technique (AET)	*AETs are network attacks that combine several different known evasion techniques to create a new technique that won't be recognized by network security. These attacks can be delivered in pieces, at different times, or over several layers of the network at the same time.*
Advanced Persistent Threat (APT)	*APTs are considered "backdoors" into a victim network. APT malware consists of a staged payload that allows an attacker to obtain shell access. Payloads are often masked with randomization and evasion techniques to bypass anti-virus scanners.*
Botnet	*Botnet malware is a collection of interconnected programs which communicate about performing malicious tasks. When placed on an endpoint device, the programs work together to extract information and infect other machines. Some tasks include stealing sensitive data and intellectual property, participating in DDoS attacks, and emailing spam.*
Legacy Malicious Files	*Legacy samples include known malware that have been in circulation for thirty days or more and consist mostly of viruses and worms. Legacy samples should not require sandbox analysis. Should any pass through an antivirus filter, the sandbox should then have identified it immediately due to the known heuristics of each malware sample.*
Malicious Documents	*An additional sample set of malicious documents used in tested contained a mix of Microsoft Office documents (Microsoft Word, PowerPoint, and Excel files) that held known macro viruses, and PDF files containing a variety of viruses, APTs and worms.*
Active Threat Malware	*Active threat malware samples are actively changing, unknown threats that have been custom-crafted. These undetected samples were acquired from external resources, private honeypots, and APTs that have undergone antivirus evasion techniques such as encryption and payloads that deliver malicious content.*
Remote Access Trojans (RATs)	*RATs are malicious code disguised inside other legitimate software. When activated in a victim host, they provide full remote control over that victim. The RAT sample set used in our testing consisted of a mixture of Microsoft Office documents and PDF files.*

4.0 Summary of Results

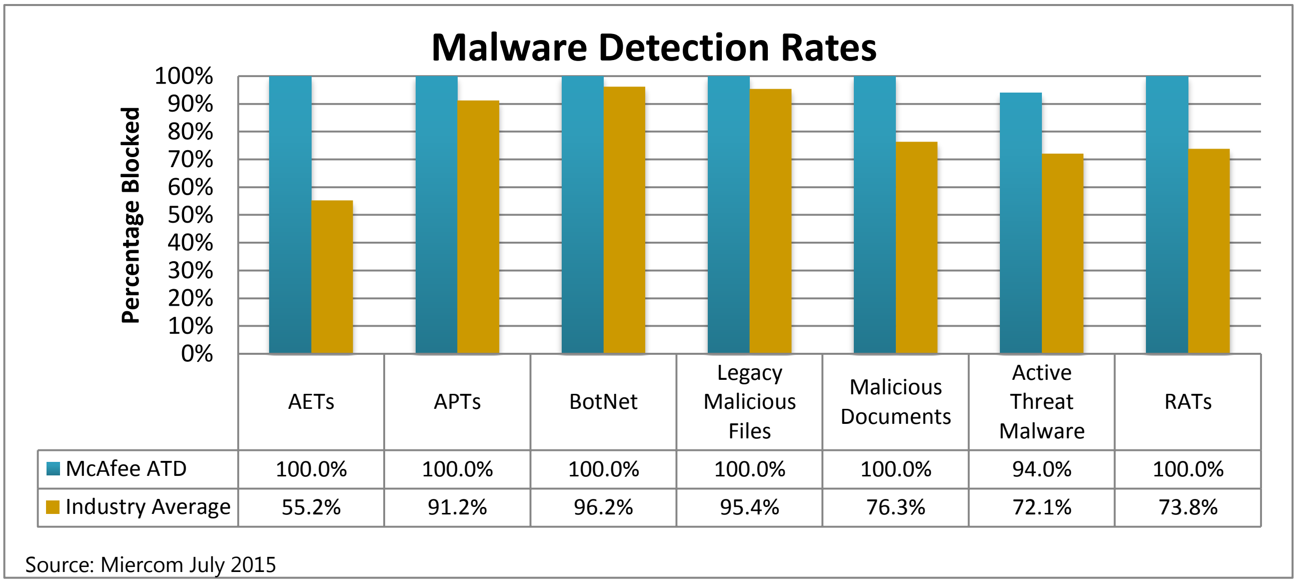
Improving the security posture of an enterprise requires threat detection accuracy, speed, and mitigation. There has been much debate over the wide variety of security controls on the market and the effectiveness of not only the products themselves, but also their implementation within the enterprise infrastructure.

Malware Detection Rate

Each bar represents the percentage of samples captured for a given sample set. Detection rate is defined as the number of samples blocked or identified divided by the total number of samples in the set.

$$\text{Detection rate (percent)} = \frac{\text{Number of Samples Mitigated}}{\text{Total Number of Samples Subjected}} \ast 100$$

Our comprehensive analysis of the Intel Security products was based on the detection rate for several malware sample sets, producing the following results:



	AETs	APTs	BotNet	Legacy Malicious Files	Malicious Documents	Active Threat Malware	RATs
🟦 McAfee ATD	100.0%	100.0%	100.0%	100.0%	100.0%	94.0%	100.0%
🟨 Industry Average	55.2%	91.2%	96.2%	95.4%	76.3%	72.1%	73.8%

Source: Miercom July 2015

Intel Security Advanced Threat Defense delivered 100% detection of all sample sets except the Active Threat Malware, which are the most complex and evasive set of malware.

Performance was excellent. The combined package of ATD and NGFW proved to have exceptional malware detection and prevention. Configuration played a huge role in the accuracy of detection. The Rules of the ATD can be set to detect any number of file types. When all the rules were set to scan its maximum quantity of file types, it had greater scope with which to detect more malware; particularly the AETs and Polymorphic threats. Initially, without these rules, the device was unable to gain visibility of the range of threats coming to the victim computers.

Malware Detection Speed

Having a granular approach to file types, unfortunately, has an effect on real-world situations where sandboxing such a high quantity can slow network performance. It is typical, and expected, that this bottleneck may occur.

There is no definition speed for how fast detection and blocking occurs, but sandboxing was directly related to file size. Larger files intuitively take longer to process. However, some non-malicious file types with extensions such as .zip, .rtf, .exe, .pdf, and other common file types were processed very quickly through the sandbox.

An issue worth noting is the impact on workflow if an enterprise typically transfers large files via web- or FTP-server.

Mitigation

The ATD and NGFW package handled malware very effectively. It did not allow the victim computers to be infected by malicious files. The first victim would receive the malicious file, and if suspected as malicious, it was immediately blocked. The same file is sent to the second victim computer and it was blocked immediately because it was already flagged as malicious in the ATD/NGFW and blacklisted.

This feature is useful for the real-world environment because its propagation of detection reduces the risk of multiple users being re-infected.

Considering the amount of files detected, it did efficiently block threats that were considered malicious. The only files that were not detected, and therefore neither blocked, were file types that the ATD rules did not give an option to scan. This is rather an issue with capability than ability.

Forensics

Reporting was extremely detail oriented, providing a wealth of useful information. The graphical user interface (GUI) was quick to report information, however navigation might be challenging for a novice user. The tabs feature was very convenient for selecting each new section of results and alleviated possible navigation issues.

5.0 About Miercom

Miercom has published hundreds of network-product-comparison 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 and 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.

6.0 About the Miercom Advanced Threat Detection Industry Study

The data of this report was obtained completely and independently by Miercom as part of its Advanced Threat Detection Industry Study. The study is an ongoing endeavor in which all vendors have an equal opportunity to participate and contribute to the most comprehensive and challenging test program in the industry.

All vendors with products featured in this report were afforded the opportunity before, during, and after testing was complete to comment on the testing results and demonstrate their product's performance. Any vendor with a product tested by Miercom in one of our published studies that disagrees with our findings is extended an opportunity to retest and provide a demonstration of their product's performance.

7.0 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. No part of any document may be reproduced, in whole or in part, without the specific written permission of Miercom or Intel Security. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.