TEST REPORT

Tolly.

#216143

September 2016

Commissioned by
SiteLock, LLC

SiteLock® SMART™ (Secure Malware Alert & Removal Tool)

Web-based Malware Comparison Versus McAfee Complete Endpoint Protection Suite

EXECUTIVE SUMMARY

Traditional endpoint security is an essential part of any enterprise security strategy, but, today, is it enough? Hackers work 24x7 to exploit systems any way that they can. Web applications are publicly visible, and frequently contain vulnerabilities, making them a prime target.

SiteLock, LLC commissioned Tolly to evaluate the SiteLock SMART web-based malware protection solution and compare its effectiveness to the McAfee Complete Endpoint Protection Suite. Testing focused on evaluating how effective each solution was at detecting and removing web-based malware.

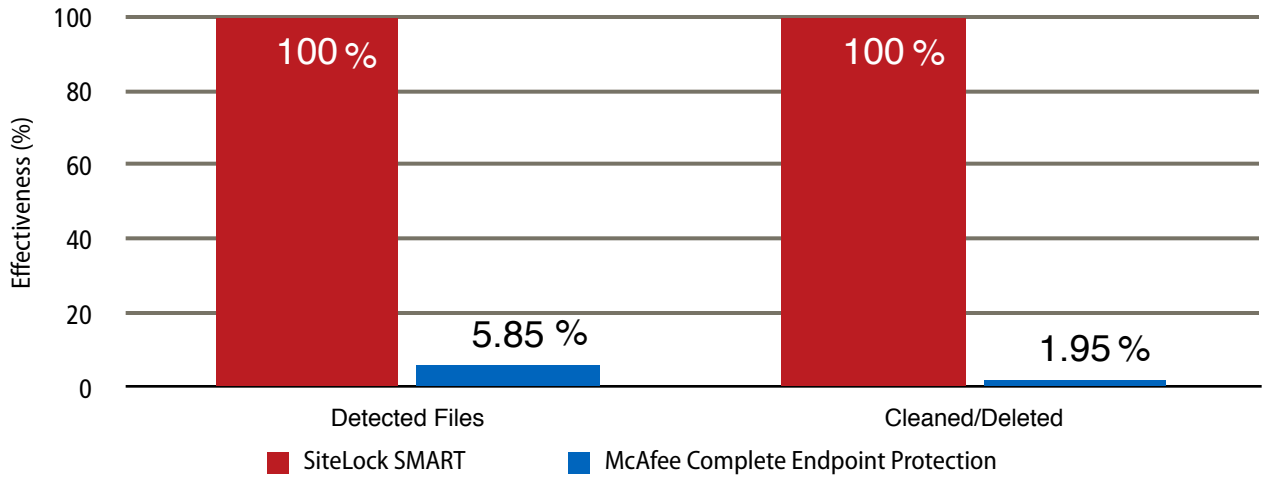
Tests showed that the SiteLock solution detected and cleaned 100% of the samples where the traditional endpoint solution detected under 6% of the samples and deleted less than 2% of the samples. See Figure 1.

THE BOTTOM LINE

SiteLock SMART provides:

1. Essential coverage of web-based malware not detected by traditional endpoint security
2. 100% PHP and JavaScript coverage vs less than 6% coverage by the traditional solution
3. Automated, always-on coverage via FTP/SFTP
4. Real-time, non-disruptive, continuous scanning

SiteLock SMART vs McAfee Endpoint Protection Suite
Web Malware Effectiveness (2,972 Samples)



Notes: Corpus primarily composed of PHP malware. See Test Methodology for additional details.

Source: Tolly, August 2016

Figure 1

Test Results

Threat Landscape

Traditionally, anti-virus solutions have focused on detecting and quarantining threats that arrived either as executable programs, scripts or even macros that run inside common document types such as Microsoft Word documents.

In more recent times, though, hackers have successfully infiltrated web applications such as WordPress and installed malware that can compromise these systems and cause significant damage. Unfortunately, traditional "virus scanning" applications are not designed to detect and counter such threats - thus leaving users' websites exposed to malware.

To complicate the situation further, some of these malware threats may be modifications to otherwise good - and required - web components. Thus, the remediation of the threat is to "clean" the module (leaving the required code while removing only the malicious pieces) rather than deleting or quarantining the module as is typically the action performed by traditional systems.

To illustrate this situation, Tolly tested a corpus of nearly 3,000 web-based malware examples to determine how many of these threats could be detected.

Tolly engineers tested the cloud-based SiteLock SMART solution and the McAfee Enterprise solution. The McAfee solution consisted of multiple components including: McAfee Agent, Host Intrusion Prevention System, Virus Scan Enterprise, McAfee Application Control, McAfee Change Control and McAfee Data Reputation. Engineers installed all endpoint security components though not all of the component were necessarily invoked as part of the test process.

Web Malware Effectiveness

Tests showed that the traditional antivirus system was only able to even detect a very small percentage of the web-based malware. McAfee detected only 174 out of 2,972 samples. This was a 5.85% effectiveness rating and only 58 or 1.95% were cleaned. See Figure 1. SiteLock, which built this corpus based on what it has found "in the wild," had a 100% detection/cleaned rate. According to SiteLock, the company scans source code of over 200,000 websites and web applications and cleans over 50,000 applications per month.

Advantages of SiteLock SMART

- Cloud-based solution ensures no disruption to web applications
- Identifies and cleans new forms of web-based malware that traditional solutions miss
- Cleans malware on a daily or real-time basis, per-customer preference
- Flexible configuration options give you control over the scan speed and frequency
- Customize which applications and directories of your websites will be monitored and cleaned
- Operates through the firewall
- Customize how and where the scan takes place
- Differential reporting enables quick identification of new issues
- Compatible with any architecture from internal hosting to cloud-based models
- Alerts in real time of any suspicious or malicious files detected within web applications

Source: SiteLock

Test Setup & Methodology

Tolly engineers tested current versions of each solution. SiteLock is a hosted solution. The McAfee endpoint solution components were installed in a virtualized Windows Server environment. See Table 1 for details.

Test engineers placed the malware corpus in a separate directory and had each solution scan the corpus. McAfee scanned the corpus in place on the server. SiteLock used FTP (SFTP and RSYNC over SSH options are also available) to copy the corpus to its cloud-based servers. Afterward, SiteLock placed the cleaned files back in the local test directory.

The test corpus was provided by SiteLock and consisted of 2,972 samples that included PHP, JavaScript and other executables that contained a variety of attacks.

SiteLock, LLC

SiteLock SMART

Web Malware Effectiveness

Tested August 2016

Solutions Under Test

SiteLock SMART	Cloud-based current as of July/August 2016
McAfee Endpoint Security Protection Suite Enterprise	McAfee Agent 4.8.0.1500 - default configuration
	Host IPS 8.0.0.3624 (McAfee Host Intrusion Prevention for Server) - enabled Host IPS, enabled Adaptive mode, enabled Network IPS
	VirusScan Enterprise 8.8.0.1528 (McAfee VirusScan Enterprise), DAT Version 8259.0000 - default configuration
	Solid core 7.0.0.646 (McAfee Application Control, McAfee Change Control) - default configuration
	Data Reputation MCDATREP1000 1.0.4.385

Source: Tolly, August 2016

Table 1

About Tolly

The Tolly Group companies have been delivering world-class IT services for more than 25 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 by E-mail at sales@tolly.com, or by telephone at +1 561.391.5610.

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

Interaction with Competitors

In accordance with Tolly's Fair Testing Charter, Tolly personnel invited representatives from McAfee/Intel to participate in the testing. Because of internal guidelines, McAfee/Intel was unable to review the test corpus in detail and had no further comment.

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.

216143 Tjeo-1 wt-2016-09-19-VerE