Network Threat Protection Evaluation

Table of Contents

Executive Summary

With a distinct shift in technologies driving detection and threat protection, there is much excitement around the promise of AI and the impact it can have in cybersecurity. However, with all the radical claims made, especially when it comes to detection rates concerning unknown threats, the question of how one scientifically gauges technologies such as Machine Learning against the current threat landscape is a topic that continually comes up in independent testing.

At PCSL, we pride ourselves on being "Scientific, Precise, Independent". We decided to put such claims to the test by launching a new testing framework that focuses exclusively on AI-based technologies. Using our experience in threat testing, as well our ability to source threat samples from campaigns globally across different threat categories, our goal is to stress test these cybersecurity products to gauge how they can perform across a wide variety of files and malware types.

Our first candidate for this framework was Blue Hexagon, a California-based deep learning company focused on threat detection. The company's network threat protection platform uses deep learning to inspect network traffic payloads and headers for threats, as an alternative to IPS and malware sandboxes. We requested that Blue Hexagon send us their product that could be tested offline. Their product featured deep learning models that were trained and released six months before the day the test was executed.

There were three key metrics we wanted to validate:

- Threat detection efficacy: how effective Blue Hexagon was at detecting threats across a wide range of threat categories and in various file types and sizes
- False positive rate: how many of the threats detected by Blue were actually benign. False positives are a problem not only because they take up manpower and time to address, but also because they can distract companies from dealing with legitimate security alerts
- Threat detection speed: with the speed of compromise the industry is dealing with, we wanted to validate how quickly Blue Hexagon detects threats. This includes the time needed for network processing

We tested Blue Hexagon against one of the largest samples of threats – more than **40,000** threat samples – from Portable Executable (PE files) to documents such as PDF, MS Office and RTF. We also explicitly tested Blue Hexagon with **2,000,000** benign files to evaluate their false positive rates. Blue Hexagon detected all threats, with an impressive threat detection rate of 100% with 0% false positives, and at an average detection speed of 125 ms.

More than 2,000,000 Samples

100 %
Detection Efficacy

0 %
False Positives

125 ms
Detection Speed

1. Threat Detection Rates for Executables

The Blue Hexagon threat prevention platform was tested against a strategic sourcing of malware, including a comprehensive volume of zero-days from global threat campaigns, as well as the most extensive corpus of malicious samples assembled by independent testers.

In total, 40,000 Portable Executable (PE) threat samples in active use, ranging in categories from Financial Malware, Cryptominers, Spyware to Ransomware, were included a part of the test set:

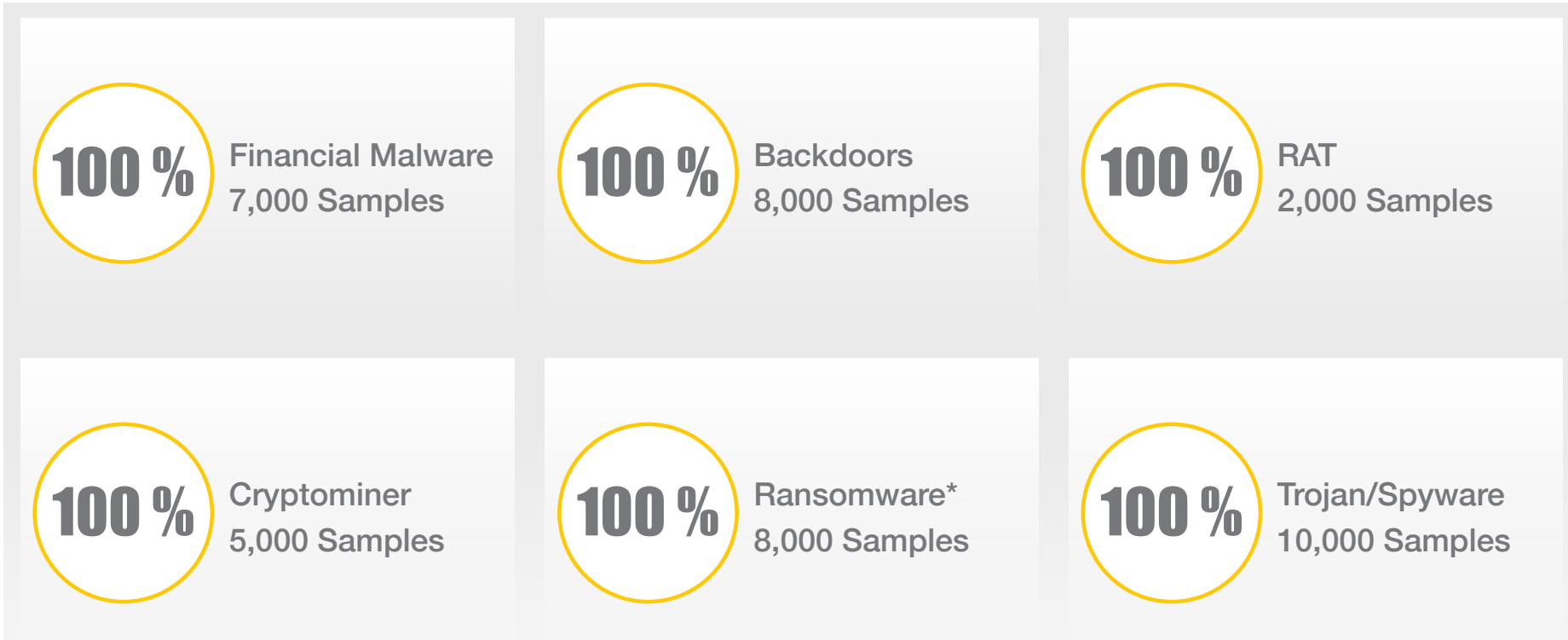
Financial Malware	Financial malware is specialized malware that is created to scan a computer or an entire network, to gain information associated with financial transactions
Cryptomining	Cryptomining malware or cryptojacking refers to software programs and malware components developed to take over a computer's resources and use them for cryptocurrency mining without a user's explicit permission
Backdoors	Backdoors enable authorized and unauthorized users to get around normal security measures and gain high level user access to a computer or network
Ransomware	Ransomware is a type of malware that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid
RAT	Remote Access Trojan (RAT) is a malware program that includes a back door for administrative control over the target computer
Trojan/Spyware	Trojan spyware are malicious programs that masquerade as benign applications used to aid the propagation of spyware. Often they are installed unknowingly as a result of installing some other software or are delivered by an exploit in order to harm the user's system

Blue Hexagon scored 100% in overall threat detection across these categories and threat families.

Overall Threat Detection Score

100 %

Threat Detection Rates – By Threat Category (Executables)



***Gandcrab** was the only family that was used that was outside of a 60 day window, as this family is no longer in active distribution

Threat Detection Rates – By Threat Family

Ransomware

FAMILY NAME	DETECTED
MEGACORTEX	100 %
BITPAYMER	100 %
ROBBINHOOD	100 %
WIXIDO	100 %
SATAN	100 %
RYUK	100 %
GOGALOCKER	100 %
WANNACRY	100 %
SODINOKIBI	100 %
KRAKEN	100 %
TESLACRYPT	100 %
SAMSAM	100 %

Coinminer

FAMILY NAME	DETECTED
SOFTMINER	100 %
WASMWEBCOIN	100 %
POWERGHOST	100 %
PLUROX	100 %
COINREG	100 %
MADOMINER	100 %
SHMINER	100 %
XMRIG	100 %

RAT

FAMILY NAME	DETECTED
LUMINRAT	100 %
COBIAN RAT	100 %
XTREMERAT	100 %
TROCHILUS RAT	100 %
REVENGERAT	100 %
TROJAN.FLAWEDAMMYY	100 %
NANOCORE	100 %
TROJAN.NANCRAT	100 %

Backdoor

FAMILY NAME	DETECTED
BACKDOOR.WHISPERER	100 %
BACKDOOR.HANNOTOG	100 %
BACKDOOR.PYMET	100 %
MOKES	100 %
SKILLIS	100 %
KORPLUG	100 %
SOFACY	100 %
FAKESLIC	100 %
WHISPERER	100 %
DARKTEQ	100 %

Financial

FAMILY NAME	DETECTED
INFOSTEALER.SCRANOS	100 %
INFOSTEALER.VIDAR	100 %
INFOSTEALER.RULTAZO	100 %
INFOSTEALER.PREDAPA	100 %
INFOSTEALER.CATCHAMAS	100 %
INFOSTEALER.LOKBOT	100 %
INFOSTEALER.SCRANOS	100 %

Trojan

FAMILY NAME	DETECTED
URSNIF	100 %
EMOTET	100 %
DANABOT	100 %
ZEXLEX	100 %
VCRODAT	100 %
NIBATAD	100 %
LIROXOD	100 %
ZLELOA	100 %
FENKRIB	100 %
HOPLIGHT	100 %
TRISIS	100 %
AMADEY	100 %
TEFOSTEAL	100 %
QAKBOT	100 %

2. Threat Detection Rates for Documents

Blue Hexagon was also tested against commonly-used document formats. These include MS office documents, RTF files and PDFs. 3,000 samples were included in this test set.

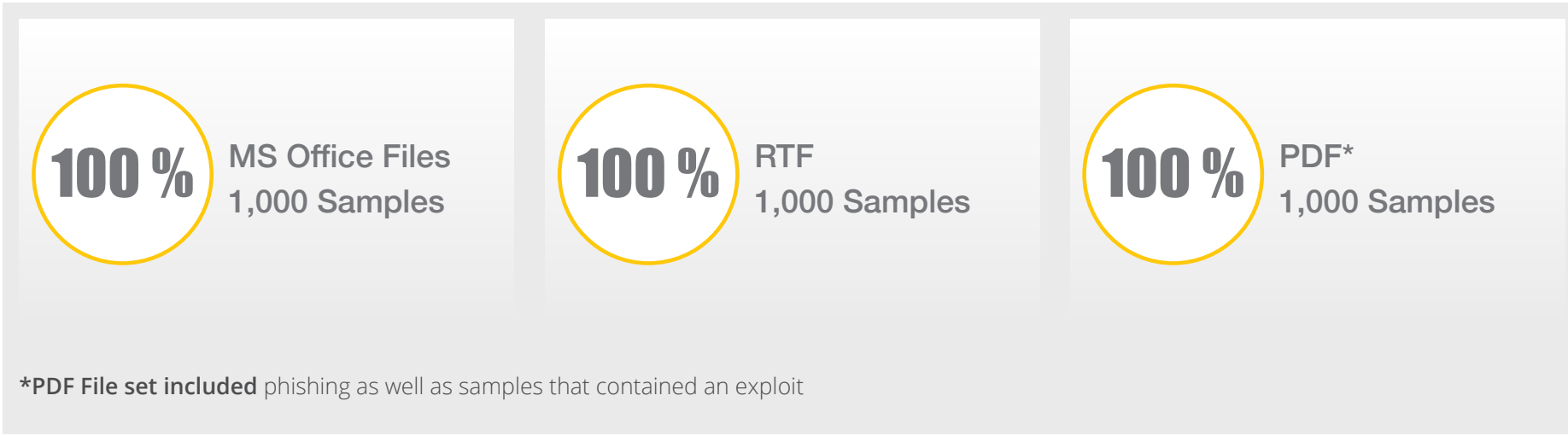
MS Office	Microsoft Office is a suite of desktop productivity applications such as Word, Excel, PowerPoint that are popular with businesses and often have malware embedded within them
RTF	A file with the .RTF file extension is a Rich Text Format file. While a normal text file stores only plain text, RTF files can include extra information about font style, formatting, images, and more. Recent attacks have taken advantage of RTF file format to infect users with malware
PDF	The Portable Document Format is a file format developed by Adobe in the 1990s to present documents, including text formatting and images, in a manner independent of application software, hardware, and operating systems. PDF file formats are popular with businesses and are also often used to distribute malware

Blue Hexagon scored 100% in overall threat detection for all these file formats.

Overall Threat Detection Score

100 %

Threat Detection Rates – By Threat Category (Documents)



***PDF File set included** phishing as well as samples that contained an exploit

3. False Positive Rates

The Blue Hexagon threat prevention platform was tested against strategic sourcing of clean files from a wide variety of categories.

Almost two million benign files were included in the test respository, ranging from Consumer applications to Enterprise tools. Also tested were documents such as PDF that are typically used in an Enterprise environment that tend to be FP candidates.

Consumer Apps	Consumer apps help consumers in their day to day tasks; they include apps for categories such as health, entertainment, finance, games, music, news, and travel
Office Documents	MS Office is a suite of desktop productivity applications such as Word, Excel, PowerPoint that are popular with businesses and often have malware embedded within them
Enterprise Apps	Enterprise apps refer to applications designated for the Enterprise space like Oracle, Sun, IBM, VMware
PDF	The Portable Document Format is a file format developed by Adobe in the 1990s to present documents, including text formatting and images, in a manner independent of application software, hardware, and operating systems
OEM Files	OEM files refer to drivers or files created/developed by device manufacturers
Signed Files	Signed files are sanctioned files digitally signed by the enterprise

Blue Hexagon had 0% False Positives, an incredible achievement, in light of the number of benign files that were tested.

False Positive Rate

0%

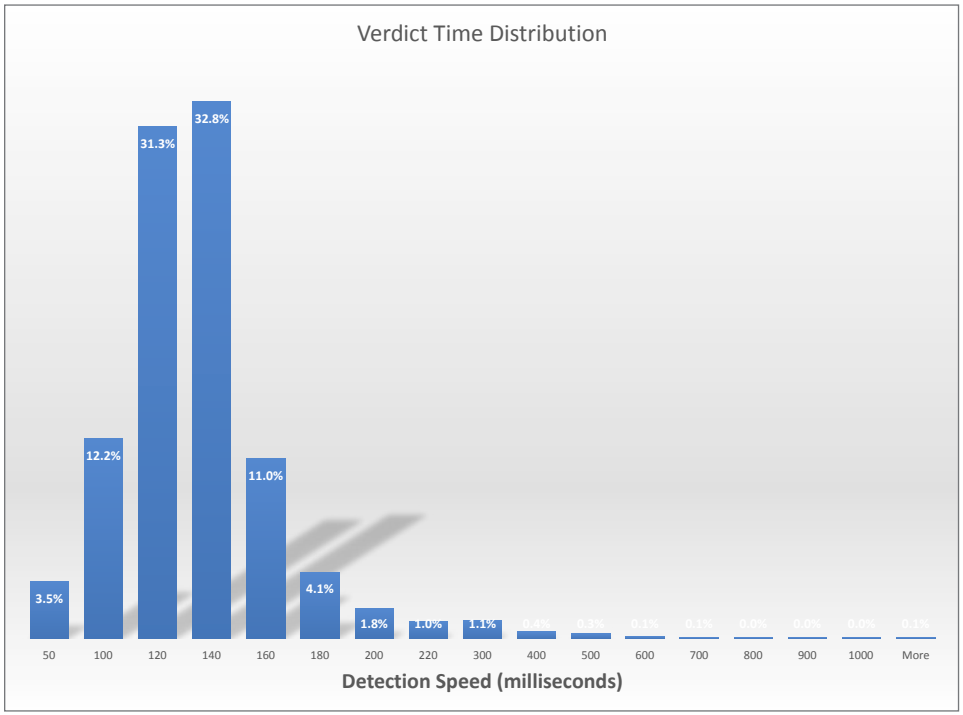
False Positive Rates – By Category

0%	Consumer Apps 100,000 Samples	0%	Enterprise* (SDK, Tools, Scripts) 100,000 Samples	0%	PDF* (Acroforms) 1,000,000 Samples
0%	Office Documents* (Docs/XLX/PPT) 300,000 Samples	0%	OEM Files (Drivers,Setup Installers) 300,000 Samples	0%	Signed Files 100,000 Samples

* Files in this category include non-PE files

4. Performance and Usability: Time to Verdict

This metric was intended to test how quickly Blue Hexagon delivered threat verdict. The chart below shows the threat detection rates across the number of samples that were tested. As observed from the chart below, the average network threat detection time was 125 ms. This includes network protocol and packet processing time, along with deep learning model verdict time.



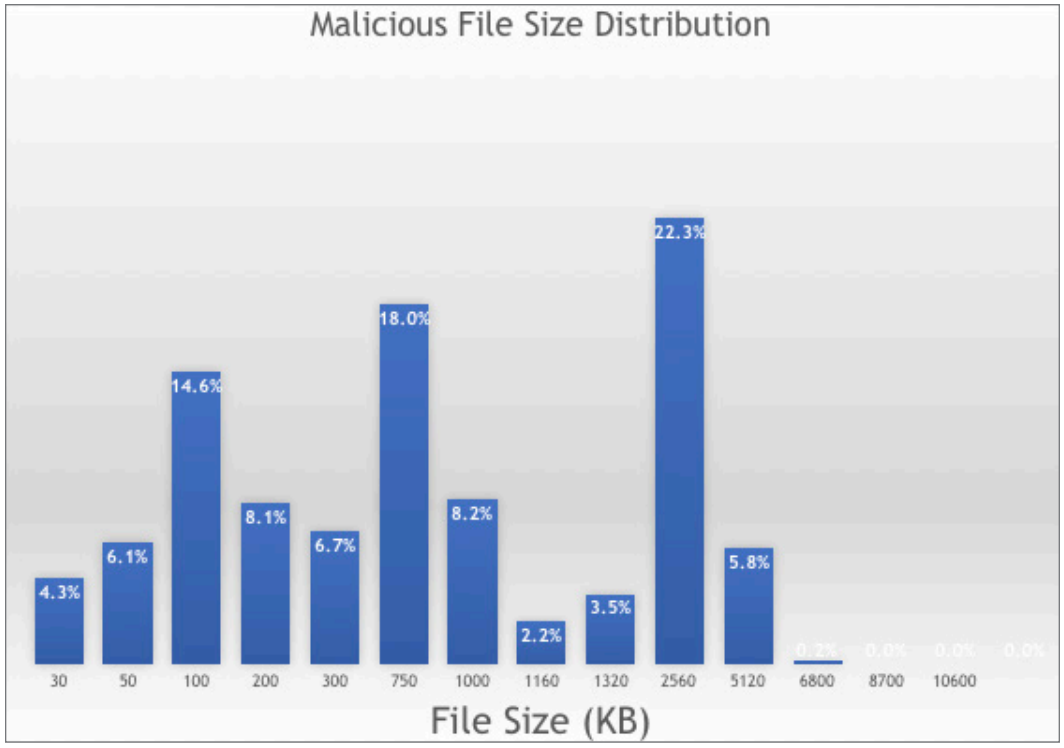
Average Threat Detection Rate

125 ms

Performance and Usability: File Size Distribution

We also tested ability of Blue Hexagon to detect threats in a wide range of file sizes. The reason this is important is because malware sandboxes can be limited by the size of files that can be submitted for “scanning”. We wanted to evaluate if an AI-centric product like Blue Hexagon suffered from this limitation.

The test files were selected from a wide range of file sizes, from 3KB all the way to large 100MB files, as seen from the chart below. Blue Hexagon was able to detect threats in this wide file distribution without any impact to the speed of threat detection or efficacy.



Conclusion

A framework to test an AI security product needs to account for the large diversity of malware that can be expected in the real world. PCSL designed such a framework to put Blue Hexagon's deep learning-powered network threat detection platform to the test. Specifically, the claims that were tested included not only efficacy of threat detection across a wide variety of threats in various file types and sizes, but also false positive rates and speed of threat detection.

Our AI test framework incorporated a strategic sourcing of malware, including a comprehensive volume of zero-days from global threat campaigns, as well as the most extensive corpus of malicious samples assembled by independent testers.

More than 40,000 threat samples from PE and document (MS Office, RTF and PDF) formats were tested. Additionally, more than 2,000,000 benign files were included in the test repository to evaluate Blue Hexagon false positive rates.

Blue Hexagon successfully detected every one of the threats we used in our AI framework. The following is a summary of the results:

- 100% threat detection rates across a wide range of threats, file sizes and file types
- 0% false positive rates
- 125 ms average threat detection speed

The results against our comprehensive testing framework demonstrates that Blue Hexagon delivers on its claims as one of the most accurate network threat detection products in the market today. Their AI-based platform showcases the speed of detection possible from non signature and non sandbox-based detection.

100 %

0 %

125 ms

Jiaxing Chenxiang Information Technology Co., Ltd., is an IT product test and consulting company located in Jiaixing, Zhejiang, P. R. China. As a professional tester of desktop security products and mobile security solutions, we are willing to provide references to users for choosing security solutions and provide security vendors with product improvement solutions and consulting services. Not only do we test security solutions for different environments, we also provide testing and consulting reports on other IT products, e.g. battery, mobile devices, computer power, etc.

Tel: +86 573 82809089
Fax: +86 573 82808561
Mail: info@pitci.com
Website: https://www.pitci.com
Address: Room 3304-3306, Building 3, NO.3339 Linggongtang Road, Jiaxing, Zhejiang, P. R. CHINA, 314000

Disclaimer

Note that before using the report issued by Jiaxing Chenxiang Information Technology Co. Ltd. (hereinafter referred to as "Chenxiang Information Technology"), please carefully read and fully understand the terms and conditions of this disclaimer (hereinafter referred to as "Disclaimer"), including the clauses of exclusion or restriction of the liabilities of Chenxiang Information Technology and the limitations of the rights of users. If you have any objection to the terms and conditions of this Disclaimer, you have the right not to use this report, the act of using this report will be regarded as acceptance and the recognition of the terms and conditions of this Disclaimer, so by using this report, you agree to the following terms and conditions:

1. The report is provided by Chenxiang Information Technology, all the contents contained herein are for reference purposes only, and will not be regarded as the suggestion, invitation, or warranty for readers to choose, purchase or use the products mentioned herein. Chenxiang Information Technology will not guarantee the absolute accuracy and completeness of the contents of the report; you should not rely solely on this report, or substitute the viewpoints of the report for your independent judgment. If you have any queries, please consult the relevant departments of the State, and then choose, purchase or use products by your independent judgment.
2. The contents contained herein is the judgment made by Chenxiang Information Technology to the product characteristics as of the date the report was published. In the future, Chenxiang Information Technology will have the right to issue new reports which contain different contents or draw different conclusions, but Chenxiang Information Technology has no obligation or responsibility to update the original report or inform readers of the update of it. In this case, Chenxiang Information Technology will bear no responsibility for readers' loss for using the original report.
3. The report may contain links to other websites, which are provided solely for the readers' convenience. The contents of the linked websites are not any part of this report. Readers shall assume the risks and losses or bear the costs when visiting such websites. Chenxiang Information Technology will not guarantee the authenticity, completeness, accuracy, and legitimacy of the contents of such websites (including but not limited to advertising, products or other information). Chenxiang Information Technology does not accept any liability (direct or indirect) for readers' damages or losses arising from their clicking on or viewing such websites to obtain some information, products, or service.
4. Chenxiang Information Technology may have or will have a business relationship with the companies which produce the products mentioned in this report, but have no obligation to notify readers about it, it doesn't matter if there has already been, or there will be such business relationship in the future.
5. The act of readers' receiving this report is not regarded as the establishment of the business relationship between readers and Chenxiang Information Technology, so there is no customer relationship existing. Chenxiang Information Technology does not accept any legal liability as the readers' customer.
6. The products which are used to be tested as samples by Chenxiang Information Technology are bought through the official channels and legal means, so the report is proper for products bought through the same, not for products bought through unofficial channels and/or illegal means. Therefore, it's the users buying such products that will be responsible for any risk or loss arising there from. Chenxiang Information Technology will not have or accept any liability whatsoever for any such risk or loss.
7. Some trademarks, photos or patterns owned by units or individuals will probably be used in this report, if you think your legal right and interests are infringed, please contact Chenxiang Information Technology promptly, Chenxiang Information Technology will handle the matter as quickly as possible.
8. Chenxiang Information Technology reserves the rights to interpret, modify, and update the Disclaimer.

Attorney: Zhejiang CongDian Law Firm