Blue Hexagon Next-Gen Network Detection and Response (NDR) Security Performance Assessment

BLUEHEXAGON

October 2020

DR200824E

Miercom

Miercom.com

Contents

1.0 Executive Summary

Networks require constant security monitoring, and most organizations analyze files using signature-based methods. As threats become more sophisticated, it isn't enough to sandbox or filter threats purely by reputation – leaving security teams with more work and less time addressing other issues.

Blue Hexagon's Next Generation Network Detection and Response (Next-Gen NDR) relieves the workload using real-time deep learning models for automatically analyzing millions of file traits for contextual, behavioral-based network protection for encrypted attacks. Unlike other products, which uses post-event analysis, Blue Hexagon's deep learning-based approach identifies the root cause of known and unknown malware such as Trojans, droppers and ransomware. Blue Hexagon claims to detect 99.8 percent of malware in under one second, preventing lateral movement of malware. All analysis and reports are delivered in a simple, digestible explanation in their one-cloud dashboard – classifying files by malware type and showing insight into how to further prevent future attacks.

Miercom was engaged by Blue Hexagon to test their product for security performance comparatively to similar products on the market. Each product was evaluated not just for security efficacy against a broad range of malware, but the ability for the device to provide helpful reports to IT teams that lessen the time and cost of attack response.

Our results provide a look into how Blue Hexagon and its competitors handle security by looking at the strengths and unique qualities.

Key Findings

- Blue Hexagon detected the most lethal zero-day malware, ransomware, worms, botnets and evasive malicious threats on the Internet today – with 99.3 percent detection efficacy
- Blue Hexagon is the only vendor proven in testing to show a False Positive Rate (FPR) of 0 percent; none of the (non-malicious) white or grey files were falsely flagged while effectively simultaneously detecting malicious content
- Blue Hexagon's dashboard shows a granular view of logged threats in an intuitive interface that helps security teams take immediate action
- Blue Hexagon has excellent detection logging capabilities, providing more details and visual aids than competing vendors

Based on our findings, the Blue Hexagon Next-Gen Network Detection and Response (NDR) security product demonstrated contextual malware detection capabilities with an exceptional dashboard experience for quick remediation. We proudly award the Blue Hexagon Next-Gen NDR product the ***Miercom Certified Secure*** certification.

Robert Smithers
CEO, Miercom

2.0 Test Summary

Summary of Competitive Security Efficacy and Performance

Tests	Vendors			
Security Efficacy (%)	Blue Hexagon Next-Gen NDR	Vendor A	Vendor B	Vendor C
Immediate Detection	99.3	N/A*	77.1	42.2
Detection After 24-Hours	99.3	57.2	77.1	86.4

PASS	MARGINAL	FAIL
≥85 %	51-84 %	≤50 %

Blue Hexagon proved the best overall detection and prevention for malicious threats and the only vendor to render a 0% False Positive Rate (FPR). The malware detection test results were determined by the device under test detecting the malicious content. The test allowed up to 24 hours for the detection to occur. Testing revealed some of the vendors flagged malicious samples as suspicious rather than malicious and consequently allowed the protected network to be at risk.

* *Vendor A could not make a determination on malicious content applied during Immediate Detection testing.*

3.0 Introduction

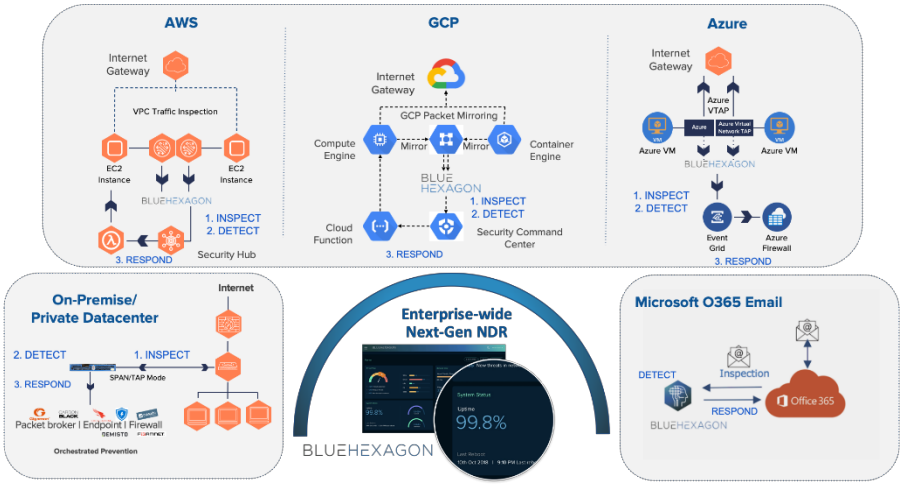
Most network traffic is encrypted to hinder attackers from hiding in plain sight from security products in place. This approach also, inadvertently, ensures that security teams are more challenged to locate threats. Moreover, malware will become more sophisticated outsmarting encryption using concealing techniques that go undetected by most security devices.

Blue Hexagon Next-Gen Network Detection and Response (NDR)

Blue Hexagon uses scalable deep learning technology to inspect all network traffic communication in real-time by discerning specific traits found in payloads, protocols or headers based on intent – not just behavior. The Blue Hexagon Deep Learning HexNet architecture identifies suspicious patterns within stages of the kill chain and stopping attacks once a detection is made. Blue Hexagon is also capable of identifying encrypted traffic communications that are used for malicious C&C communications.

It is also possible for Blue Hexagon to optionally inspect encrypted traffic by first decrypting it using third party network controls (e.g. Palo Alto Networks, Gigamon, Ixia, A10 Networks, F5 Networks). When decryption is not possible, the solution can provide verdicts on pure encrypted traffic by inspecting the traffic headers to glean potentially suspicious or malicious encrypted C2 patterns if present.

How does this compare to other solutions?



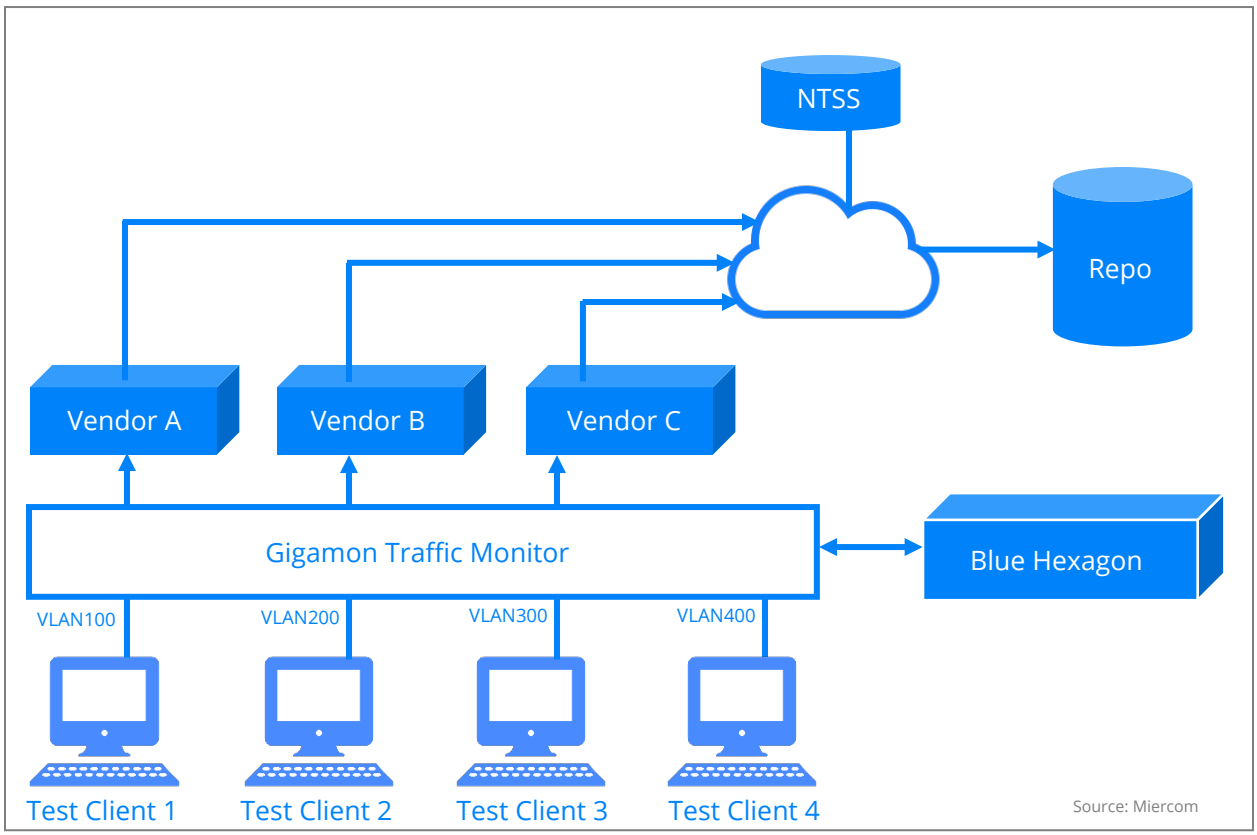
Most security technologies compare large volumes of data or signatures to determine suspicious events. This can result in many false positives since there is no context. The Deep Learning HexNet models work in real-time to save time and cost of analyzing irrelevant data that may not prove harmful to the network in the end. This approach does not require baselining or tuning and can deliver high quality verdicts from the moment it is deployed.

The bottom line: Blue Hexagon goes beyond the new era of anomalistic detection by integrating other technologies to perform real-time detection of new, unique encrypted obfuscation techniques in encrypted web and network communications.

4.0 How We Did It

Our hands-on security testing used a live business environment to challenge each device for a realistic assessment of efficacy and performance capabilities. We tested security using a custom-crafted set of threats for determining detection performance.

Test Bed Overview



In test topology above, we used four identical test clients (Linux virtual machines) to download malicious content from a repository in the cloud. Vendor A, B and C were deployed in the path of the downloaded traffic. Blue Hexagon was deployed in passive mode with traffic mirrored to it via Gigamon. Tests were run simultaneously to eliminate variances in threat intelligence about samples.

Test Tools

The following tools are a representative list of software tools and exploits we used to carry out our analysis.

Network Test Suite Server (NTSS)	Our proprietary NTSS is a high-bandwidth, high-performance server running a highly optimized Debian Linux setup hosting a network performance suite. This suite allows us to quickly deploy multiple test scenarios for specially crafted, multi-threaded Apache setup for delivering a custom-file set to simulate normal web usage, with file sizes ranging from 128KB through 4MB. Files are delivered using an increasing number of clients for different protocols.
Linux Attacker/Control Machine and Test Client	Using Debian 10 with Kernels 4.1.x and 5.1.x. We tested using 64-bit Linux. The client consisted of virtual machines.

5.0 Malware Security

Malware is delivered to networks using different methods, so a network security device should handle any attack, on any protocol, and guard against these threats. These attacks include common malware (e.g. botnets, legacy, malicious documents, and remote access Trojans) and more sophisticated malware (e.g. polymorphic, evasive, and persistent threats) which are not already known by any intelligence database are more challenging to detect.

Using more than a thousand samples from our proprietary malware suite, we assessed each security device. The Miercom malware samples include a broad range of attack techniques which consist of a mixture of file types (e.g. .MSO, .PDF, .RTF, .JS). Popular malware threats include Spidey Bot, CCleaner malware, Mirai, Skynet and OZH RAT.

Common Malware	
Backdoor	Remote attacks use port binding, control and command servers, and dormant malware to infiltrate networks using legitimate services to go unrecognized
Botnet	Communicating programs delivering spam and distributed DoS attacks
Legacy	Variants of known malware older than 30 days (e.g. virus, worms)
Malicious Documents	Mix of Microsoft and Adobe documents with macro viruses, APTs, worms
Remote Access Trojans (RATs)	Trojans disguised as legitimate software remotely controlling victim once activated

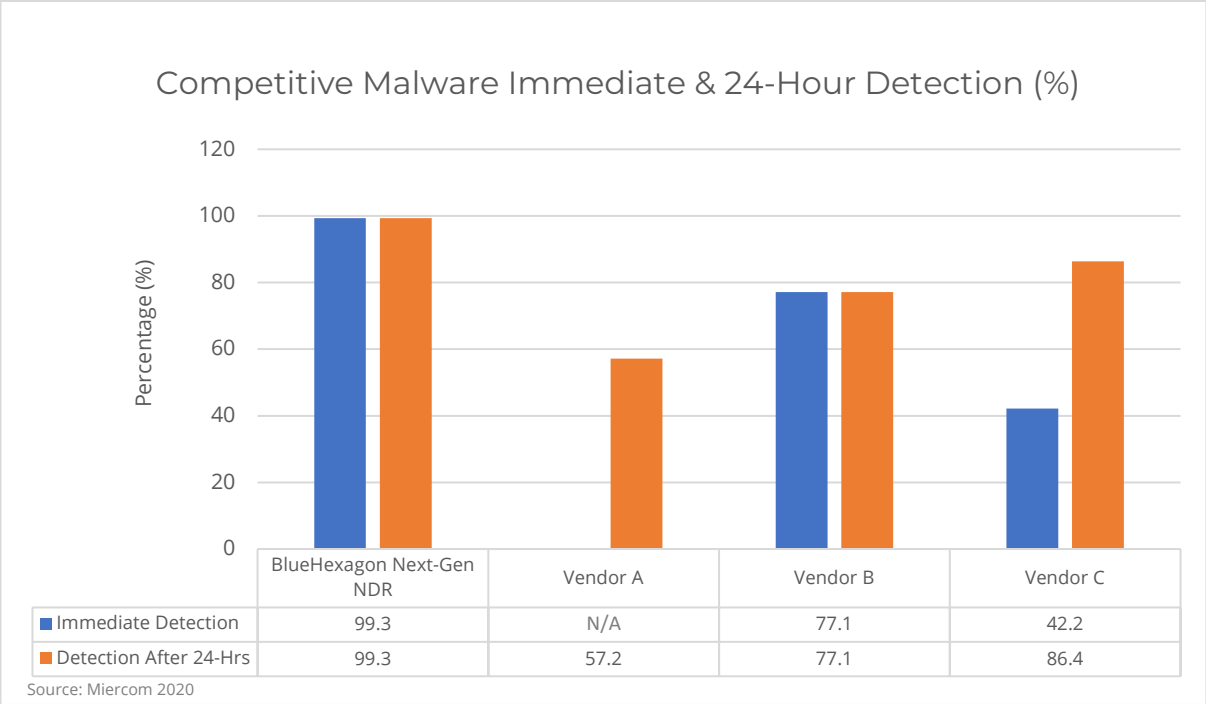
Advanced Malware	
Active Threats	Custom-crafted, constantly changing evasive malware
Advanced Evasive Techniques (AETs)	Combined evasion tactics that create multi-layer access
Advanced Persistent Threats (APTs)	Continuous hacking with payloads opened at the administrative level
Polymorphic, Zero-Day Malware	Constantly changing, difficult to detect; exploit known vulnerabilities

The device under test was deployed between untrusted and trusted zones of a simulated network with a switch, firewall and endpoint devices to represent a real-world environment. An attacker in the untrusted zone (our test suite) attempted to deliver malware to the trusted zone.

Any sample that successfully transferred to a target endpoint (undetected) was considered a fail. Security efficacy was recorded as the percentage of samples detected out of the total set attempted. High detection efficacy against this blend of malicious files indicates well-rounded protection from multiple attack vectors. Detected samples are analyzed to determine visibility and intelligence of threats on the network.

We then further analyzed malware security using the False Positive Rate (FPR). False positives are benign, but suspicious, "grey" files that vendors accidentally mark as malicious. For this test, we used a mixture of 2 percent grey and 50 percent malware and 48 percent white files within malicious traffic. The device under test was expected to only flag malicious files – with an ideal FPR of 0 percent.

5.1 Malware Detection and Prevention Efficacy



	BlueHexagon Next-Gen NDR	Vendor A	Vendor B	Vendor C
Immediate Detection	99.3	N/A	77.1	42.2
Detection After 24-Hrs	99.3	57.2	77.1	86.4

Source: Miercom 2020

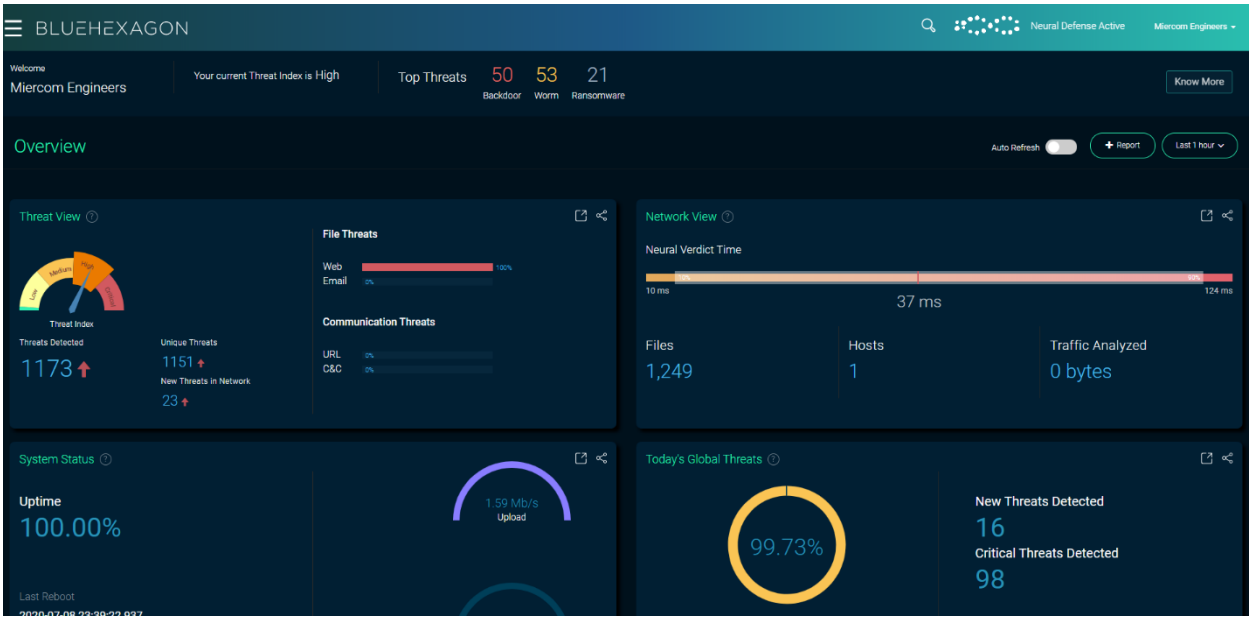
Blue Hexagon detected and prevented the most malware at 99.3 percent efficacy, both after 24 hours with sandboxing and immediately upon discovery. Vendor A was unable to immediately detect malware samples but after 24 hours, it could detect 57.2 percent of threats. Vendor B immediately detected 77.1 percent of threats and was able to repeat this efficacy after 24 hours. While Vendor C had reasonable 24-hour detection efficacy at 86.4 percent, it only identified 42.2 percent of samples during immediate detection testing.

5.2 False Positive Rate (FPR)

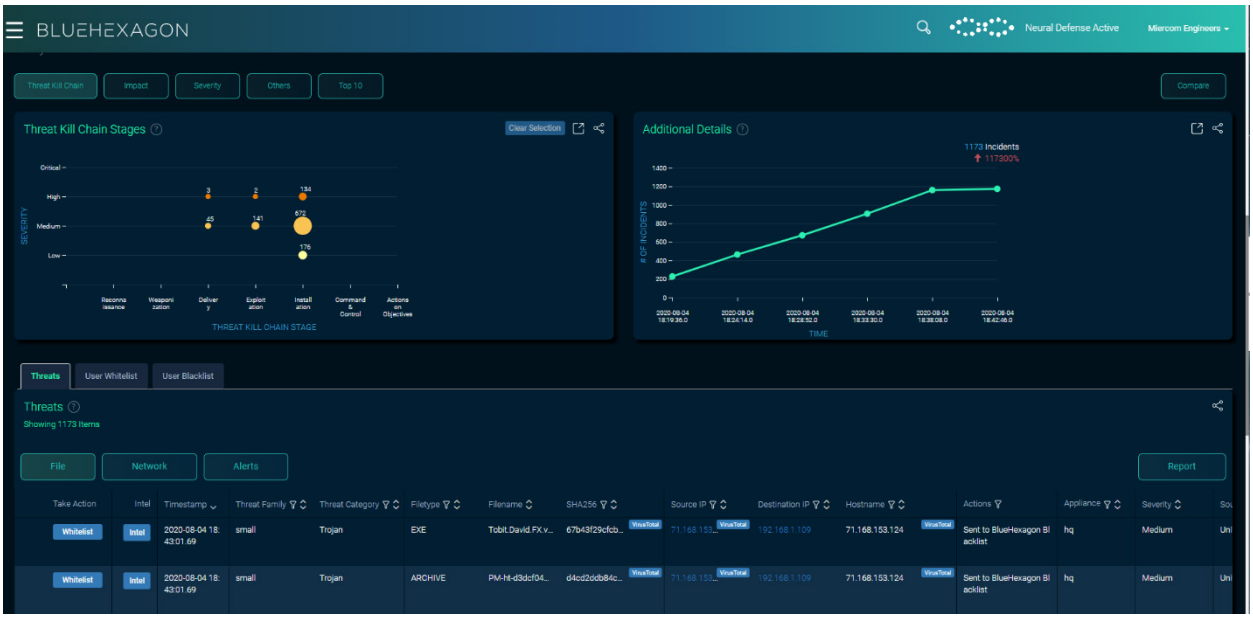
Blue Hexagon can detect "grey" (benign but suspicious) and Potentially Unwanted Application (PUA) files at the administrators' preference. Miercom observed successfully detected malicious files only; there were no incidents of erroneously flagged grey files that were not inherently malicious. Blue Hexagon was the only vendor to show an FPR of 0 percent. We did not penalize the competing vendors for failing the false positive testing, other than recognizing Blue Hexagon as the only vendor that passed FPR tests successfully.

5.3 Dashboard User Interface

Blue Hexagon Next-Gen NDR



The aesthetically pleasing Blue Hexagon dashboard offers a wealth of information – giving contextual threat visibility, status, and network performance. Navigating the dashboard is straightforward and simple to do.



The Threat Kill Chain Stages allows IT teams to see the severity and clustering of threats within the attack phases to pinpoint vulnerability and begin a plan of action. Additional details, like the number of incidents, shows the trends of attacks across time. All threats are shown in a list, with a Take Action option for whitelisting or blacklisting. These threats are displayed with timestamp, threat family (e.g. small), category (e.g. Trojan), type, name, signature, source and destination IP addresses, hostname, actions and more. All threats can be exported to a report for further investigation.

Vendor A

The environment was not straightforward; the configuration did not make it apparent on how to block files it finds malicious. From what we observed, the different configuration options were unreliable and too complex to perform a simple task, like malware prevention. Malware detection was compiled into a list view – showing the malware type, severity, infections, blocked files, timestamp and more.

Vendor B

Vendor B showed malware found in a list view – by timestamp, source IP address, device, result (e.g. blocked), and action taken.

Vendor C

Vendor C does not always detect malware files in real-time, but its post-download detection further enhances prevention capabilities. Above are the verdicts of the post-download analysis. It then displays the blocked malware in a list view – showing files by timestamp, type, name, zone, victim IP address, action, severity and more. In terms of updates, Vendor C does not show the changes that need to be committed in this dashboard. Also, these changes take longer than normal to accomplish (e.g. a few minutes for a simple password change). Additionally, we did not observe a log out feature.

6.0 Conclusion

Malware Security

Blue Hexagon Next-Gen NDR had the highest malware detection and prevention rate, at 99.3 percent. Vendor A had the lowest malware detection rate of 57.2 percent, after 24 hours; it was unable to immediately detect samples. Vendor B showed average detection efficacy, at 77.1 percent for both immediate and 24-hour detection. Vendor C had the second highest detection rate at 86.4 percent, but its immediate detection was only 42.2 percent.

Blue Hexagon was the only vendor to display an ideal False Positive Rate of 0 percent – showing no incidents of falsely blocked files that were not malicious.

WebUI

Blue Hexagon had the most comprehensive, aesthetically pleasing, and informative dashboards of all competing vendors. The numerous visual aids of ongoing trends, coupled with straightforward navigation, made viewing, analyzing and remediating threats simple and intuitive.

Competing vendors' dashboards all offered the same view: list of discovered threats. All lacked the helpful visual indicators provided by Blue Hexagon. Vendor A had unclear, unreliable configurations that complicated a normally simple prevention task. Vendor C only shows adequate detection in a post-download discovery and requires unusual wait time for basic updates or changes.

Explainable AI

Most malware analysis systems, including sandboxes, provide information on malware by family and category. However, this information is not particularly useful to the Security Operations Center (SOC) analyst on what the malware does or why it needs to be blocked. This is where predictive Indicators of Compromise (IOCs) come into play. Blue Hexagon can map IOCs associated with malicious samples based on IOCs commonly associated with similar malware. These IOCs are mapped to the well-known MITRE ATT&CK framework, which effectively explains the verdict to the analyst. This approach proves superior to sandboxing from two standpoints – speed and scalability. Further, it is immune to evasion techniques like virtual machine detection, timing, click detection, and others that are known to defeat most sandboxes. In fact, the Blue Hexagon HexNet even predicts Sandbox Evasion as one of the techniques used by malware – a unique capability of the platform that separates it from its competitors.

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.

By downloading, circulating or using this report this report in any way you agree to Miercom's Terms of Use. For full disclosure of Miercom's terms, visit: https://miercom.com/tou.