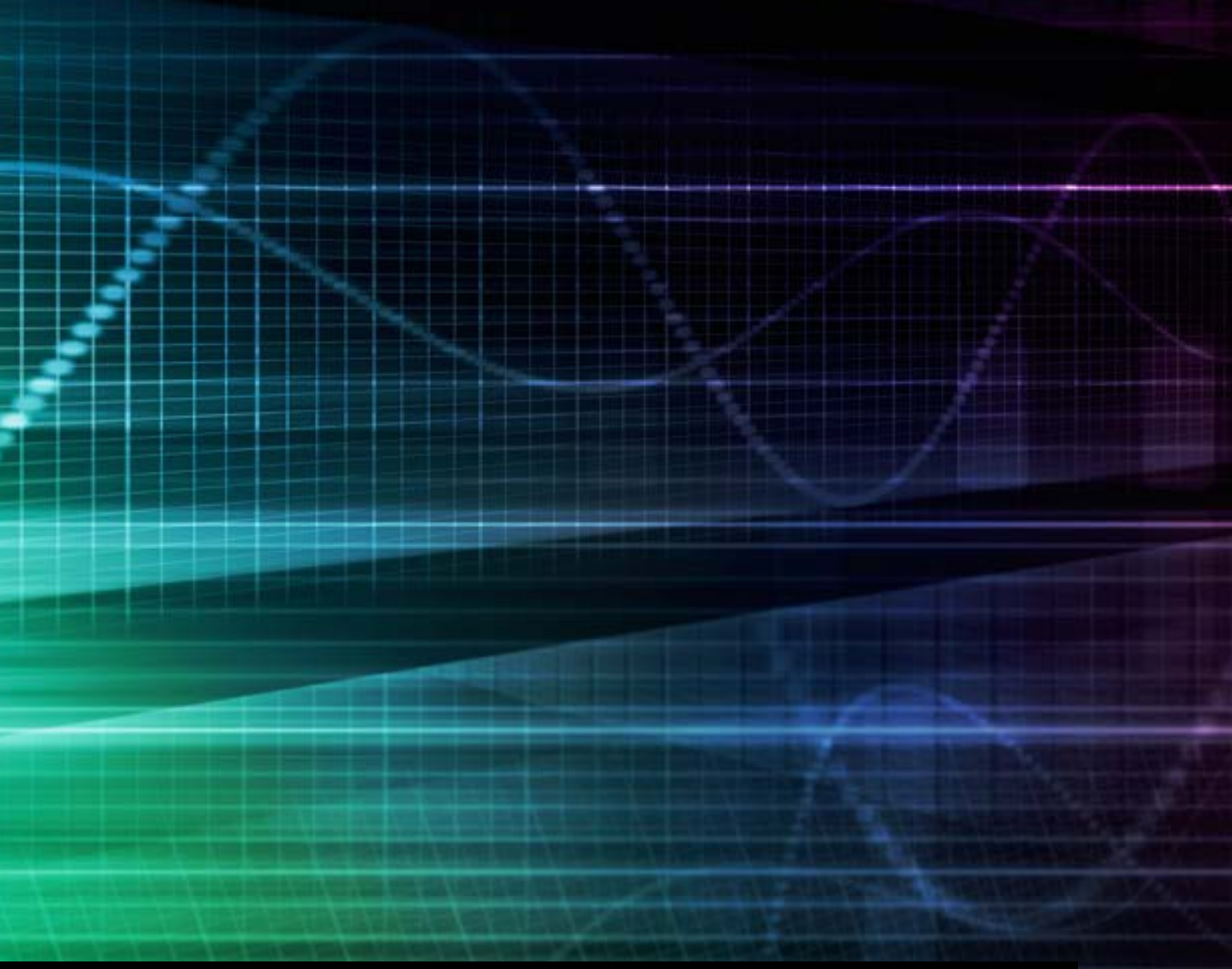


Resource Impact Testing

CylancePROTECT® Goes Head-to-Head with Signature-Based Antivirus Solutions

CYLANCE

Security administrators struggle to balance the mandate of providing adequate security against malware threats with the needs of end-users to work in an unfettered manner. One of the side effects is the administrative overhead burden on the central processing unit on the endpoint. Should these administrative tasks monopolize the processing power, administrators risk having end-users simply deactivate the protection in order to carry on with their work routine. Further, simple, elegant solutions are preferred to preserve the integrity of the data. "Complexity is the enemy of security" notes professor Alan Woodward from the UK's University of Surrey in a recent blog post on the challenges of signature-based antivirus. But even if the protection is not deactivated, the average toll on worker productivity can exceed **$1000 per employee per year.**

This paper is oriented toward security administrators whose daily tasks include endpoint security administration and their leadership who balance organizational objectives and budgetary constraints.

Forward-thinking security administrators target minimal intrusiveness on work activity by security measures, and nominally, that can vary from 5-10% of CPU utilization. Above that, productivity suffers, and help desk calls, end-user deactivation, and general dissatisfaction often ensue.

Cylance® conducted several tests to determine the impact on a computer system and the user's ability to perform several common actions, such as copying or creating files, and their impact while detecting and quarantining malware.

Methodology:

Systems:

There were three types of systems utilized during this testing to simulate a range of performance and capabilities. A 'low-end' laptop with an older, slower processor and a spinning hard drive, a 'mid-range' laptop with relatively modern i7 quad-core CPU and SSD, and a 'higher-end' desktop with a current i7 quad-core CPU and high-speed M.2 NVMe SSD storage.

Systems used:

'**Low-end**' **—** Laptop:

- Toshiba Satellite C55
- Intel Celeron N2820 @ 2.13GHz (2 cores)
- 8GB RAM
- Toshiba MQ01ABF050 500GB 5400RPM
- Windows 10 Enterprise

'**Medium-end**' **—** Laptop:

- Dell Latitude E7450
- Intel Core i7-5600U 2.60GHz (4 cores)
- 16GB RAM
- Samsung PM851 M.2 PCIe 256GB SSD
- Windows 7 SP1

'**Higher-end**' **—** Desktop:

- Intel "Skull Canyon" NUC6i7KYK
- Intel Core i7-6770HQ 2.60GHz (4 cores w/hyperthreading – 8 logical cores)
- 32GB RAM
- Samsung 960 PRO M.2 PCIe NVMe 1TB SSD
- Windows 10 Enterprise

All systems were put in 'High-Performance' power settings and all sleep/idle functions were set to 'Never'.

Software Tested:

In this test, three software packages were tested: two market share leaders, which we will call Brand X and Brand Y, and CylancePROTECT.

The testing methodology sought to provide equivalent protection levels across the three tested products. An astute reader might conclude that management and administrative costs would likely increase as layered protection proliferates.

Software Policies:

All of the tests were run three times on each system and the results of the three runs were averaged to determine a test average on that specific system.

CylancePROTECT policy was configured as:

File Actions — Auto-quarantine – no exclusions

Memory Protection — Enabled and all settings set to Terminate – no exclusions

Protection Settings — Enabled prevent shutdown, enabled kill unsafe running processes, disabled background threat detection, enabled watch for new files – no exclusions

Application Control — OFF

Agent Settings — Enabled desktop notifications

Script Control — OFF

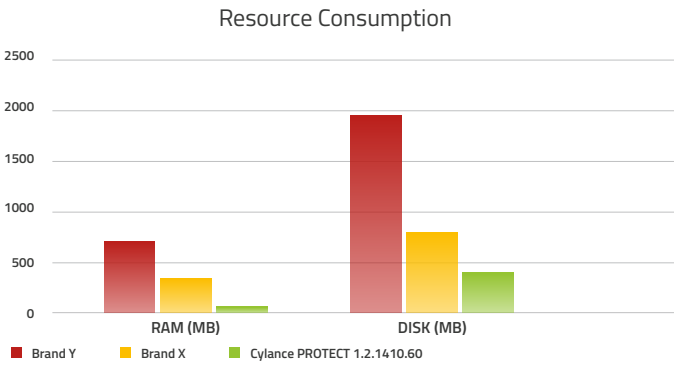
Device Control — Enabled all devices full access – no exclusions

Test Scenarios:

There were several testing scenarios designed to measure system and user impact.

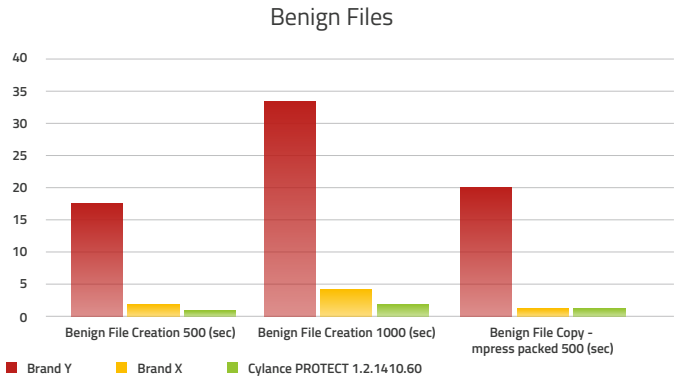
Resource Consumption Test:

1. Designed to determine what system resources were being utilized by the installed product after installation but sitting idle.
   - RAM usage is determined by adding the 'in-use' RAM utilized by new processes/services added to the system during the install.
   - Disk usage is determined by measuring the primary hard drive 'Used Space' in bytes – from drive properties; before the installation then after the installation and all updates have been applied.



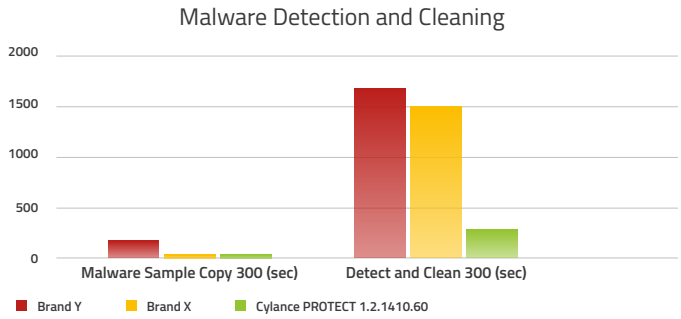
Benign Files:

1. Benign File Creation – 500
   - This test is designed to judge any system impact by the security software on creating new files on the disk. A simple FOR loop that copies the Windows Media Player setup file (setup_wm.exe) 500 times renaming the copied file to setup_wm###.exe. A simple timing batch script was used to time the creation of these files.
2. Benign File Creation – 1,000
   - This test is designed to judge any system impact by the security software on creating new files on the disk. A simple FOR loop that copies the Windows Media Player setup file (setup_wm.exe) 1,000 times renaming the copied file to setup_wm###.exe. A simple timing batch script was used to time the creation of these files.
3. Benign File Copy – MPRESS packed 500
   - This test is designed to judge any system impact by the security software when copying 500 files from an external USB 3 hard drive. This test utilized 500 copies of the Windows Media Player setup file (setup_wm.exe) that were all packed with a common packer – MPRESS.

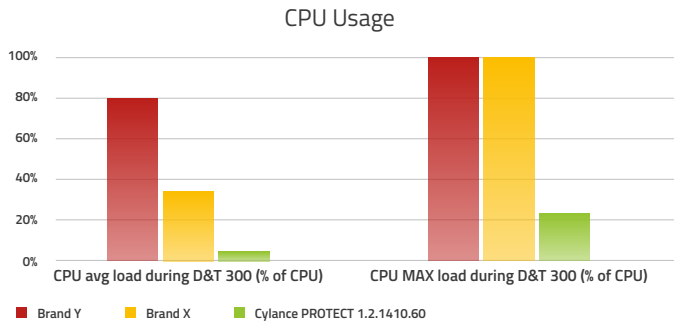


Malware Detection and Cleaning:

1. Malware Samples Copy 300
   - This test is designed to judge any system impact by the security software when copying 300 samples of malware from a network share. This test utilized 300 samples of malware consisting of 100 random ransomware samples, 100 random malware samples greater than 3MB in size, and 100 ransomware samples that have been packed.
2. Detect and Clean 300
   - This test is designed to judge system impact during the detection and cleaning of the 300 samples copied to the system from the previous test. Time to detect and clean was determined by starting the PERFMON data monitor at the start of the file copy process and was stopped when the security software had stopped scanning the files and CPU load returned to ~0%.



3. CPU Impact
   - CPU average and max load were determined by creating a PERFMON data set to gather CPU load (in percentage) while the installed security software detected and cleaned the 300 samples of malware.



Conclusions:

1. Brand Y and Brand X have entirely different approaches to scanning and detecting malware.

Brand Y uses a driver to inject itself into all read/write functions whether on a local disk, removable storage, or network drive. Brand Y calls this feature 'on-access protection' and is enabled by default. Many AV vendors commonly use this method and it is a major driver in users complaining that the AV is making their box 'crawl to a halt'. When performing common tasks, such as unzipping large archives, or copying many files, this type of system severely impacts performance. As you can see from the results, in most cases Brand Y's scanning during these file creation and copy events, on average, took 16 times longer than on a CylancePROTECT system.

Brand X however, uses a method called 'Deferred Scanning'. This is similar to what CylancePROTECT does with the File Watcher feature — keeps tracks of files written to disk and then queues them up for scanning at a later time. This results in little immediate user interruption as you can see from the results where Brand X and CylancePROTECT were pretty much equal in the file creation/copy tests.

2. Brand X and Brand Y use significantly more system resources (at idle) than CylancePROTECT.

Both Brand X and Brand Y use significantly more resources on a host than does CylancePROTECT. CylancePROTECT sits idle at about 55MB of RAM and about 380MB of hard disk space consumed with two running processes.

Sitting idle, Brand Y consumes nearly 13 times the RAM used and over 5 times the disk space (nearly 2GB) consumed by the installed applications and updates. Brand Y also has 13 processes running.

Brand X's latest version has a much lower RAM and process usage than previous versions. However, even while sitting idle, Brand X still uses five times the memory and double the disk space of CylancePROTECT.

3. The biggest performance differences are in detection and cleaning.

We saw the biggest differences in the impact on the end-user system when copying 300 malware samples to the hosts.

As Brand Y injected itself in the copy process, it began detecting malware as soon as the file copy started. While it was the fastest at detecting and cleaning some of the 300 samples, taking only 203 seconds, the CPUs were essentially totally consumed during this process. The average CPU load during the 300-file copy was over 79% and maxed out at 100%. It should also be noted that Brand Y only had to perform cleaning on 2/3 of the files – as they missed detecting 99 of the 300 samples. Compared to CylancePROTECT, Brand Y was 20% quicker in detecting and cleaning 67% of the samples, however Brand Y's average CPU utilization during this time was nearly 20 times that of CylancePROTECT doing the same task.

Brand X's results were significantly different than Brand Y's. As Brand X does not inject itself into the file copy, the actual copying of the files happens very quickly. However, once their 'deferred scanning' begins, their CPU consumption dramatically increases to an average of 33.6% of the CPU (maxing out at 100%) and it took them nearly 1,500 seconds to detect and clean 94.3% of the 300 samples. Compared to CylancePROTECT, Brand X used 8.4 times the CPU and took nearly six times longer to detect and clean the samples.

CylancePROTECT utilized (on average) only 4% of the CPU (maxed at 23.4%) and took 277 seconds to detect and quarantine 99.7% of the samples. There was one file remaining out of the 300. This file was a corrupt file — not a valid WIN32 application when it was executed.

Other Observations During the Test:

These are other observations seen during the test.

Brand Y:

- The update process upon initial install took over an hour to complete, even when downloading the updates from a locally connected management console software repository.
- Upon reboot, the on-access scanning process consumes significant CPU resources while loading data. On the low-end laptop, hard disk access was significant for many minutes after login.

Brand X:

- The update process downloaded 15 separate updates and took about 10 minutes to complete.
- Upon installation Brand X REQUIRED a reboot.
- The Brand X agent downloaded an update that REQUIRED a reboot to take affect several times during malware sample testing.

Conclusion

If you're using a bloated antivirus program, you're likely losing over **$1,000 a year per employee!**

The average worker works **5 days** a week, **50 weeks** a year.

5 days
× 50 weeks
250 days

Let's assume the average knowledge worker looses **10 minutes** a day.

10 minutes
× 250 days
2,500 mins. / 42.67 hours

The average American worker earns **$26.00** an hour.

$26.00
× 42.67 hours
$1,109 .42

Source: https://www.bls.gov/news.release/empsit.t19.htm

Even if one minute a day is lost to productivity drains because of PC horsepower allocation to security scans and remediation, the cost over a year across a medium sized enterprise adds up quickly. A 10,000 employee operation would face over $10M in direct productivity losses alone. As an early trigger for expensive PC hardware refresh is an onslaught of help desk calls, many companies find that they can actually extend the hardware refresh cycle out another 12-24 months simply by employing a security solution that does not tax the PC as heavily. The indirect costs associated with brand reputation, opportunity losses, etc. add untold thousands of dollars per year as well. Further, some institutions under 'green initiatives' monitor power consumption related to security measures favor solutions that use less energy. As such, forward-thinking enterprises are looking beyond the software license fees when evaluating security software alternatives.

The following table represent the raw results from the test:

Brand Y	Data	CylancePROTECT, 1.2.1410.60 — Data	Ratio X Times Cylance
RAM	689MB	**55MB**	**13**
DISK	1,932MB	**381MB**	**5**
Benign File Creation 500	17.49sec	**1.02sec**	**17.1**
Benign File Creation 1,000	33.82sec	**1.98sec**	**17.1**
Benign File Copy - mpress Packed 500	20.13sec	**1.28sec**	**15.7**
Malware Samples Copy 300	203sec	**28.3sec**	**7.2**
Detect and Clean 300	203.0sec	**277.0sec**	**0.8**
CPU Avg. Load During D&T 300	79%	**4.0%**	**19.9**
CPU MAX Load During D&T 300	100%	**23.4%**	**4.3**
Brand X	**Data**	**CylancePROTECT, 1.2.1410.60 — Data**	**Ratio X Times Cylance**
RAM	269MB	**55MB**	**5.0**
DISK	785MB	**381MB**	**2.0**
Benign File Creation 500	2.02sec	**1.02sec**	**2.0**
Benign File Creation 1,000	3.98sec	**1.98sec**	**2.0**
Benign File Copy - mpress Packed 500	1.76sec	**1.28sec**	**1.4**
Malware Samples Copy 300	29.2sec	**28.3sec**	**1.0**
Detect and Clean 300	1,496sec	**277.0sec**	**5.7**
CPU Avg. Load During D&T 300	33.6%	**4.0%**	**8.4**
CPU MAX Load During D&T 300	100.0%	**23.4%**	**4.3**

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612

CYLANCE

20170302-0407