

Anti-Virus Comparative



PC Matic PC Pitstop SuperShield 2.0

Language: English
September 2016

Last Revision: 29th November 2016

www.av-comparatives.org

Commissioned by PC Matic

Introduction

This report has been commissioned by PC Matic.

We found PC Matic PC Pitstop very easy to install. The wizard allows the user to change the location of the installation folder and the placing of shortcuts, but the average user only needs to click *Next* a few times. The program can be started as soon the setup wizard completes.

A Different Approach

PC Matic approaches security differently than traditional security products. PC Matic relies mainly on a white list to defeat malware; this can lead to a higher number of false alarms if users have files which are not yet on PC Matic's whitelist. Unknown files are uploaded to PC Matic servers, where they get compared against a black- and white list (signed and unsigned).

By default, PC Matic SuperShield only blocks threats and unknown files on-execution, but does not remove/quarantine them.

Additional features

In addition to malware protection, PC Matic also provides system maintenance and optimization features. These include checking for driver updates, outdated programs with vulnerabilities, erroneous registry entries and disk fragmentation. A single scan can be run which checks not only for malware, but also for any available system optimization opportunities.

The screenshot displays the PC Matic software interface. At the top left is the PC Matic logo with a green tree icon. The main header shows 'MY PCS 2 out of 5 PCs Licensed' and 'Master Scheduler' and 'Master Reports' buttons. Below this, the 'This Computer' section shows 'Windows 10', 'Last Test 9/13/2016', and 'Next Test None Scheduled'. There are buttons for 'Details', 'Super Shield', 'Options', and 'Scan'. A section below shows two computer icons, one with a green shield and one with a green plus sign. The 'Maintenance statistics: 2 PCs' section is sorted by 'All Time' and includes the following data:

Category	Count
(0) Viruses Removed	0
(0) Patched Vulnerabilities	0
(4468) Analyzed (1321) Blocked	4468 / 1321
(30) Registry Corrections	30
(525) MB Cleaned	525
(0) Files Defragged	0
(0) Services Stopped	0
(0) Scheduled Tasks Disabled	0
(0) Startups Disabled	0
(0) Drivers Updated	0

Tested products

The tested products have been chosen by PC Matic. We used the latest available product versions and updates available at time of testing (August and September 2016).

- AVG Internet Security 2016
- Avira Antivirus Pro 15.0
- Bitdefender Internet Security 20.0
- ESET Smart Security 9.0
- iolo System Shield 5.0
- Kaspersky Internet Security 2017
- MalwareBytes Anti-Malware Premium 2.2
- McAfee Internet Security 18.0
- Panda Free Antivirus 16.1
- PC Matic PC Pitstop SuperShield 2.0
- Sophos Endpoint Security and Control 10.6
- ThreaTrack Vipre Internet Security Pro 9.3
- TotalDefense AntiVirus 9.0
- Trend Micro Internet Security 10.0
- Webroot SecureAnywhere 9.0

Test

The test has been performed under Windows 10 64-bit English in August and September 2016.

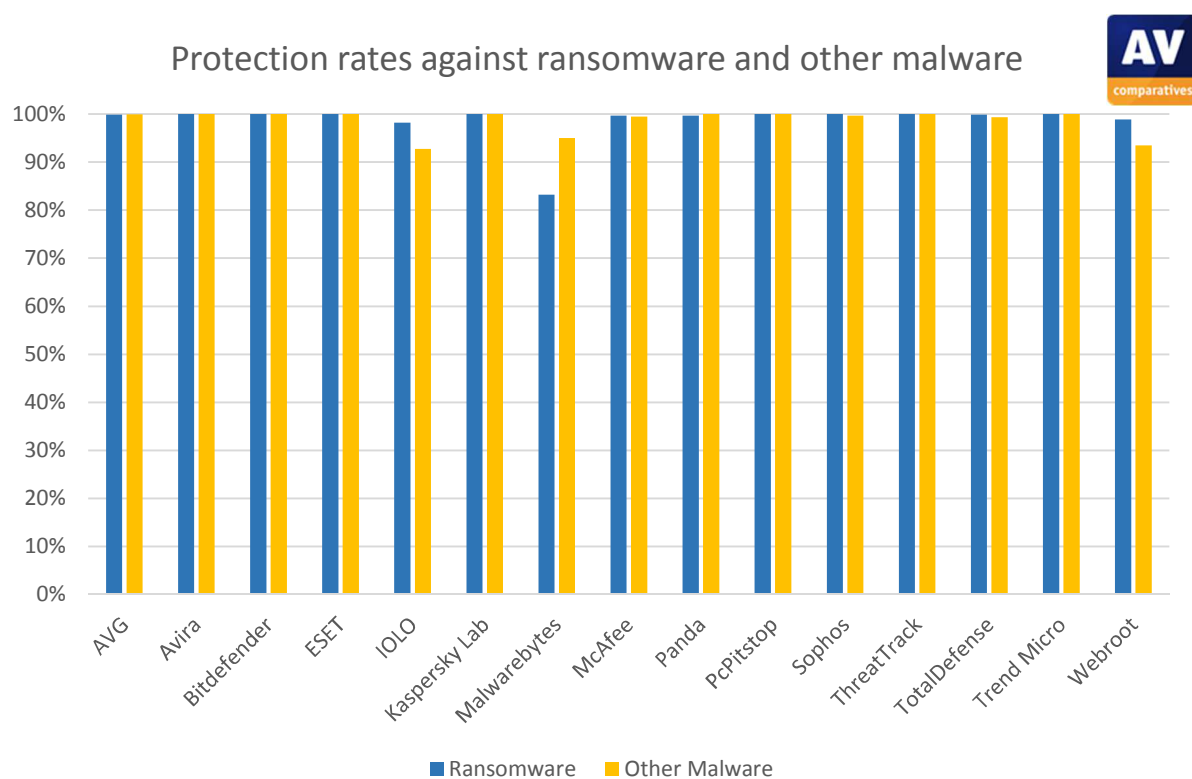
The test sets consisted of **1000** recent ransomware samples and **4000** other malware samples. None of the samples were submitted to VirusTotal at time of testing. All products were tested with cloud connection and the samples were **executed** using AV-Comparatives' Real-World-Testing Framework.

For the false alarm test, **500** clean files have been executed.

	# of samples in test-set
Ransomware	1000
Other malware	4000
Clean files	500

Results

The chart below shows the protection rates against the used ransomware and other malware samples.



	Ransomware (1000 samples)	Other Malware (4000 samples)
AVG	99,9%	99,9%
Avira	100%	100%
Bitdefender	100%	100%
ESET	100%	100%
IOLO	98,2%	92,7%
Kaspersky Lab	100%	100%
Malwarebytes	83,2%	95,0%
McAfee	99,7%	99,5%
Panda	99,7%	100%
PC Pitstop	100%	100%
Sophos	100%	99,7%
ThreatTrack	100%	100%
TotalDefense	99,9%	99,3%
Trend Micro	100%	100%
Webroot	98,9%	93,5%

False Alarm Test

During the false alarm test, in which **500** clean applications have been **executed**, only three products had false alarms. The table below shows the prevalence of the encountered FPs:

	Very low	Low	Medium	High	FP rate
AVG	-	-	-	-	none
Avira	-	-	-	-	none
Bitdefender	-	-	-	-	none
ESET	-	-	-	-	none
IOL0	-	-	-	-	none
Kaspersky Lab	-	-	-	-	none
MalwareBytes	-	-	-	-	none
McAfee	-	-	-	-	none
Panda	19	8	5	1	low
PC Pitstop	34	337	9	1	very high
Sophos	-	-	-	-	none
ThreatTrack	-	-	-	-	none
TotalDefense	-	-	-	-	none
Trend Micro	-	5	-	-	very low
Webroot	-	-	-	-	none

PC Pitstop had a very high FP rate in this test, but they are working on that problem and are happy that AV-C helps them to find further bugs and to improve their product.

Copyright and Disclaimer

This publication is Copyright © 2016 by AV-Comparatives ®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives, prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives (November 2016)