

Results of antivirus product self-protection testing (September 2007)

Table 1a. Brief results of the self-protection test and the awards received




Products tested	Awards	Total points (out of 33)	% of maximum points
Kaspersky Internet Security 7.0	 Gold Self-Protection Award	32	97%
VBA32 Antivirus 3.11	 Silver Self-Protection Award	23.5	71%
Symantec Internet Security 2007		23.5	71%
F-Secure Internet Security 2007		20	61%
ZoneAlarm Internet Security 7.0	 Bronze Self-Protection Award	19	58%
Panda Internet Security 2007		16	48%
McAfee Internet Security 2007		15.5	47%
Eset Smart Security 3.0		14.5	44%
Trend Micro PC-Cillin 2007		14	42%
Avast! Professional Edition 4.7		Failed the test	11
Avira Premium Security Suite 7.0	11		33%
Sophos Anti-Virus 6.5	11		33%
DrWeb 4.44 Beta	10.5		32%
Microsoft Windows Live OneCare 1.6	10.5		32%
BitDefender Internet Security 10	10		30%

Table 1b. The number of attacks blocked and missed; total points received

Products tested	The number of attacks blocked		The number of attacks not blocked; no self-protection (0 points awarded) ³	Total points received (out of 33)
	The number of attacks completely blocked (1 point awarded) ¹	The number of attacks partly blocked (0.5 points awarded) ²		
Kaspersky Internet Security 7.0	31	2	0	32
VBA32 Antivirus 3.11	23	1	9	23.5
Symantec Internet Security 2007	19	9	5	23.5
F-Secure Internet Security 2007	16	8	9	20
ZoneAlarm Internet Security 7.0	9	20	4	19
Panda Internet Security 2007	11	10	12	16
McAfee Internet Security 2007	6	19	8	15.5
Eset Smart Security 3.0	7	15	11	14.5
Trend Micro PC-Cillin 2007	7	14	12	14
Avast! Professional Edition 4.7	8	6	19	11
Avira Premium Security Suite 7.0	4	14	15	11
Sophos Anti-Virus 6.5	6	10	17	11
DrWeb 4.44 Beta	6	9	18	10.5
Microsoft Windows Live OneCare 1.6	3	15	15	10.5
BitDefender Internet Security 10	4	12	17	10


1) - The product's self-protection successfully blocked the attack.

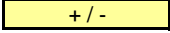
2) - Self-protection from these types of attacks is partly absent, but the main functionality was preserved (or automatically restored).


3) - The product does not have self-protection from these types of attacks; or, self-protection is present, but the main functionality was disabled by the attack.

Table 2a. Testing results (system level)

Products tested	Total points (out of 7)	Resulting mark
Kaspersky Internet Security 7.0	6	Good
Symantec Internet Security 2007	4	Satisfactory
ZoneAlarm Internet Security 7.0	3.5	
Trend Micro PC-Cillin 2007	2	Failed the test
Panda Internet Security 2007	1	
Avast! Professional Edition 4.7	0	
Avira Premium Security Suite 7.0	0	
BitDefender Internet Security 10	0	
DrWeb 4.44 Beta	0	
Eset Smart Security 3.0	0	
F-Secure Internet Security 2007	0	
McAfee Internet Security 2007	0	
Microsoft Windows Live OneCare 1.6	0	
Sophos Anti-Virus 6.5	0	
VBA32 Antivirus 3.11	0	

1 point
 Self-protection successfully blocked the attack.

0.5 points
 Self-protection from these types of attacks is partly absent, but the main functionality was preserved (or automatically restored).

0 points
 The product does not have self-protection from these types of attacks; or, self-protection is present, but the main functionality was disabled by the attack.









 Testing this type of attack was impossible.

Table 2b: Detailed testing results (system level)

Integrated Security Solution / Self-Protection Level	System			Files		Registry Keys			Summary (points)
	Restore Hooks*	File Permission Modification	Permission Modification of Registry Keys	Moduls Modification or Removing	Antivirus Database Removal	Modify or Remove Important Keys			
						Start-up Keys	Service Keys	Configuration Keys	
Avast! Professional Edition 4.7		-	-	-	-	-	-	-	0
Avira Premium Security Suite 7.0		-	-	-	-	-	-	-	0
BitDefender Internet Security 10	-	-	-	-	-	-	-	-	0
DrWeb 4.44 Beta		-	-	-	-	-	-	-	0
Eset Smart Security 3.0		-	-	-	-	-	-	-	0
F-Secure Internet Security 2007	-	-	-	-	-	-	-	-	0
Kaspersky Internet Security 7.0	-	+	+/-	+	+	+/-	+	+	6
McAfee Internet Security 2007		-	-	-	-	-	-	-	0
Microsoft Windows Live OneCare 1.6		-	-	-	-	-	-	-	0
Panda Internet Security 2007	-	+	-	-	-	-	-	-	1
Sophos Anti-Virus 6.5		-	-	-	-	-	-	-	0
Symantec Internet Security 2007	-	+	-	+	+	-	-	+	4
Trend Micro PC-Cillin 2007	-	-	-	+	+	-	-	-	2
VBA32 Antivirus 3.11	-	-	-	-	-	-	-	-	0
ZoneAlarm Internet Security 7.0	-	-	-	+/-	+	-	+	+	3.5

* Analysis of protection from hook restoration was outside the scope of this study and did not affect the final test score.

Table 3c. Detailed testing results (process termination), part 2

Integrated Security Solution / Self-Protection Level	Processes							Summary (points)
	Process Termination							
	User Level API		Send Message			Kernel Level API		
	"Bruteforce" message posting	Remove after System Reboot	WM_CLOSE	WM_QUIT	WM_SYS COMMAND	ZwTerminat e Process	ZwTerminate Thread	
Avast! Professional Edition 4.7	+	-	+	+	+	-	-	5.5
Avira Premium Security Suite 7.0	+/-	-	+	+/-	+	-	-	5
BitDefender Internet Security 10	+/-	-	+	+/-	+	-	-	5
DrWeb 4.44 Beta	+/-	-	+	+/-	+	-	-	5
Eset Smart Security 3.0	-	-	+/-	+	+	+/-	+/-	7.5
F-Secure Internet Security 2007	+	+	+	+	+	+	+	13
Kaspersky Internet Security 7.0	+	+	+	+	+	+	+	15
McAfee Internet Security 2007	+/-	-	+	+/-	+	+/-	+/-	8
Microsoft Windows Live OneCare 1.6	+/-	-	+/-	+/-	+/-	-	-	5.5
Panda Internet Security 2007	+/-	-	+	+	+	+	-	10
Sophos Anti-Virus 6.0	+/-	-	+	+/-	+	-	-	4.5
Symantec Internet Security 2007	+/-	+	+/-	+/-	+/-	-	+	11
Trend Micro PC-Cillin 2007	+/-	+	+/-	+/-	+/-	-	-	5.5
VBA32 Antivirus 3.11	-	-	+/-	+	+	+	+	12.5
ZoneAlarm Internet Security 7.0	+/-	+/-	+	+/-	+/-	-	+/-	7.5

Table 4a. Testing results (Process modification)

Products tested	Total points (out of 9)	Resulting mark
Kaspersky Internet Security 7.0	9	Excellent
VBA32 Antivirus 3.11	9	
Symantec Internet Security 2007	7.5	
McAfee Internet Security 2007	6	Good
ZoneAlarm Internet Security 7.0	6	
Eset Smart Security 3.0	5.5	
Avira Premium Security Suite 7.0	5	Satisfactory
F-Secure Internet Security 2007	5	
Trend Micro PC-Cillin 2007	5	Failed the test
Sophos Anti-Virus 6.5	4.5	
Avast! Professional Edition 4.7	3.5	
BitDefender Internet Security 10	3.5	
DrWeb 4.44 Beta	3.5	
Microsoft Windows Live OneCare 1.6	3.5	
Panda Internet Security 2007	3.5	

1 point
+

Self-protection successfully blocked the attack.

0.5 points
+ / -

Self-protection from these types of attacks is partly absent, but the main functionality was preserved (or automatically restored).

0 points
-

The product does not have self-protection from these types of attacks; or, self-protection is present, but the main functionality was disabled by the attack.

Table 4b. Detailed testing results (process modification)

Integrated Security Solution / Self-Protection Level	Processes									Summary (points)
	Process or Code Modification									
	Code Injection (Create Remote Thread)		DLL Injection			Modification of Memory Protection Attributes		Write in Process Memory		
	1	2	1	2	3	1	2	1	2	
Avast! Professional Edition 4.7	+ / -	-	+	+	-	-	+ / -	-	+ / -	3.5
Avira Premium Security Suite 7.0	+ / -	-	+	+	+ / -	+ / -	+ / -	+ / -	+ / -	5.0
BitDefender Internet Security 10	+ / -	+ / -	+ / -	+	-	-	+ / -	-	+ / -	3.5
DrWeb 4.44 Beta	+ / -	-	+	+	-	-	+ / -	-	+ / -	3.5
Eset Smart Security 3.0	+	+ / -	+	+	+ / -	+ / -	+ / -	-	+ / -	5.5
F-Secure Internet Security 2007	+ / -	-	+ / -	+	+	-	+ / -	+	+ / -	5.0
Kaspersky Internet Security 7.0	+	+	+	+	+	+	+	+	+	9.0
McAfee Internet Security 2007	+ / -	+ / -	+	+	+ / -	+ / -	+	+ / -	+ / -	6.0
Microsoft Windows Live OneCare 1.6	+ / -	-	+	+	-	-	+ / -	-	+ / -	3.5
Panda Internet Security 2007	+ / -	-	+	+	-	-	+ / -	-	+ / -	3.5
Sophos Anti-Virus 6.5	+ / -	-	+	+	-	+ / -	+ / -	+ / -	+ / -	4.5
Symantec Internet Security 2007	+	+	+	+	+	-	+ / -	+	+	7.5
Trend Micro PC-Cillin 2007	+ / -	-	+	+	-	+ / -	+ / -	+ / -	+	5.0
VBA32 Antivirus 3.11	+	+	+	+	+	+	+	+	+	9.0
ZoneAlarm Internet Security 7.0	+ / -	+ / -	+ / -	+	+	+ / -	+ / -	+ / -	+	6.0

Table 5a. Testing results (driver protection)

Products tested	Total points (out of 2)	Resulting mark
ZoneAlarm Internet Security	2	Excellent
VBA32 Antivirus 3.11	2	
Sophos Anti-Virus 6.5	2	
Kaspersky Internet Security 7.0	2	
F-Secure Internet Security 2007	2	
DrWeb 4.44 Beta	2	
Avast! Professional Edition 4.7	2	
Trend Micro PC-Cillin 2007	1.5	Good
Panda Internet Security 2007	1.5	
Microsoft Windows Live OneCare 1.6	1.5	
McAfee Internet Security 2007	1.5	
Eset Smart Security 3.0	1.5	
BitDefender Internet Security 10	1.5	
Symantec Internet Security 2007	1	Satisfactory
Avira Premium Security Suite 7.0	1	

1 point
+

Self-protection successfully blocked the attack.

0.5 points
+ / -

Self-protection from these types of attacks is partly absent, but the main functionality was preserved (or automatically restored).

0 points
-

The product does not have self-protection from these types of attacks; or, self-protection is present, but the main functionality was disabled by the attack.

Table 5b. Detailed testing results (driver protection)

Integrated Security Solution / Self-Protection Level	Processes		Summary (points)
	Driver Unloading		
	Halt Driver	Uninstall Driver	
Avast! Professional Edition 4.7	+	+	2.0
Avira Premium Security Suite 7.0	+ / -	+ / -	1.0
BitDefender Internet Security 10	+ / -	+	1.5
DrWeb 4.44 Beta	+	+	2.0
Eset Smart Security 3.0	+ / -	+	1.5
F-Secure Internet Security 2007	+	+	2.0
Kaspersky Internet Security 7.0	+	+	2.0
McAfee Internet Security 2007	+	+ / -	1.5
Microsoft Windows Live OneCare 1.6	+ / -	+	1.5
Panda Internet Security 2007	+ / -	+	1.5
Sophos Anti-Virus 6.5	+	+	2.0
Symantec Internet Security 2007	+ / -	+ / -	1.0
Trend Micro PC-Cillin 2007	+ / -	+	1.5
VBA32 Antivirus 3.11	+	+	2.0
ZoneAlarm Internet Security	+	+	2.0