TEST REPORT

Tolly.

#223114

April 2023

Commissioned by BlackBerry Ltd.

BlackBerry CylanceENDPOINT

Resource Efficiency and Efficacy vs. Microsoft, Sophos, and Trellix

EXECUTIVE SUMMARY

Endpoint security is essential, but there can be a hidden price to pay when it comes to how some solutions use system resources. While computing systems, physical and virtual, continually become more powerful, new and updated applications are ever more hungry for those resources. BlackBerry's focus is on providing superior endpoint protection - even in offline environments - while consuming minimal system resources.

BlackBerry commissioned Tolly to compare the efficacy and resource demands of its CylanceENDPOINT endpoint solution in a Windows 10 environment and compare that to several competing solutions.

BlackBerry excelled in offline protection with exceptionally low performance impacts which is particularly crucial for hybrid workforce fleets that connect/disconnect from access points as well as isolated operational technology environments that may not be directly connected to the internet. See Figure 1.

THE BOTTOM LINE

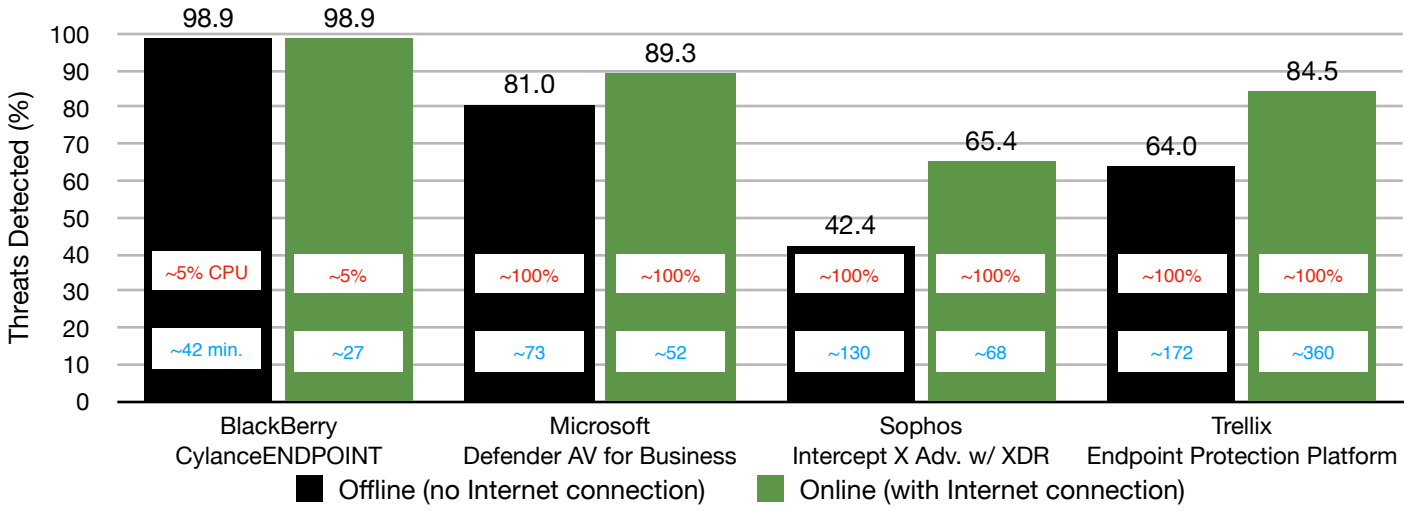
BlackBerry CylanceENDPOINT:

1. Offered dramatically lower CPU resource consumption while scanning, enabling computer resources to be available for end-user, business tasks
2. Delivered superior threat protection both offline and online to ensure safety from malicious files, regardless of Internet connectivity status
3. Will help extend the lifecycle of endpoints it protects by minimizing continued resource utilizations and eliminating expensive device reimaging cycles caused by malware breaches

Windows 10 Endpoint Protection Efficacy & Resource Utilization

Scanning Two Collections of 1,000 Recent VirusTotal Samples

(Detection % determined by number of files remaining in folder after scan)



Note: Scan is triggered by system decompressing a password-protected "zip" file containing 1,000 malware samples. Different collections of samples used for offline and online tests. Same sample set used for each solution. Approx. run time in minutes indicated in blue text, typical CPU utilization reported by the endpoint protection process during run in percentage indicated in red text. Recent samples from VirusTotal. Query to pull samples found in Test Setup & Methodology section.

Source: Tolly, March 2023

Figure 1

Test Results

Background

Endpoint protection solutions, by their very nature, are always present and, thus, always consuming at least some system resources. If an endpoint security solution consumes excessive resources, such as CPU, then response time for the end user and business applications may suffer.

The nature of this test is very focused and, thus, the results can be presented quite succinctly. To highlight the differences in resource consumption (and efficacy) across several popular endpoint security solutions, Tolly evaluated both the threat protection detection effectiveness and the resource consumption when scanning folders containing 1,000 recent malware samples downloaded from Google-owned VirusTotal website. All test results are summarized in Figure 1 on the previous page. In all tests, BlackBerry was tested first as testing newer samples is the more challenging test. BlackBerry tested with EDR disabled. Details of solutions tested are found in Table 1 near the end of the report.

Efficacy - Offline Test

For the offline test, the Internet connections of all the endpoint were disabled. This was done to force the endpoints to rely only on local information when examining the malware.

BlackBerry CylanceENDPOINT detected 98.9% of the malware samples. Microsoft Defender for Business detected 81% of the samples. Sophos Intercept X Advanced with XDR detected 42.4% of the samples. Trellix Endpoint Protection detected 64% of the samples.

BlackBerry Ltd.

CylanceENDPOINT

Resource Efficiency & Efficacy

Tolly. Certified

Tested March 2023

Efficacy - Online Test

For the online test, the Internet connections of all the endpoint were re-enabled. This allows the solution under test to query their centralized databases when examining the malware. A different set of samples was used for this test.

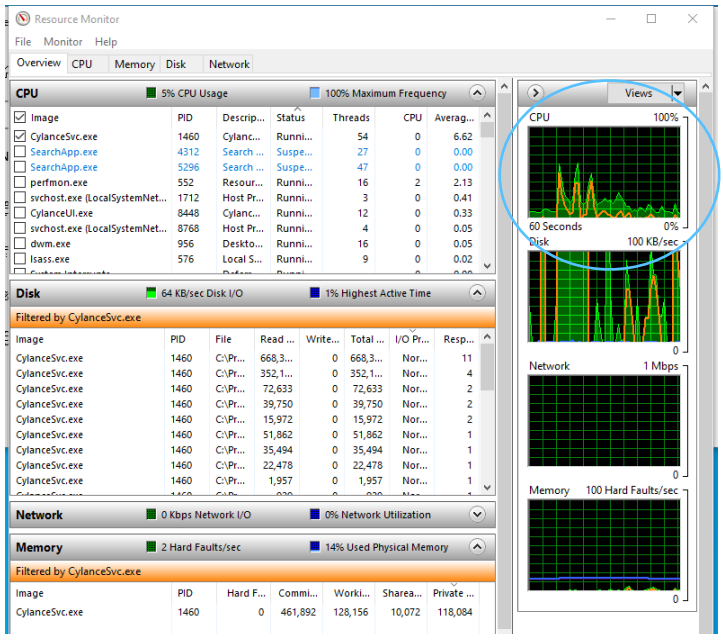
As with the offline test, BlackBerry CylanceENDPOINT detected 98.9% of the malware samples. Microsoft Defender for Business improved and detected 89.3% of the samples. Sophos Intercept X Advanced with XDR results improved by some 50% by detecting 65.4% of the samples. Trellix Endpoint Protection detected 84.5% of the samples.

Resource Utilization

As noted, a particular focus of this test was how the endpoint solutions managed precious Windows resources.

Given that endpoint solutions typically are at work in the background and the arrival of malware is unpredictable, it can be very challenging to pinpoint resource usage.

BlackBerry CylanceENDPOINT
Windows 10 Resource Utilization During Scan
(as reported by Microsoft Resource Monitor)

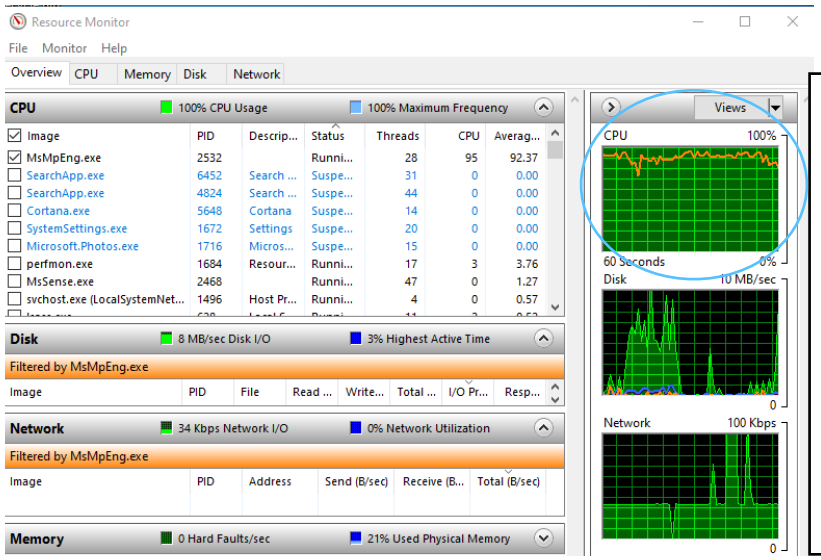


Resource snapshot in the middle of the scan. BlackBerry CPU usage averaging ~6%. Resource usage remained consistent throughout the test.

Source: Tolly, March 2023

Figure 2

Microsoft Defender for Business
Windows 10 Resource Utilization During Scan
(as reported by Microsoft Resource Monitor)



Resource snapshot in the middle of the scan. Microsoft CPU usage averaging 95 to 100% from beginning to end of scan.

Source: Tolly, March 2023

Figure 3

Ultimately, this has the potential of degrading the performance of end users performing their business tasks.

Microsoft

With Microsoft, its core security process, MsMpEng.exe, grabs the CPU resource immediately upon the beginning of "extracting" the malware from the ZIP. That process consumes ~95 to 100% of the CPU until all malware samples are examined. See Figure 3. Scanning required roughly 73 minutes in the offline test and 52 minutes in the online test.

Sophos

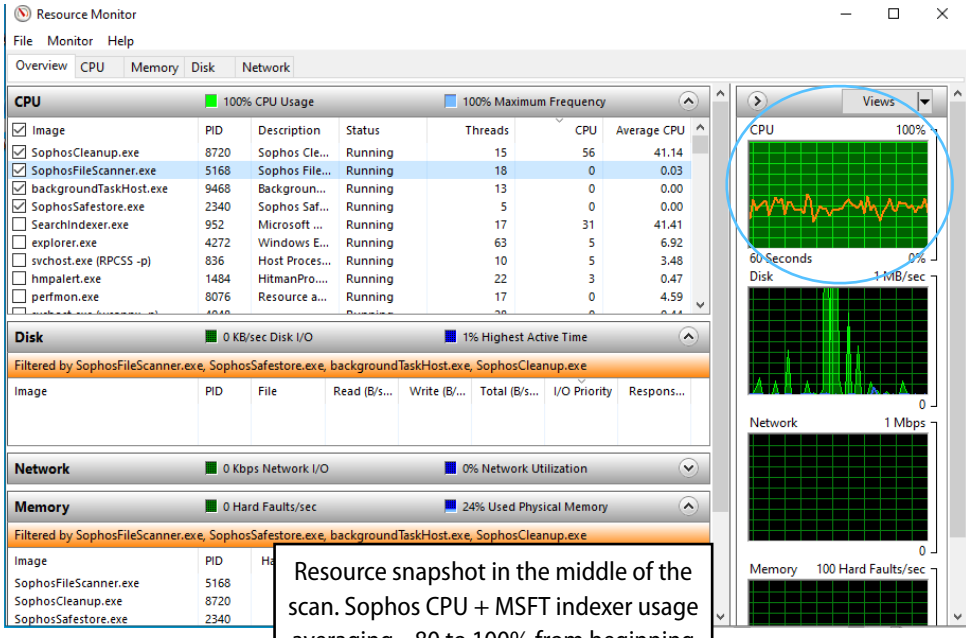
The Sophos solution, too, consumes ~90 to 100% of the CPU commencing with the extraction of the files from the ZIP file. Sophos differs primarily in that different processes are called during the scanning

For that reason, the test used folders containing 1,000 samples to drive the test.

The results were somewhat startling and there was a stark difference in resource utilization from BlackBerry to the other vendors. BlackBerry throttled its use of CPU resource to approximately 6% throughout the test and, even with that self-imposed constraint, completed the tests faster than the competition. See Figure 2.

The other vendors CPU usage immediately hit 100% as soon as the test started and remained at or near that level for the entire duration of the test which, at least for one vendor in one scenario, was over two hours. While the scenario tested is not being put forth as a common scenario, it does illustrate that the other solutions tested do not throttle their usage of CPU resource but take all that they can get for the duration of whatever task they are performing.

Sophos Intercept X Advanced with XDR
Windows 10 Resource Utilization During Scan
(as reported by Microsoft Resource Monitor)



Resource snapshot in the middle of the scan. Sophos CPU + MSFT indexer usage averaging ~80 to 100% from beginning to end of the scan.

Source: Tolly, March 2023

Figure 4

including SophosCleanup.exe, SophosFileScanner.exe, and SophosSafestore.exe. In addition, the Microsoft SearchIndexer.exe module is running nearly constantly during the Sophos scanning process. Tolly engineers can only assume that this process is called by and used by the Sophos endpoint solution as it was not present in this manner in any of the other solutions tested. See Figure 4. Scanning required roughly 130 minutes in the offline test and 68 minutes in the online test.

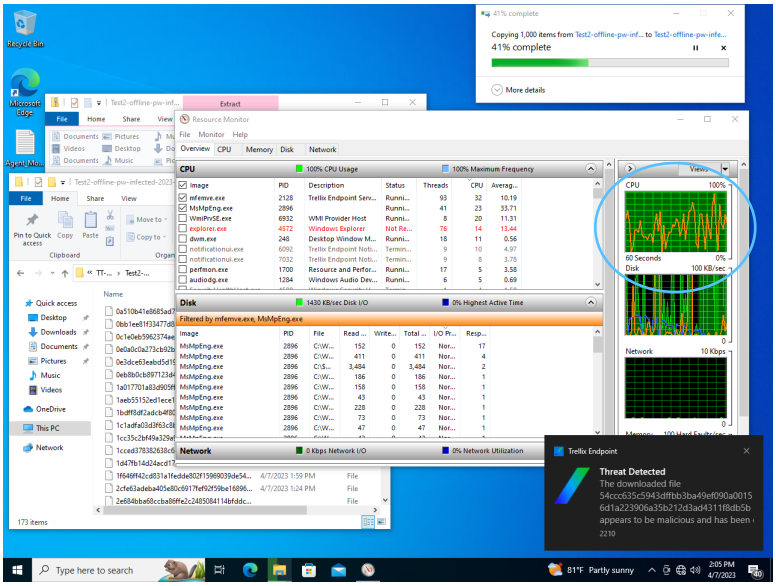
Trellix

The Trellix solution, too, consumes ~90 to 100% of the CPU commencing with the extraction of the files from the ZIP file. Trellix differs primarily in that different processes are called during the scanning. Mfemve.exe is the Trellix Endpoint Service core process[1]. and appears to work in conjunction with Microsoft Defender's core process, MsMpEng.exe built in to Windows 10 (and a subset of the Microsoft Windows Defender for Business that is part of this test).

It would seem that Trellix does its work through other Microsoft system processes that, put together, consume ~100% of the CPU throughout the extract and scanning process. In fact, for some threats that apparently are not caught by Trellix, Microsoft Defender caught the threat and displayed its message. As it isn't possible to tell which threats are detected by which components, the Trellix results are a composite of both.

Where other solutions complete the extract and then continue scanning, Trellix appears to scan every file while extracting. The specific process taking the most CPU varies considerably throughout but always address up to ~100%. See Figure 5. Scanning required roughly 172 minutes in the offline test and 360 minutes in the online test. In both tests, the Microsoft Defender process continued to run at 100% continually after the test completed.

Trellix Endpoint Protection
Windows 10 Resource Utilization During Scan
(as reported by Microsoft Resource Monitor)



Resource snapshot in the middle of the scan. Trellix CPU usage averaging ~100%.

Source: Tolly, March 2023

Figure 5

Test Setup & Methodology

Environment

All testing was run using Windows 10 2022H2 64-bit systems running in a virtualized environment under Oracle VirtualBox 6.1. All Windows system were updated with all available updates as of late March 2023. After the updates were applied the automatic update function was paused to avoid any changes to the systems while testing.

[1] The process name is a reference to "McAfee," the company's former name. Some components are copyright Musaruba, another former name, and the CASB element of the MVISION solution is branded as "SkyHigh Networks." The branding is both inconsistent and confusing.

The VirtualBox host system processor was a 3.7GHz Intel Core i7 with 96GB of DDR4 RAM.

Each virtual desktop was configured with one CPU and 16GB RAM[2]. Internet connectivity was provided by a virtualized Gigabit Ethernet network adapter. Solutions were tested serially with only a single virtual desktop booted at any one time.

Solution Installation

Each solution tested provided a cloud-managed administration environment. For each solution, the Windows installer was downloaded to onboard the endpoint.

For Sophos and BlackBerry, only the endpoint protection option was enabled. Other functions, such as encryption, were not installed.

No special configuration was done for the endpoints. As cloud services continually update threat protection databases, client version numbers are not relevant.

Network Test Environments

Tests were run twice (with different samples sets) with the Windows system in different states of network connectivity.

Offline

For these tests, the Ethernet network adapter providing connectivity to the Internet was disabled. Thus, each endpoint protection solution could only reference its local resources when reaching a verdict on a malware sample.

Although systems were tested serially, all systems were taken offline at the same time and then shut down until it was time to be tested.

Online

For these tests, the Ethernet network adapter was enabled. The endpoint protection solution was thus able to query its centralized threat database when reaching a verdict on a threat.

Malware Samples

All malware samples were downloaded from the VirusTotal collection less than 24 hours prior to testing.

The sample set consisted of 1,000 files submitted to VirusTotal as malware with a single not to exceed 5MB. A compressed (ZIP), password-protected file of approximately 275MB was produced for each test. The file was password protected so that engineers could trigger the start of the scan manually.

The following query was used to provide samples. fs:1d+ size:5MB- type:peexe positives:15+ not engines:pup not engines:adware not tag:corrupt not tag:assembly not tag:overlay not tag:nsis not tag:upx not tag:64bits not tag:bobsoft not tag:armadillo not magic:"PE32 executable for MS Windows (unknown subsystem) unknown processor 32-bit".

Test Process

Malware samples were copied to the endpoint solution under test. The network connection was enabled/disabled as required by the scenario. Engineers opened the Microsoft Resource Monitor window on the Windows system under test.

Start time was recorded as the time that the password was typed in and the "extract all" command began to process. End time was recorded as the time when the endpoint processes ceased removing files from the test malware folder.

As the target folders contained 1,000 samples of malware (as determined by VirusTotal) a perfect score would leave zero files remaining in the target folder. The number of files remaining in the target folder was used to calculate the threat detection percentage.

Except for Trellix, all production efficacy testing was run on the same days, March 26 & 27th, 2023. Because of logistics issues, Trellix was not deployable at that time. The Trellix testing was conducted on April 7 & 8th, 2023. Because the majority of testing was conducted in late March 2023, that date remains on the results references.

Endpoint Protection Solutions Under Test

Vendor	Solution
BlackBerry Ltd.	CylanceENDPOINT (EDR disabled)
Microsoft	Defender for Business
Sophos	Intercept X Advanced with XDR
Trellix	Endpoint Protection (MVision)

Source: Tolly, March 2023 Table1

[2] During endpoint installation the Sophos installer issued a warning recommending more than one core (CPU). As noted, only one CPU was used for testing.

About Tolly

The Tolly Group companies have been delivering world-class IT services for more than 30 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 info@tolly.com, or by telephone at
+1 561.391.5610.

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

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.

cm-1-wt-2023-05-04—VerK