



ADVANCED ENDPOINT PROTECTION TEST REPORT

Fortinet Technologies FortiClient 6.0.3

MARCH 5, 2019

Authors – James Hasty, Justin Cole, Scott Robin

Overview

NSS Labs performed an independent test of the Fortinet Technologies FortiClient 6.0.3. The product was subjected to thorough testing at the NSS facility in Austin, Texas, based on the Advanced Endpoint Protection (AEP) Test Methodology v3.0, which is available at www.nsslabs.com. This test was conducted free of charge and NSS did not receive any compensation in return for Fortinet’s inclusion.

This report provides detailed information about this product and its security effectiveness. Additional comparative information is available at www.nsslabs.com.

As part of the initial AEP group test setup, 96 instances of the endpoint product were deployed on Windows 7 and Windows 10 operating systems. All product configurations were reviewed, validated, and approved by NSS prior to the test. Figure 1 presents the overall results of the test.

Product						3-Year Cost – 2500 Agents (US\$)		
Fortinet Technologies Fortinet FortiClient 6.0.3						\$44,009		
	HTTP	Email	Docs & Scripts	Offline Threats	Unknown Threats	Exploits	Blended Threats	Evasions
Block Rate	100%	98.5%	91.9%	93.3%	100%	100%	50.0%	100%
Additional Detection Rate	0.0%	0.3%	6.5%	6.7%	0.0%	0.0%	0.0%	0.0%

Figure 1 – Overall Test Results

Block Rate is defined as the percentage of exploits and malware blocked within 15 minutes of attempted execution. The *Additional Detection Rate* is defined as the percentage of exploits and malware detected but not blocked within 15 minutes of attempted execution.

An AEP product with a low block rate will incur less security savings, since additional operational overhead will be required to remediate the effects of a compromised system and protect the business. For detailed total cost of ownership (TCO) analysis, please see the TCO Comparative Report at www.nsslabs.com.

Table of Contents

Overview	2
Security Effectiveness	4
False Positive Rate	5
Malware.....	6
Exploits	7
Blended Threats.....	8
Resistance to Evasion Techniques	9
Resistance to Tampering Techniques	9
Additional Test Engineer Observations	10
Threat Event Reporting Criteria.....	11
Three-Year Product Acquisition Cost.....	12
Cost Information.....	12
Appendix A: Product Scorecard	13
Test Composition	13
Contributors (Samples and Techniques).....	13
Test Methodology.....	14
Contact Information	14

Table of Figures

Figure 1 – Overall Test Results.....	2
Figure 2 – False Positive Rate	5
Figure 3 – Malware (Various Delivery Methods)	6
Figure 4 – Exploits.....	7
Figure 5 – Blended Threats	8
Figure 6 – Resistance to Evasions	9
Figure 7 – Threat Event Reporting Capabilities	11
Figure 8 – Three-Year Cost (US\$).....	12
Figure 9 – Scorecard	13

Security Effectiveness

The aim of this section is to verify that the AEP product is capable of detecting, preventing, and continuously logging threats accurately, while remaining resistant to false positives. This section utilizes real threats and attack methods that are being used by cybercriminals and other threat actors, based on attacks collected from NSS' global threat intelligence network.

The ultimate goal of any attack on a computer system is to gain access to a target host and perform an unauthorized action that results in the compromise or destruction of an asset or data. Computer systems are designed with many levels of protection to prevent unauthorized access. However, intruders may use several techniques to circumvent these protections, such as targeting vulnerable services, invoking privilege escalation, or replacing key operating system files. AEP products protect against automated and manual threats by leveraging the following key capabilities:

- Inbound threat detection and prevention (prior to execution)
- Execution-based threat detection and prevention (during execution)
- Continuous monitoring post-infection and ability to act in the event of compromise (post-execution)

NSS has created a unique testing infrastructure—the NSS Labs Live Testing™ harness, which incorporates multiple product combinations, or “stacks,” within the attack chain. Each stack consists of either an operating system alone or an operating system with additional applications installed (e.g., a browser, Java, and Adobe Acrobat). This test harness continuously captures suspicious URLs, exploits, and malicious files from threat data generated from NSS and its customers, as well as data from open-source and commercial threat feeds. Captured malicious samples are further validated to confirm that they are malicious in nature. During testing, NSS combines its knowledge of a product's defensive capabilities with these samples.

An AEP product must be able to detect, prevent, continuously monitor, and take action against threats while providing end-to-end visibility through event logs generated by the endpoint product. Each type of threat (e.g., malware, exploits, blended threats, and evasions) contains unique infection vectors. This test aims to determine how effectively the AEP product can protect against a threat, regardless of infection vector or method of obfuscation. Within this report, the term “threat” is used to refer to malware, exploits, or blended threats that are able to successfully access, download, and execute on a target system, with or without subsequent post-infection compromise and/or outbound communication attempts.

One of the most common threats to the enterprise is the infection of enterprise systems by malicious software. Products were tested against threats from the following categories:

- Malware
- Blended threats
- Offline threats
- Unknown threats
- Documents and scripts
- Evasions
- Exploits
- Any combination of the above in addition to follow-on threat actions or behaviors

Each type of threat is generally deployed via one of the following common infection vectors:

- **HTTP:** These are web-based attacks where the user is deceived into clicking on a malicious link (on, for example, a web page or a banner advertisement) to download and execute malware, or where the user merely needs to visit a web page hosting malicious code in order to be infected via exploits (also known as a drive-by exploit).
- **Email (IMAP4/POP3):** These are inbound, email-based attacks where the user is deceived into clicking on a malicious link within an email to download and execute malware, or where the user is asked to visit a web page that hosts malicious code in order to be infected via exploit.

False Positive Rate

The ability of the AEP product to correctly identify and allow benign content is as important as its ability to provide protection against malicious content. NSS ran various samples of legitimate application files and documents, all of which the product was required to properly identify and allow. If any legitimate files could not be opened or executed immediately, this was recorded as a false positive. Figure 2 depicts the false positive rate for the FortiClient.

Product	False Positive Rate
Fortinet Technologies FortiClient 6.0.3	0.0%

Figure 2 – False Positive Rate

Malware

One of the most common ways in which systems are compromised is through the use of malware. Malware can infect an endpoint using numerous attack vectors or delivery methods.

Figure 3 depicts test results for malware delivered via HTTP, email, documents and scripts, offline mechanism, and previously unknown threats.

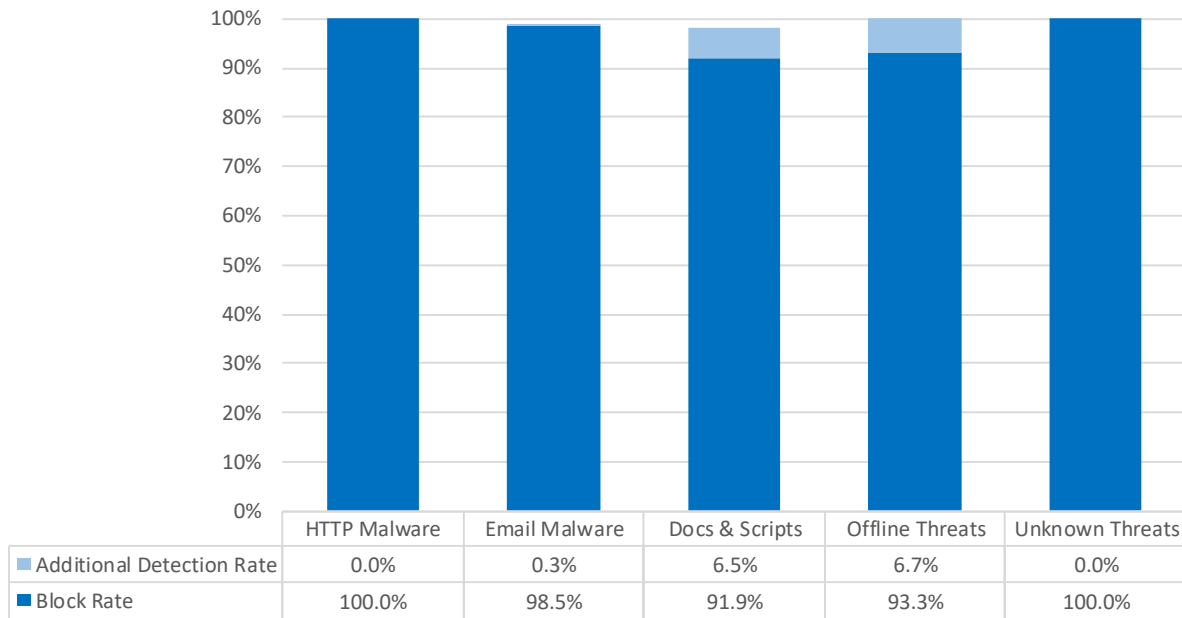


Figure 3 – Malware (Various Delivery Methods)

During testing for malware delivered via HTTP and malware delivered using email, NSS intentionally tested a large number of the same samples in order to validate whether or not the introduction mechanism had any significant impact on detection or block results. Test results demonstrate that there was no significant difference in detection and block rates regardless of introduction mechanism.

Exploits

Figure 4 depicts the results of exploit testing for the FortiClient. Exploits are defined as malicious software designed to take advantage of existing deficiencies, such as vulnerabilities or bugs, in hardware or software systems.

Figure 4 does not include results for 138 drive-by exploit test cases. Following testing, it could not be determined that these drive-by exploits executed consistently across all products in the test. However, additional analysis was performed to assess a product’s ability to detect or block drive-by exploits.

It was observed that the FortiClient can block HTTP drive-by-exploit attacks. The product’s Application Firewall module prevented users from visiting malicious websites by displaying the built-in Internet Explorer message: “This page cannot be displayed.” The product generated the following alert for these events: “MS.Windows.VBScript.Engine.Class_Terminate.Code.Execution has been blocked because it tried to receive network data.”

Other technologies and alerts exist to block exploits, but they were not observed during testing. The product’s management console did not identify the malicious domain that was navigated to in the block alert. Syslog messages corresponding to the same event gave destination IP addresses for the threat’s source.

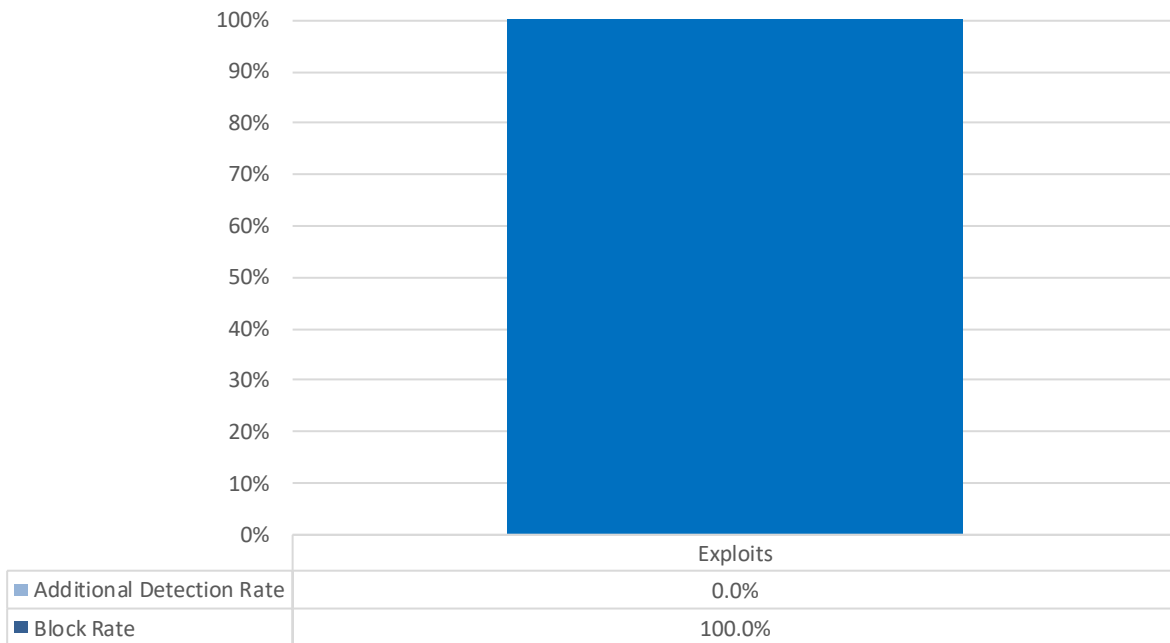


Figure 4 – Exploits

Blended Threats

Figure 5 depicts the results of blended threats testing for the FortiClient. Blended threats possess the characteristics of socially engineered malware as well as the features of legitimate applications. In these tests, all blended threats were delivered via deceptive emails. Blended threats attempt to make it difficult to distinguish between malicious and legitimate activity. Enterprises expect AEP products to be able to address this type of threat. During this testing, a series of attack techniques was used to execute code using legitimate functionality in Microsoft Office products. The same series of attack techniques was also used for 20% of the malware samples delivered via documents and scripts. Ten unique techniques were used across three different Microsoft Office applications. If the attacks were successful, the test cases deployed custom ransomware payloads.

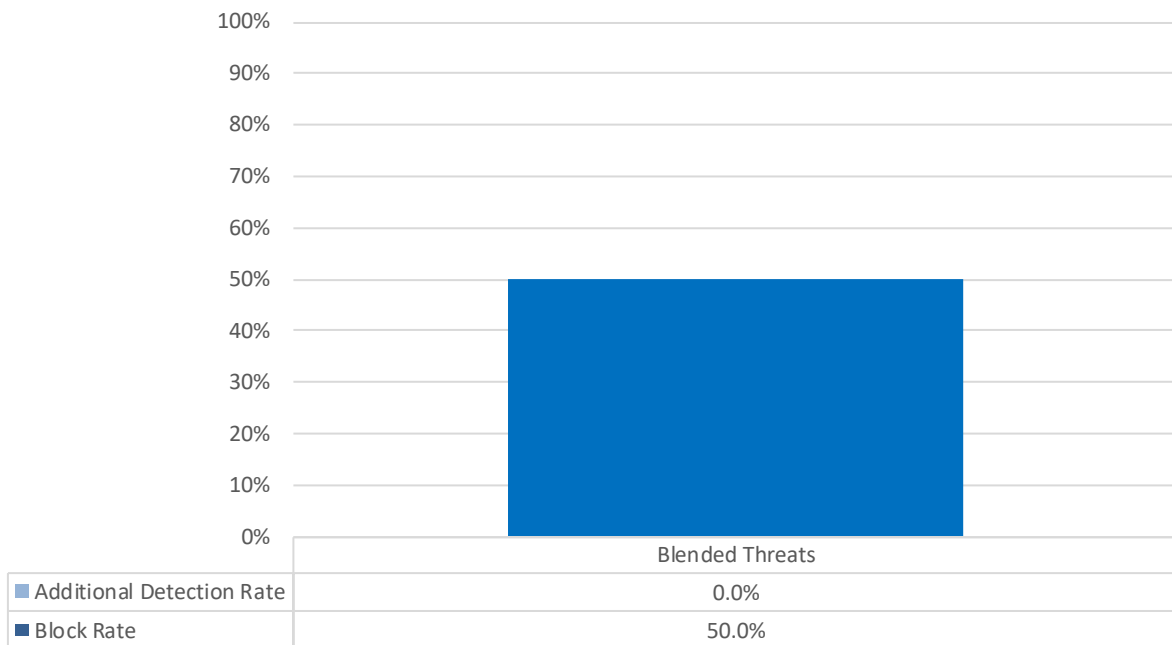


Figure 5 – Blended Threats

Resistance to Evasion Techniques

Figure 6 depicts the results of evasions testing for the FortiClient. Cybercriminals deploy evasion techniques to disguise and modify attacks at the point of delivery in order to avoid detection by AEP products. If an AEP product fails to correctly identify a specific type of evasion, an attacker can potentially deliver malware that the product would normally detect. Attackers can modify attacks and malicious code in order to evade detection in a number of ways.

This test aims to verify that the AEP product is capable of detecting, preventing, and continuously monitoring threats and that it is able to take action against malware, exploits, and blended threats when subjected to common evasion techniques. Please contact NSS for information on the evasions utilized.

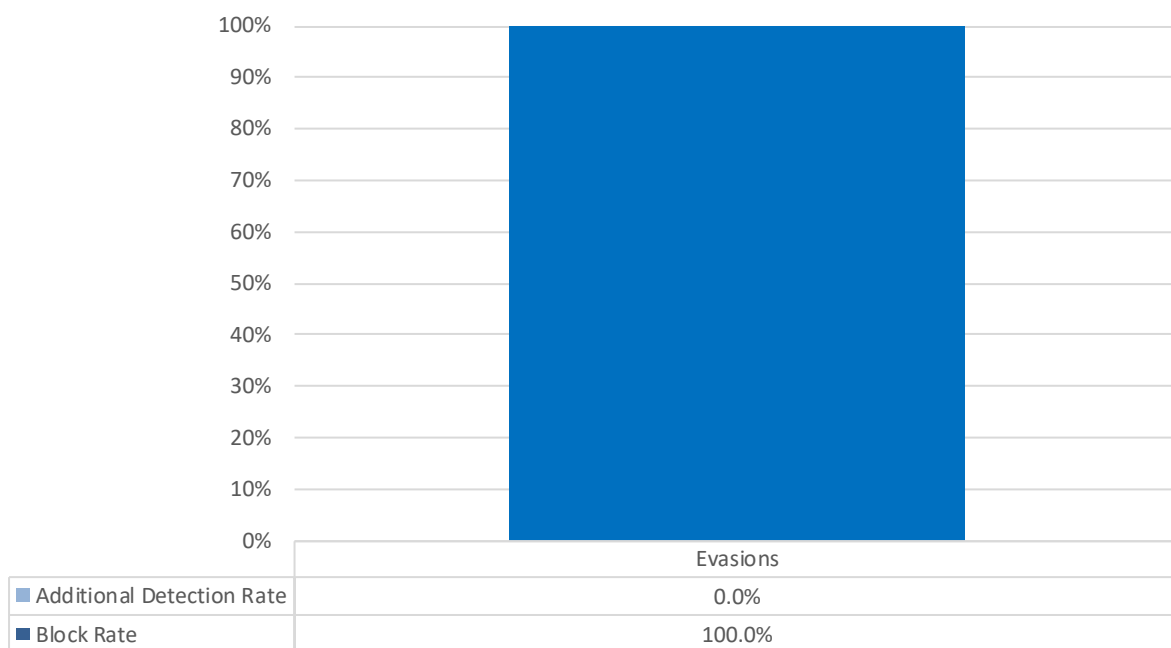


Figure 6 – Resistance to Evasions

Resistance to Tampering Techniques

This test measured whether a product was vulnerable to tampering techniques that target the product itself. The following techniques were leveraged during testing:

- Disabled the product through the GUI or command line
- Disabled protections by using a combination of Windows Service Functions or process termination
- Uninstalled the product using traditional Windows-installed software removal methods and the product’s own installer/uninstaller files
- Used DLL hijacking to execute code and disable protections with an arbitrary DLL

All of these tampering techniques leverage administrator privileges. In enterprises where users are not granted administrator privileges, privilege escalation exploits (such as those utilized during this testing) would allow similar outcomes.

When tampering techniques were utilized, at least one potential issue or security vulnerability was discovered in each product tested.

Additional Test Engineer Observations

The FortiClient provides information about threats that have occurred, the status of updates, and the product and engine version the endpoint is running. In this test, the on-premises management console, FortiClient Enterprise Management Server, was tested, but Fortinet also offers a cloud-based management console. The on-premises console has an interesting feature where administrators can track software installed on all endpoints using the Software Inventory section. FortiClient's FortiSandbox sends files to Fortinet for analysis before they are allowed to run on the endpoint. The timeout value is configurable, and IT administrators can allow a file to run on an endpoint, or deny it, once the timeout value expires. The console does not provide a graphical representation of the attack chain that occurs on compromised endpoints.

Threat Event Reporting Criteria

During TCO evaluations, it is important to understand an AEP product’s reporting capabilities, as these capabilities can vary among products. Figure 7 presents data that is used in the Security Value Map™ (SVM) calculations for the FortiClient. Please refer to the TCO and SVM Comparative Reports for more detail.

Threat Event Reporting Capabilities	Score
Management Console	
Lists hostname or IP address of compromised endpoint?	Yes
Lists URL of source of threat?	Yes
Lists hash of file binaries?	Yes
Lists file path of threats?	Yes
Lists outbound IPs?	Yes
Conveys difference between detection and block?	Yes
Provides detail about reason for conviction?	Yes
Syslog Messages	
Lists hostname or IP address of compromised endpoint?	Yes
Lists URL of source of threat?	Yes
Lists hash of file binaries?	Yes
Lists file path of threats?	Yes
Lists outbound IPs?	Yes
Conveys difference between detection and block?	Yes
Provides detail about reason for conviction?	Yes
Syslog Alternative (API, Splunk Connector, etc.)	Yes
Additional Forensics Capabilities	Yes*
Describes registry changes in the management console?	Yes
Provides view of shell commands in the management console?	No*
Provides threat attack chains/trees in the management console?	No

Figure 7 – Threat Event Reporting Capabilities

*The Fortinet FortiSIEM product is available at an additional cost to provide additional syslog and endpoint detection and response capabilities.

Three-Year Product Acquisition Cost

Implementation of AEP products can be complex, with several factors affecting the overall cost of deployment, maintenance, and upkeep. All of these factors should be considered over the course of the useful life of a product, as well as any of its components and any application or service that is leveraged during testing.

- **Product purchase** – The cost of acquisition
- **Product maintenance** – The fees paid to the vendor (including software, maintenance, and updates)
- **Installation** – The time required to configure the product, deploy it in the network, apply updates and patches, and set up desired logging and reporting

For the purposes of this report, capital expenditure (capex) items (the cost of acquisition and installation) are included for only 2,500 agents.

Cost Information

Calculations are based on vendor-provided pricing information. Where possible, the 24/7 maintenance and support option with 24-hour replacement is used, since this is the option typically selected by enterprise customers. Prices depicted include the purchase and maintenance costs for 2,500 software agents only; costs for central management solutions (CMS) may be extra. Please contact NSS for additional detail. Year 1 Cost includes an additional \$600 installation cost that was applied to all products in the test.

Product	Year 1 Cost	Year 2 Cost	Year 3 Cost	3-Year TCO
Fortinet FortiClient 6.0.3	\$15,070	\$14,470	\$14,470	\$44,009

Figure 8 — Three-Year Cost (US\$)

For additional TCO analysis, including operational costs, refer to the AEP TCO Comparative Report, which is available at nsslabs.com.

Appendix A: Product Scorecard

Tests	Samples ¹	Test Results (%) ²	
False Positives (detection accuracy)	1,053	0.0%	
Malware (various delivery mechanisms)	Percentage of Total Samples	Block Rate	Additional Detection Rate
HTTP	29.1%	100.0%	0.0%
Email	50.5%	98.5%	0.3%
Documents and Scripts	6.9%	91.9%	6.5%
Offline Threats	1.7%	93.3%	6.7%
Unknown Threats	2.5%	100.0%	0.0%
Exploits	1.9%	100.0%	0.0%
Blended Threats	2.9%	50.0%	0.0%
Evasions	4.6%	100.0%	0.0%

Figure 9 – Scorecard

Test Composition

Each product was initially tested against 1,629 unique malicious samples and 1,061 unique false positive samples. Ultimately, 897 unique malicious samples and 1,053 unique false positive samples met NSS’ validation criteria and were included as part of the test.

Contributors (Samples and Techniques)

Jorge Damian, Eric Llana, Faiz Merchant, Edsel Valle, Kevin Valle

¹ No product is able to provide 100% protection against attacks. A single successful attack is often all an attacker needs to gain unauthorized access, infiltrate an organization, and steal or destroy data.

² *Block Rate* is defined as the percentage of exploits and malware blocked within 15 minutes of attempted execution. The *Additional Detection Rate* is defined as the percentage of exploits and malware detected but not blocked within 15 minutes of attempted execution.

Test Methodology

NSS Labs Advanced Endpoint Protection (AEP) Test Methodology v3.0

NSS Labs Evasions Test Methodology v1.2

Copies of the test methodologies are available at www.nsslabs.com.

Contact Information

NSS Labs, Inc.

3711 South Mopac Expressway

Building 1, Suite 400

Austin, TX 78746

info@nsslabs.com

www.nsslabs.com

This and other related documents are available at: www.nsslabs.com. To receive a licensed copy or report misuse, please contact NSS Labs.

© 2019 NSS Labs, Inc. All rights reserved. No part of this publication may be reproduced, copied/scanned, stored on a retrieval system, e-mailed or otherwise disseminated or transmitted without the express written consent of NSS Labs, Inc. (“us” or “we”).

Please read the disclaimer in this box because it contains important information that binds you. If you do not agree to these conditions, you should not read the rest of this report but should instead return the report immediately to us. “You” or “your” means the person who accesses this report and any entity on whose behalf he/she has obtained this report.

1. The information in this report is subject to change by us without notice, and we disclaim any obligation to update it.
2. The information in this report is believed by us to be accurate and reliable at the time of publication, but is not guaranteed. All use of and reliance on this report are at your sole risk. We are not liable or responsible for any damages, losses, or expenses of any nature whatsoever arising from any error or omission in this report.
3. NO WARRANTIES, EXPRESS OR IMPLIED ARE GIVEN BY US. ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, ARE HEREBY DISCLAIMED AND EXCLUDED BY US. IN NO EVENT SHALL WE BE LIABLE FOR ANY DIRECT, CONSEQUENTIAL, INCIDENTAL, PUNITIVE, EXEMPLARY, OR INDIRECT DAMAGES, OR FOR ANY LOSS OF PROFIT, REVENUE, DATA, COMPUTER PROGRAMS, OR OTHER ASSETS, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.
4. This report does not constitute an endorsement, recommendation, or guarantee of any of the products (hardware or software) tested or the hardware and/or software used in testing the products. The testing does not guarantee that there are no errors or defects in the products or that the products will meet your expectations, requirements, needs, or specifications, or that they will operate without interruption.
5. This report does not imply any endorsement, sponsorship, affiliation, or verification by or with any organizations mentioned in this report.
6. All trademarks, service marks, and trade names used in this report are the trademarks, service marks, and trade names of their respective owners.