

**ProSecure™ UTM10 Unified Threat Management Appliance:
Malware Detection Evaluation Versus Fortinet, Inc., SonicWALL, Inc., and
WatchGuard Technologies, Inc.**

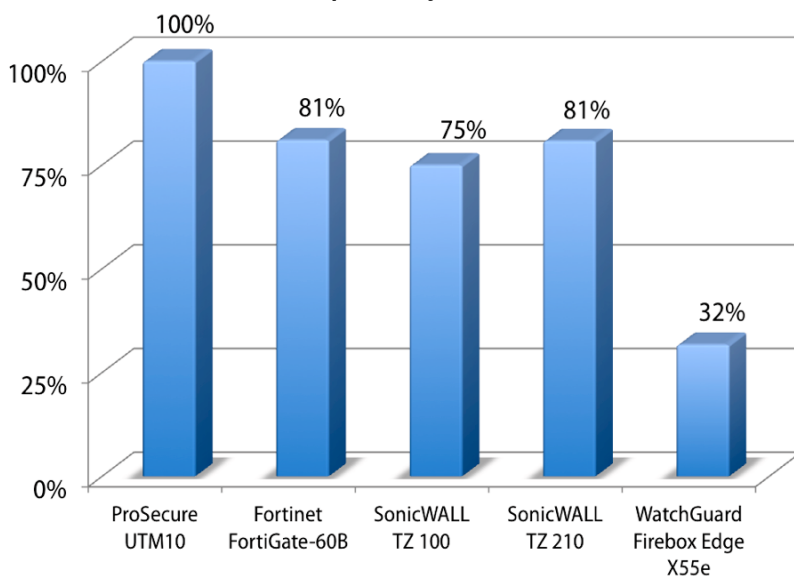
EXECUTIVE SUMMARY

Unified Threat Management (UTM) appliances aimed at small and medium businesses should deliver protection right out of the box against malware threats propagating on the Internet. Tests show that the ProSecure UTM10 appliance achieved a 100% detection rate for The WildList Organization International's latest list of viruses 'propagating in the wild', and up to 90% detection of other important Win32 malware tested over HTTP, SMTP and POP3 protocols. These results outperform those of the competing, sometimes pricier, UTM appliances tested from Fortinet, SonicWALL and WatchGuard.

THE BOTTOM LINE

- 1** ProSecure UTM10 detected 100% of the WildList malware (viruses and worms), and 90.15% of other major Win32 malware (sometimes called 'zoo malware'), tested
- 2** SonicWALL TZ 100 appliance detected just 74.97% of the WildList malware, and detected just 34.54% of the zoo malware tested
- 3** SonicWALL TZ 210 appliance detected just 80.83% of WildList malware, and just 62.74% of the zoo malware tested
- 4** Fortinet FortiGate-60B appliance detected just 81% of WildList malware, and just 24.97% of the zoo malware tested
- 5** WatchGuard Firebox Edge X55e appliance detected just 31.73% of the WildList malware, as well as just 21.24% of the zoo malware tested

WildList Malware Detection Rate Over HTTP
(As Reported by AV-Test)



Note: Based on the detection of 3,583 viruses and worms based on WildList Organization International's July 2009 WildList list of viruses and worms.

Source: Tolly/AV-Test, August 2009

Figure 1



Background

Growing businesses (30 users or less) are more sensitive than large enterprises to the cost of providing the best security. Unified Threat Management (UTM) appliances are very appealing to such businesses due to the combination of convenience and cost savings of having a single appliance to manage to protect multiple vectors (anti-malware, firewall, Web filtering, etc.) As the same appliance is providing multiple security services,

UTM vendors sometimes compromise on the resource intensive security functions like anti-virus/anti-malware protection in the default configuration. But simply because the businesses are looking for value, does not mean that they need to settle for a lowered bar for protection out of the box.

Tolly engineers, in collaboration with AV-Test GmbH - a leading authority on anti-malware research and testing, evaluated the malware detection accuracy of ProSecure UTM10, Fortinet FortiGate-60B,

NETGEAR, Inc.

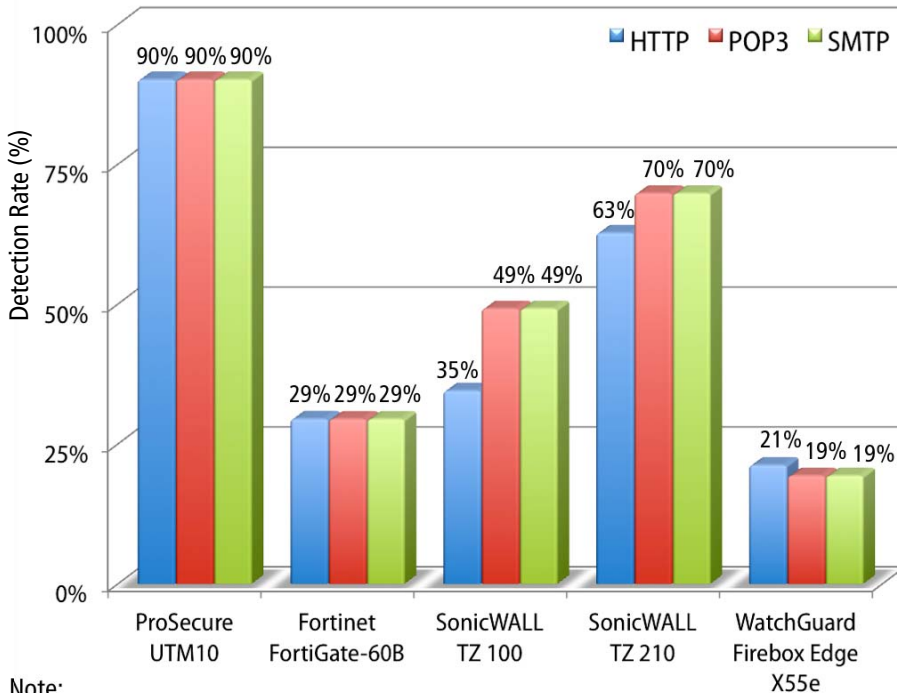
ProSecure™ UTM10

Malware Detection Evaluation



Tested August 2009

Zoo Malware Detection Result Comparison Using HTTP, POP3 and SMTP Protocols (As Reported by AV-Test)



Note:

- Tests were performed using one protocol at a time.
- Adware/spyware, backdoors, trojans, bots/zombies, viruses, worms, etc. are sometimes collectively referred to as Zoo malware.
- All zoo malware tests were performed by AV-Test GmbH, using 60,000 samples collected by AV-Test from all over the world, comprised of a wide range of threats propagating on the Internet
- SonicWALL products used the same Appliance OS version and the latest signatures at the time of testing, but contained different number of signatures in their default configuration, likely resulting in different detection rates.

Source: Tolly/AV-Test, August 2009

Figure 2

Tested in collaboration with AV-Test GmbH



AV-Test GmbH is a leading worldwide IT security testing and consultancy services provider.

Located in Magdeburg, Germany, the AV-Test team has more than 15 years of experience in the area of anti-virus research and data security, and is an active member of Anti-Malware Testing Standards Organization (AMTSO).

For more details on AV-Test, please visit <http://av-test.org>.

Source: AV-Test GmbH



Detailed Summary of Malware Detection over HTTP Protocol
(As Reported by AV-Test)

	Malware Samples Tested	ProSecure UTM10		Fortinet FortiGate-60B		SonicWALL TZ 100		SonicWALL TZ 210		WatchGuard Firebox Edge X55e	
		Malware Detected Number	Malware Detected %	Malware Detected Number	Malware Detected %	Malware Detected Number	Malware Detected %	Malware Detected Number	Malware Detected %	Malware Detected Number	Malware Detected %
WildList Malware	3,583	3,583	100%	2,903	81%	2,686	75%	2,896	81%	1,137	32%
File viruses and worms (Win32)	3,461	3,461	100%	2,848	82%	2,680	77%	2,872	83%	1,121	32%
Macro viruses (MS Office)	102	102	100%	44	43%	1	1%	9	9%	11	11%
Script viruses (JS, VBS)	20	20	100%	11	55%	5	25%	15	75%	5	25%
Other important Win32 malware (aka 'zoo malware')	60,000	54,090	90%	17,682	29%	20,724	35%	37,646	63%	12,746	21%
Ad-/Spyware	10,000	5,894	59%	644	6%	1,759	18%	6,019	60%	358	4%
Backdoors	10,000	9,572	96%	3,056	31%	2,268	23%	5,637	56%	1,863	19%
Bots (Zombies)	10,000	9,452	95%	1,724	17%	3,761	38%	6,340	63%	838	8%
Trojan Horses	10,000	9,386	94%	1,691	17%	3,325	33%	5,948	59%	896	9%
Viruses	10,000	9,980	100%	6,079	61%	4,231	42%	5,770	58%	5,710	57%
Worms	10,000	9,806	98%	4,488	45%	5,380	54%	7,932	79%	3,081	31%

Note:

- WildList malware tested were the variants of viruses and worms propagating in the wild, and listed on The WildList Organization International's July 2009 issue of WildList.
- The zoo malware were collected by AV-Test GmbH from all around the world, representing the most prevalent threats propagating around the Internet.
- SonicWALL products used the same Appliance OS version and the latest signatures at the time of testing, but contained different number of signatures in their default configuration, likely resulting in different detection rates.

Source: Tolly/AV-Test, August 2009

Figure 3

SonicWALL TZ 100, SonicWALL TZ 210 and WatchGuard Firebox Edge X55e UTM appliances. Tests focused on the malware detection capabilities of the above mentioned UTM appliances using their default security policies, over the Web traffic and email vectors using HTTP, POP3 and SMTP protocols. Test malware samples consisted of The WildList

Organization International's latest WildList (a list of viruses and worms found propagating on the Internet) along with other major Win32 malware. Figures 1 and 2 show that the ProSecure UTM10 provided best malware detection out of the devices tested, across all the malware categories and protocols tested.

WildList Malware Detection

The WildList Organization International publishes the WildList, a periodical list of viruses and worms propagating on the Internet. This WildList for July 2009 (released in August 2009) used for this test represented the latest WildList available at the time of testing. While



**Detailed Summary of Malware Detection over POP3 and SMTP Protocol
(As Reported by AV-Test)**

	Malware Samples Tested	ProSecure UTM10		Fortinet FortiGate-60B		SonicWALL TZ 100		SonicWALL TZ 210		WatchGuard Firebox Edge X55e	
		Malware Detected Number	Malware Detected %	Malware Detected Number	Malware Detected %	Malware Detected Number	Malware Detected %	Malware Detected Number	Malware Detected %	Malware Detected Number	Malware Detected %
WildList Malware	3,583	3,583	100%	2,903	81%	3,110	87%	3,240	90%	1,096	31%
File viruses and worms (Win32)	3,461	3,461	100%	2,848	82%	3,016	87%	3,135	91%	1,081	31%
Macro viruses (MS Office)	102	102	100%	44	43%	88	86%	90	88%	11	11%
Script viruses (JS, VBS)	20	20	100%	11	55%	6	30%	15	75%	4	20%
Other important Win32 malware (aka 'zoo malware')	60,000	54,090	90%	17,666	29%	29,509	49%	41,886	70%	11,600	19%
Ad-/Spyware	10,000	5,894	59%	642	6%	3,982	40%	6,902	69%	355	4%
Backdoors	10,000	9,572	96%	3,054	31%	3,832	38%	6,448	64%	1,807	18%
Bots (Zombies)	10,000	9,452	95%	1,723	17%	4,672	47%	6,987	70%	787	8%
Trojan Horses	10,000	9,386	94%	1,690	17%	4,961	50%	6,799	68%	877	9%
Viruses	10,000	9,980	100%	6,072	61%	4,931	49%	6,237	62%	4,706	47%
Worms	10,000	9,806	98%	4,485	45%	7,131	71%	8,513	85%	3,068	31%

Note:

- Tests were first done over POP3 protocol, and then using SMTP protocol. Test results were identical.
- WildList malware tested were the variants of viruses and worms propagating in the wild, and listed on The WildList Organization International's July 2009 issue of WildList.
- The zoo malware were collected by AV-Test GmbH from all around the world, representing the most prevalent threats propagating around the Internet.
- SonicWALL products used the same Appliance OS version and the latest signatures at the time of testing, but contained different number of signatures in their default configuration, likely resulting in different detection rates.

Source: Tolly/AV-Test, August 2009

Figure 4

new viruses and worms get released all the time, detection for the latest WildList gives a good idea about the currency and breadth of protection offered by the UTM appliances in their default security policy with the latest security updates. Figures 1 through 4 show that ProSecure detected 100% of the WildList malware on HTTP, POP3 and SMTP protocols.

In contrast, the closest performing competitor in detecting WildList malware over HTTP traffic was Fortinet FortiGate-60B with about 81% detection. In the same test, SonicWALL's TZ 100 and TZ 210 appliances detected about 75% and 81% of the WildList malware; and the WatchGuard appliance performed the worst of the field, by detecting just about 32% of the WildList malware.

When testing the WildList malware detection over POP3 and SMTP protocols, ProSecure's competitors once again demonstrated lower detection. In contrast to ProSecure's 100% detection, SonicWALL's TZ 210 and TZ 100 appliances detected around 90% and 87% respectively; followed by Fortinet FortiGate-60B with around 81% detection and WatchGuard Firebox Edge X55e once again detecting



Polymorphic Viruses

Polymorphic viruses try to avoid detection by anti-virus tools by constantly changing [or mutating] their code and/or using encryption upon successful infection. It is a constant battle between the detection technology from anti-virus researchers and the evasion techniques used by virus writers to constantly stay one step ahead of each other.

The WildList viruses and worms include polymorphic variants, and a high detection rate for the latest WildList malware indicates that an anti-malware product is providing effective protection against the latest threats on the Internet.

Source: Tolly

the least malware - around 31% - among the appliances under test.

This shows that ProSecure UTM10 offered the best WildList malware detection over HTTP, POP3 and SMTP protocols, among the UTM appliances tested.

Zoo Malware Detection

Engineers also tested UTM appliances under test with 60,000 samples of other major Win32 malware (adware/spyware, backdoors, bots/zombies, trojan horses, viruses and worms) sometimes referred to as 'zoo malware'.

These malware samples were collected by AV-Test GmbH from all over the world, and represent other major Win32 malware propagating on the Internet. These malware samples complement the WildList malware samples. Tests once again examined the malware detection over HTTP, POP3 and SMTP protocols.

Test results show that the ProSecure UTM10 once again achieved the best detection of ~90% of the zoo malware over HTTP, POP3 and SMTP protocols, while its competitors detected just between just 19% and around 70%. See Figures 2 to 4.

When testing detection of zoo malware over HTTP protocol, ProSecure's UTM10 detected ~90% of the zoo malware, followed by SonicWALL's TZ 210 and TZ 100 appliances with ~63% and ~35% detection; followed by Fortinet FortiGate-60B detecting just ~30% of the malware. WatchGuard Firebox Edge X55e detected the least amount of malware, at just ~21%.

Similar results were observed while testing detection of zoo malware over POP3 and SMTP protocols, with ProSecure's UTM10 detecting the most zoo malware at ~90%. SonicWALL's TZ 210 and TZ 100 appliances detected just ~70% and ~49% respectively, of the zoo malware tested. Fortinet's FortiGate-60B

Devices Under Test and Version Info

Developer, Distributor	NETGEAR, Inc.	Fortinet, Inc.	SonicWALL, Inc.	SonicWALL, Inc.	WatchGuard Technologies, Inc.
Product name	UTM10	FortiGate-60B	TZ 100	TZ 210	Firebox Edge X55e
Language of the tested version	English	English	English	English	English
Appliance OS version	1.0.0-31	4.0.3, build0106, 090616	SonicOS Enhanced 5.3.0.1-17o	SonicOS Enhanced 5.3.0.1-17o	10.2.10 build 229975
Appliance OS date	2009-08-11	2009-06-16	n/a	n/a	2009-07-07
Signature version	200908251432	10.00755	Signature Database Timestamp UTC 08/24/2009 15:21:05.000	Signature Database Timestamp UTC 08/24/2009 15:21:05.000	51.9734
Signature date*	August 25th, 2009	August 25th, 2009	August 24th, 2009	August 24th, 2009	August 24th, 2009

Note:

- The appliances were updated to their latest software/signature levels within a small window of time on August 25th, 2009, and then isolated from the Internet to set the appliance configuration in stone. The signature date shown indicates the latest available signature set at the time of the update on August 25th.

Source: Tolly/AV-Test, August 2009

Figure 5

appliance followed, detecting just 29% of the zoo malware, and WatchGuard Firebox Edge X55e once again detected the least amount of malware at just ~19%.

The zoo malware detection tests once again show ProSecure UTM10's superior malware detection over the competing UTM appliances tested, using the default security policies.

TEST SETUP AND METHODOLOGY

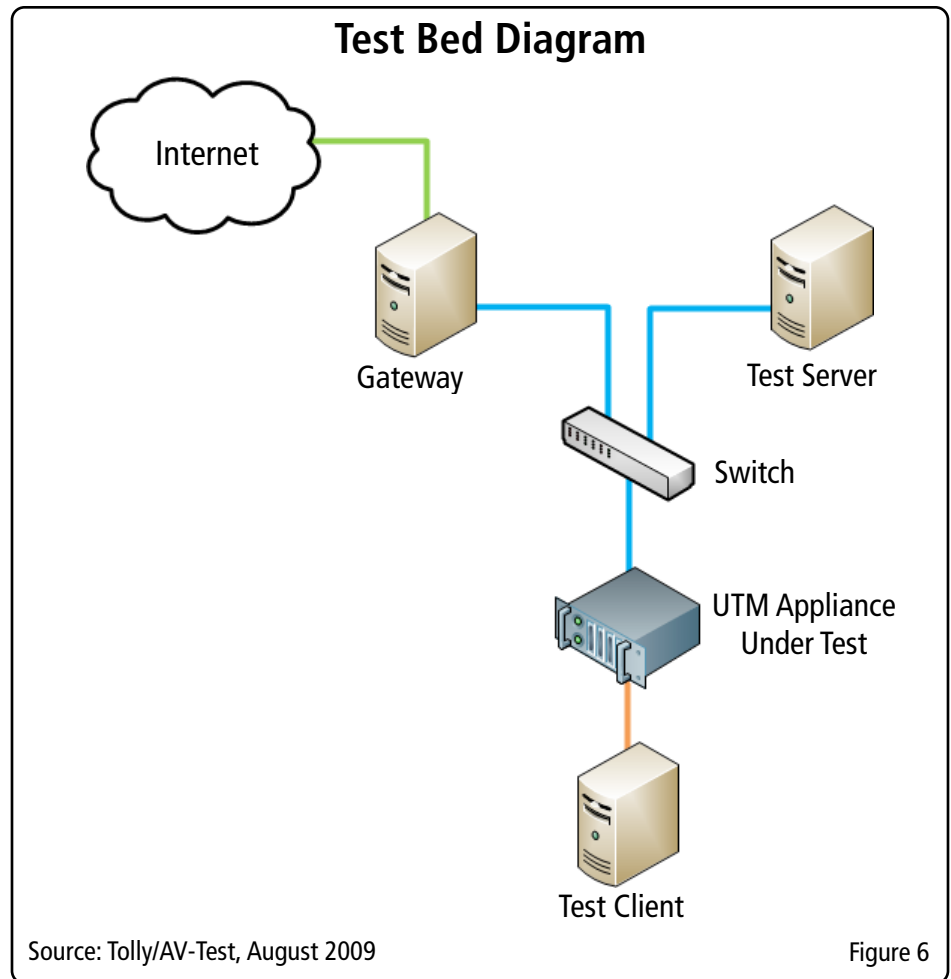
Test Bed Setup

Tolly tested competing Unified Threat Management (UTM) appliances from ProSecure, Fortinet, SonicWALL and WatchGuard. See Figure 5 for detailed information on the software and hardware version of the appliances tested. All the appliances were tested with their default security policies with the latest security updates as of the day of testing, with the appliances in a transparent proxy mode in the test network.

The test bed diagram to test each appliance under test looked as shown in Figure 6, and consisted of the following components:

Test Client

The client was running as a virtual machine (VM) running under VMware Workstation (version 6.0.2 build 59824). The client VM was configured with one CPU, 768 MB RAM, 200 GB growable virtual disk, a DVD-ROM drive, and one virtual network adapter, and ran Microsoft Windows XP SP2 operating system and a custom-developed HTTP



test client.

The physical PC running the client VM was equipped with an Intel Core 2 Duo 6600 CPU, 3GB RAM, 400 GB 7200 RPM HDD, one DVD-ROM, a floppy drive, an on-board Gigabit Ethernet network adapter, and Microsoft Windows Server 2003 operating system.

Test Server

The hardware configuration of the server was identical to the test client mentioned above. The operating system was Ubuntu Server 7.10 (kernel ver. 2.6.24-16-server), with the following services running:

- Apache 2 server running PHP5 to automate several preparation tasks
- Another Apache 2 server to provide virtual domains
- PowerDNS to provide name resolution services

Gateway

To provide Internet access, the gateway PC is connected to a DSL line. The PC was running Ubuntu Server 7.10 (kernel ver. 2.6.22-15-server), and was equipped with an AMD Athlon 64 3500+ CPU, 1 GB RAM, 250 GB 7200 RPM hard disk, DVD-ROM, floppy drive, a Marvell Gigabit Ethernet PCI network adapter, as well as



an onboard 100 Mbps network adapter. The Gateway was configured to provide DNS resolution with BIND (version 9.4.1-P1-3ubuntu2), and Internet connection (ICPM, TCP port 80, 443) services.

Test Methodology

Before the start of the tests, the appliances under test were updated with the latest security updates from the corresponding vendors. Once the updates were performed, the appliances were disconnected from the Internet to prevent further changes to the test configuration. The appliances were configured with their default security policies as shipped by their vendor.

There were two network segments used for the test; an internal and an external segment. The test client PC and the internal network side of the appliance under test, constitute the internal network segment. The external side of the appliance and the test server constitute the external network segment. The test server provided the WildList and zoo malware test samples.

To start a certain test, the client connects to the test server and specifies to the

server the test that needs to be performed. The server then creates the necessary settings and prepares the backend for the test. When the preparation is complete the client starts the test procedure.

While testing each protocol (HTTP or POP3 or SMTP) the client will fetch a list of files that should be transferred from the server. After the list is completely transferred the client will start to download the listed files one by one and create detailed log files which can be used for further analysis. The log files include MD5 checksums and HTTP response codes. All content that passes the appliance gets saved into ZIP archives for further analysis later.

After the test is completed, the created log files are analyzed by comparing the MD5 checksum of the backend server content with the MD5 checksum of the fetched data. If they are equal the content is considered to have been transferred without errors. If the checksums do not match, the file is considered to have been modified.

A fully transferred test file will be counted as a failure of the appliance under test to

block the malware. In the case of partially fetched data, further checks of that data can be done. These checks are not included in the standard procedure. If there is nothing left for calculating a MD5 checksum, the corresponding file is counted as blocked.

Sometimes, appliances present a block page to the user instead of transferring the file content. This block page content is also saved and would be counted towards the number of malware blocked successfully.

The fetched data is further analyzed in several ways:

- Simple check of the fetched data against a multi-scanner system, which will scan the files with approx. 30 different anti-virus command line scanners. The results of this scan show if the fetched data is still recognized as malicious content.
- Semiautomated dynamic analysis by executing the file in a sandbox environment and trace if the sample is still executable and if so which actions are done.
- Manual static analysis by using a disassembler.

About ProSecure™

ProSecure™ Gateway Security Appliances employ a best-of-breed security architecture that provides up to 400x the virus and malware coverage over other solutions at speeds up to 5x faster using patent-pending Stream Scanning Technology.

ProSecure has forged security technology partnerships with industry-leading Kaspersky Lab, Commtouch®, Mailshell™, and Sophos™ to bring best-of-breed enterprise-strength Anti-virus, Anti-spam, and Web filtering security technologies to the UTM and STM platforms.

For more information please visit www.prosecure.netgear.com.

Source:
ProSecure™

Security Architecture by NETGEAR



About Tolly

The Tolly Group companies have been delivering world-class IT services for 20 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.

You can reach the company via E-mail at sales@tolly.com, or via telephone at +1 561.391.5610.

Visit Tolly on the Internet at:
<http://www.tolly.com>

Interaction with Competitors

In accordance with The Tolly Group's Fair Testing Charter, Tolly representatives contact competing vendors to participate in the testing. Since the competing vendor products in this test were being tested in their default configuration, Tolly personnel did not engage the representatives of Fortinet, Inc., SonicWALL, Inc., and WatchGuard Technologies, Inc.



For more information on the Tolly Fair Testing Charter, visit:
<http://www.tolly.com/FTC.aspx>

Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is", and Tolly Enterprises, LLC (Tolly) 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 herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com. No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. 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.