# BluVector Cyber Threat Detection and Hunting Platform

DR160205D

June 2016

Miercom
www.miercom.com

# Contents

# Executive Summary

Miercom was engaged by Acuity Solutions to conduct independent security efficacy testing of the BluVector Cyber Threat Detection & Hunting platform. Testing, which employed industry-leading assessment tools, was conducted in February 2016. Results were compared to the average security efficacy percentage for comparable products, derived from the malware detection portion of Secure Web Gateway Industry Assessment of 2016.

The product was tested for its ability to detect our mixed, sophisticated sets of legacy and advanced malware. This report is intended to highlight the distinctive features this device has in its defense against the most threatening, complex threats to date.

BluVector was equipped with malware detection functionality, discussed in detail within this report. The product was deployed in SPAN Monitor Mode to scan all traffic from WAN to LAN over the network switch. The product operates to inspect traffic, but not block any samples. It is in intended to work cohesively with existing security measures of an enterprise infrastructure.

Miercom was impressed by performance of the following:

**Key Findings**

- Real-time detection and instantaneous reporting of 99.6% of the latest malware samples
- Achieved a detection efficacy of 99.1% against Miercom's industry standard samples
- Capable of 100% detection against varied threats – including polymorphic and anonymously shared files
- Granular, user-friendly event log of organized threats for quick remediation
- Suspicious samples were flagged for future blocking, allowing for detection through machine learning

BluVector outperformed the vendor average by more than 18%, making its detection capability among the highest on the market.

Detection occurred in real-time to drastically reduce network vulnerabilities and was made visible in the console event log for further investigation. By employing this platform in an existing infrastructure, network security can be enhanced by its immediate threat awareness, making mitigation easier to execute.

Based on the results of our testing, BluVector has proven exceptional malware detection efficacy for both legacy and advanced malware, earning the Miercom Certified Secure Certification.

Robert Smithers

CEO

Miercom

# Overview

## Product Tested

The BluVector Cyber Threat Detection & Hunting platform version 1.6 goes beyond signature-based and behavioral-based approaches to identifying and classifying threats within a network. This product uses machine-learning techniques to handle zero-day threats and others that borderline malicious and benign, depending on network policies.

The platform intends to monitor and classify all content received by and transmitted from the network, detecting all malicious software in real-time to minimize durations of vulnerability. Analyses of supposed threats are executed in milliseconds to quickly provide a plan for immediate remediation by integrated security tools, such as sandboxing.

## Test Focus

The purpose of this report is to demonstrate the capabilities of this product as a malware detection appliance against sophisticated sets of active, advanced threats from around the globe. The report is organized to discuss the following:

**Detection** The samples detected by the device are recorded and analyzed to determine visibility and intelligence of threats on the network. The product is expected to detect 100% of known malicious samples.

Malware detection results are compared to the industry average of products with malware detection mechanisms from the Miercom Secure Web Gateway Industry Assessment of 2016.

**Reporting** The product is evaluated for its reporting capabilities that would allow an IT administrator in a real-life scenario to assess threatening network situations. The device is expected to have a transparent view of the machine learning process the product uses to identify threats.

A summary of all results and user experience with the product is discussed to provide a general view of how the product earned the Certified Secure certification.

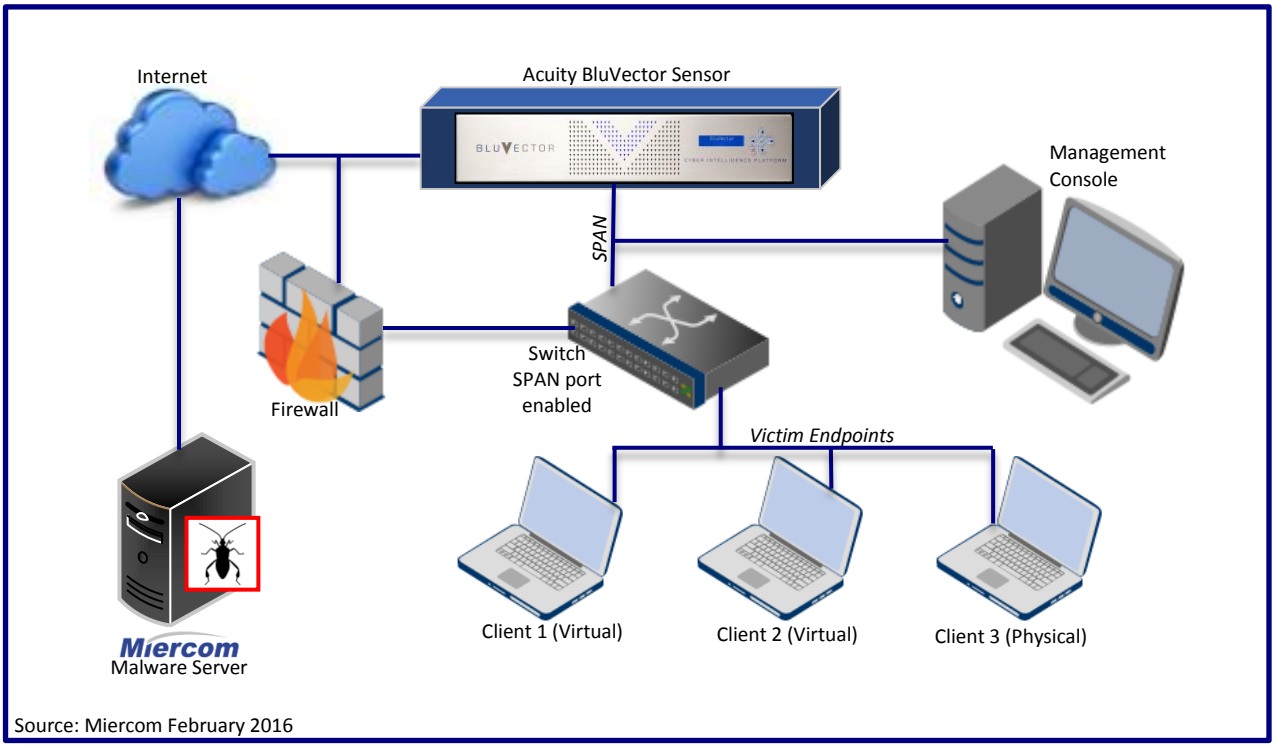
## How We Did It

The BluVector appliance was deployed in a simulated network environment which represents a real-world scenario of switch, firewall and endpoints. The device acted as an intermediary between untrusted and trusted zones. An "attacker" was sourced in the untrusted zone and attempted to deliver malware to targets within the trusted zone in order to establish communication. BluVector was evaluated for its ability to detect and alert of all attempted exploits and malicious activity leaving the boundaries of the trusted network.

Testing focused on detection efficacy of the following:

| Malware Set |
| --- |
| **Active Threats**<br>Custom-crafted, constantly changing evasive malware |
| **Advanced Evasion Techniques (AETs)**<br>Combined evasion tactics that create multi-layer access |
| **Advanced Persistent Threats (APTs)**<br>Continuous hacking with payloads opened at the administrative level |
| **BotNet**<br>Communicating programs that collectively spam and deliver DDoS attacks |
| **Legacy**<br>Variants of known malware older than 30 days (e.g. virus, worms) |
| **Malicious Documents**<br>Mix of Microsoft and Adobe documents with Macro viruses, APTs, worms |
| **Remote Access Trojans (RATs)**<br>Trojans disguised as legitimate software which remotely control victim once activated |
| **TOR/P2P/I2P**<br>Malware contained in downloads via torrent sites on P2P or I2P networks |
| **Polymorphic Malware**<br>Constantly changes, making it difficult to detect |
| **Zero Day Malware**<br>Exploits a known vulnerability before the vulnerability is fixed |
| **Mobile Malware**<br>Targets mobile devices and shuts them down or accesses them remotely |

## Test Bed Setup




Source: Miercom February 2016

The device under test was the Acuity Solutions BluVector Sensor. It was connected to a Dell N2024P 24-port 1GB switch. Three victims were also connected to the switch; one physical Windows 7 computer and two virtual Windows 7 computers.

The SPAN port was enabled in the switch to mirror all traffic through the BluVector sensor. This is required for the sensor to function as a malware detection solution. Malware was downloaded individually and within zip files to determine if the device created events for each file.

# Detection

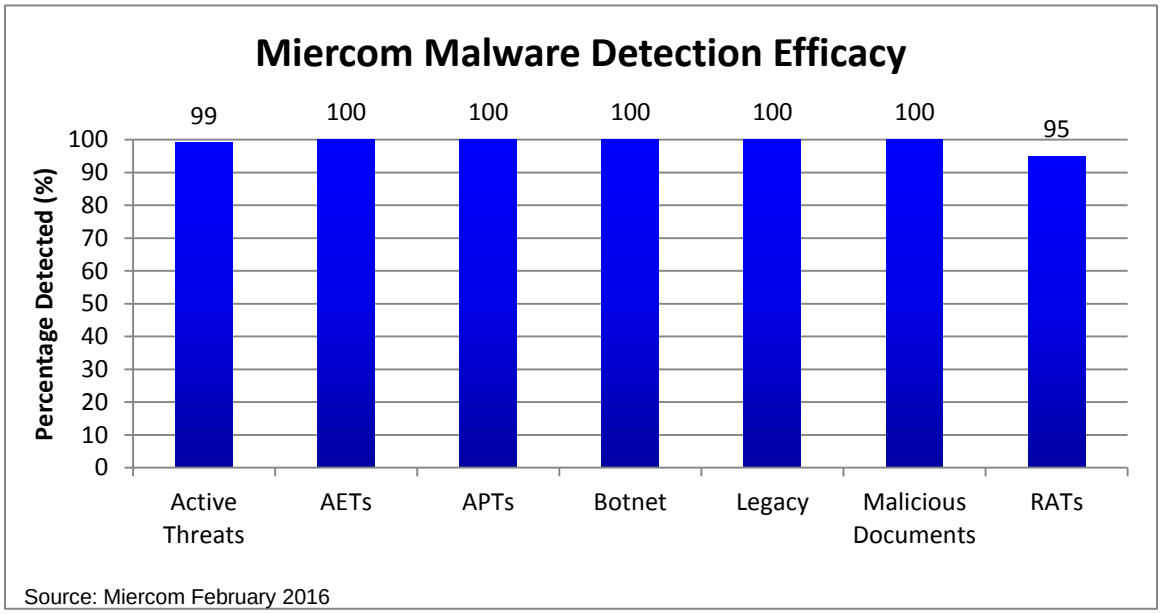
## Miercom Malware

These sets of malware are used in the industry-wide study of malware detection for network security devices. Common malware are botnets, legacy, malicious documents and RATs. An emphasis is placed on active threats, AETs and APTs which are more complex and more challenging for security solutions to identify. Detection results will inform the individual approaches to different malware types, as well as its granularity amongst market competitors.

### Metric

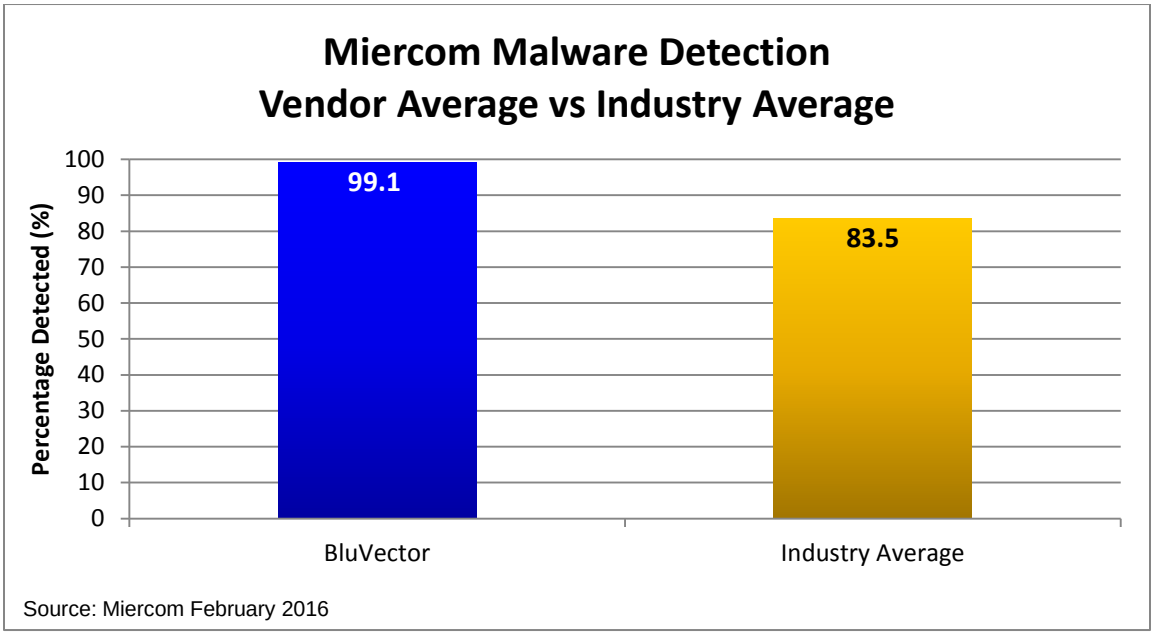
A known amount of malware samples of each category were sent to the device and the percentage of those detected were recorded.

### Results




*BluVector scored 100% for common malware: botnet, legacy and malicious documents. These malware are expected to have higher efficacy scores throughout the market. RATs were detected 95% of the time, displaying the sensing capability of remote malware is very high, but not at the same efficacy of the simpler malware. Active threats, which are constantly modifying themselves, were identified 99% of the time; AETs and APTs, also complex and sophisticated, were detected with 100% efficacy. BluVector has notable strength against evasive, persistent and polymorphic threats.*

Miercom uses its proprietary sample set to assess security solutions for detection across the marketplace. The average of the BluVector device's individual results were compared that of competing devices to provide context to its efficacy score.

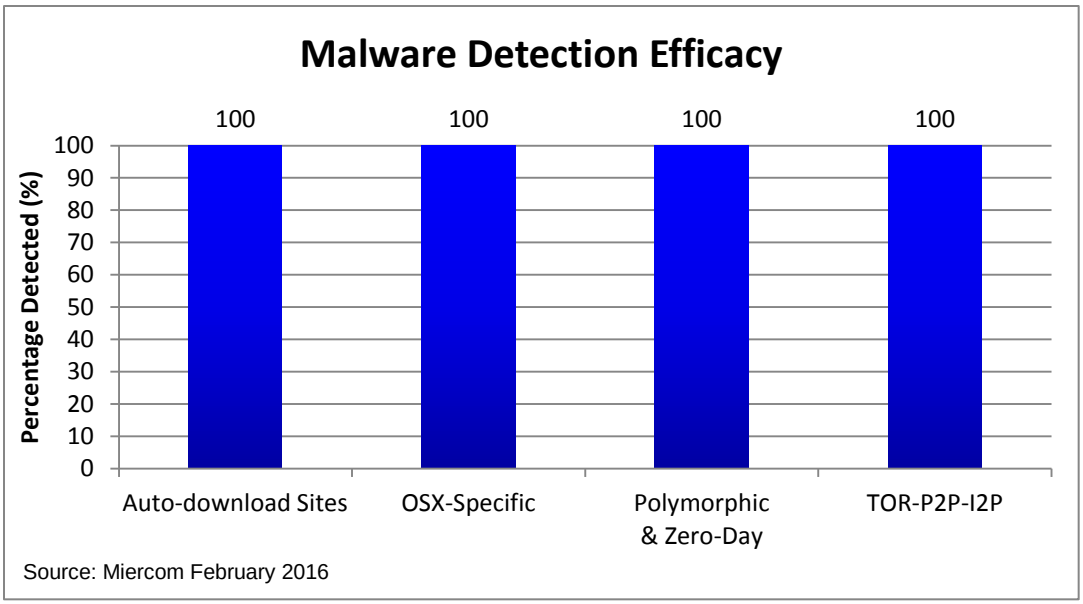



*BluVector was able to detect more than 18.5% of the samples than the average security solution with malware detection capabilities. Comparable industry devices consist of secure web gateways, next generation firewalls and advanced threat protection products.*

## Sophisticated Malware Sets

This test measures how effectively the device detects and issues alerts for malicious software attacks. More specifically, these sets are of any of the following: web-based attacks containing malware, malware geared towards OSX environments, polymorphic, zero-day or anonymously delivered. These sets differ from the Miercom set because they require intelligence that is not typically seen in initial-stage detection devices.

### Results




*BluVector was able to detect each sample from sites that automatically began to load malware onto a physical or virtual endpoint on the network. This signifies its intelligence considering its approach uses neither signature nor behavioral based methods to determine which sites would typically introduce malware. Despite a set of OSX- specific malware, which requires sophisticated means of evading a typically solid Apple environment, the BluVector detected 100% of these threats. Complex polymorphic and zero-day threats were all detected. Additionally, malware delivered over Tor and anonymous peer-to-peer networks was detected with 100% efficacy.*

# Reporting

### Visibility

Having great detection efficacy mostly defines a useful security device, but what's also important is how threats are communicated to IT administrators. Communication and structured results yield the most effective remediation steps to secure a network. The BluVector product was evaluated for its visibility of threats and its ease of deployment for a technical user.

### Results

The BluVector dashboard had real-time accuracy for all samples detected by the sensor. The event log was very granular and provided a good deal of properties for each event. The options for charts, whether pie charts or bar graphs, were available as straightforward visuals of events recorded. The initial setup required a moderate learning curve, but the sensor connection and dashboard navigation were simple to understand.

# Conclusion

Testing of the BluVector Cyber Threat Detection & Hunting platform involved sending samples of known malware through a test network where the BluVector sensor was deployed in SPAN mode from the network switch. Its ability to detect Miercom malware samples, sophisticated malware samples, and report these events in a concise and useful manner was recorded and documented. The product was evaluated to perform accurate detection in real-time.

The BluVector device was 99.1% effective against malware samples of Miercom's proprietary malware set. The industry average efficacy was over 15% lower, at 83.5%. Against sophisticated, polymorphic and peer-to-peer shared malware sets the device achieved 100% efficacy in each category.

Its reporting dashboard was detailed, concise and contained multiple visual options for all events logged. Combining its excellent efficacy scores and user-friendly dashboard, this device is an exceptional choice for an enterprise looking for an additional layer of refined malware detection in its security infrastructure.

## 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.

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.