COMPARATIVE REVIEW

WINDOWS SERVER 2003

John Hawes

This month's platform is *Windows Server 2003*, which is not the very latest server offering from *Microsoft* – indeed it has been succeeded by both *Server 2008*, which closely followed the release of *Windows Vista*, and the refreshed *Server 2008 R2* (essentially *Windows 7 Server* edition). Nevertheless, the 2003 version, closest in spirit as it is to the evergreen *Windows XP*, remains widely used and relied on for its relative maturity, stability and dependable performance. The single permanent *Windows* system maintained in the *VB* test lab continues to run the 2003 edition, after a brief experiment with 2008 R2 was quickly aborted.

Products available to protect the platform are, of course, not limited to dedicated server editions, and this month's comparative was open to all products expected to operate on the operating system. As usual, however, the server test was somewhat less oversubscribed than some of our recent desktop comparatives, with a much more modest, but still fairly broad field of entrants. Two of the largest providers are notable by their absence. With a large cluster of the notoriously tough W32/Virut strains included in our core WildList set this month, several of which were added into the most recent list issued just days before the deadline for our test sets (a week before the product deadline), several providers – especially those who have had issues with these families in the recent past – have chosen to give this difficult test a miss, judging discretion to be the better part of valour. However, many others bravely stood up to be counted, and are due a salute for their openness and consistency.

PLATFORM AND TEST SETS

The test set deadline was 20 August, with products frozen on 25 August. The July 2010 WildList, released on 18 August, was thus used to define our core certification set. As mentioned above, one of the most notable points of the list was the inclusion of several new strains of polymorphic viruses, including some Sality variants as well as a handful of Viruts. Several Viruts remained on the list from previous tests, and with a minimum of 1,000 replicated samples representing each variant, the total size of the WildList set reached over 14,000 samples – something of a record, at least in recent years.

The clean set underwent its usual expansion, with large swathes of new items added to challenge the products. This being a server test, the new items focused on business software, with many packages from the business tools sections of popular download sites, as well as items from major software houses including *IBM*, *Microsoft*, *Oracle* and others. After pruning out some older and less relevant items, the set came in at over 450,000 individual files, and over 100GB of data. The speed measurement sets remained unchanged from several previous tests, but we hope to refresh them in the near future.

Elsewhere, as has become our standard practice, the sets of trojans and worms & bots were compiled mainly from items first appearing on our radar in the last few months, prior to the compilation of the RAP sets. These latter were built in the three weeks leading up to the product deadline and for a week afterwards, filtered to try to reflect the most common items observed around the world. At the final measure the RAP weekly sets averaged 18,000 samples per week, with the trojans set pushing 80,000 and the worms & bots set containing around 20,000 samples.

The chosen version of the platform was *Microsoft*'s *Windows Server 2003, R2*, with Service Pack 2 – we used the Enterprise Edition as it was the most complete. Preparation of the test systems was simple and straightforward thanks to the mature and familiar platform, with only the addition of some drivers necessary to enable networking hardware in our fairly new machines. Everything was in place well in advance, which proved to be a boon when a large number of products were submitted at the last minute with instructions requiring Internet access to activate or update (in clear breach of our deadline arrangements for such requirements). We have tried to be as accommodating as possible to ensure the best possible coverage of products, but may have to be stricter in future.

With a reasonably large and diverse set of products and some interesting additions to our test sets, we expected an eventful month.

Agnitum Outpost Security Suite Pro 7.0.3 (3392.517.1242)

ItW	100.00%	**Polymorphic**	89.49%
ItW (o/a)	100.00%	**Trojans**	64.99%
Worms & bots	87.50%	**False positives**	0

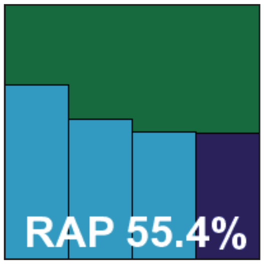
On-demand tests	WildList viruses		Worms & bots		Polymorphic viruses		Trojans		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
Agnitum Outpost Security Suite Pro	0	100.00%	2543	87.50%	191	89.49%	28220	64.99%		1
AhnLab V3Net	0	100.00%	4170	79.51%	11	99.60%	32339	59.88%	4	
ArcaBit ArcaVir	4	99.9997%	6336	68.87%	1854	83.14%	29407	63.51%		2
Avast Software avast!	0	100.00%	2010	90.12%	9	99.40%	4797	94.05%		
Avertive VirusTect	0	100.00%	2636	87.05%	191	89.49%	29017	64.00%		1
AVG Internet Security	0	100.00%	2342	88.49%	51	97.71%	2929	96.37%		
Avira AntiVir	0	100.00%	200	99.02%	0	100.00%	1482	98.16%		
BitDefender Security	0	100.00%	227	98.88%	0	100.00%	3689	95.42%		
Bkis BKAV	0	100.00%	1236	93.93%	1601	64.29%	7783	90.34%		
Bullguard Antivirus	0	100.00%	347	98.30%	0	100.00%	5023	93.77%		
CA Threat Manager	0	100.00%	5018	75.34%	3469	92.34%	44680	44.57%		
Central Command Vexira	0	100.00%	2485	87.79%	191	89.49%	27782	65.53%		1
Commtouch Command	0	100.00%	2855	85.97%	3	99.86%	28471	64.68%	1	
Comodo AntiVirus	7	99.03%	2847	86.01%	5128	60.96%	19805	75.43%		
Comodo Internet Security	7	99.03%	2838	86.06%	5154	60.93%	19710	75.55%		
Coranti 2010	0	100.00%	139	99.32%	0	100.00%	2130	97.36%	1	3
Defenx Security Suite Pro	0	100.00%	2609	87.18%	191	89.49%	28717	64.37%		1
Digital Defender AntiVirus	0	100.00%	4143	79.64%	191	89.49%	30370	62.32%		1
Emsisoft Anti-Malware	0	100.00%	415	97.96%	1315	79.84%	6657	91.74%	2	1

Please refer to text for full product names.

On-demand tests contd.	WildList viruses		Worms & bots		Polymorphic viruses		Trojans		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
eScan Internet Security	0	100.00%	297	98.54%	0	100.00%	4420	94.52%		
ESET NOD32	0	100.00%	302	98.52%	0	100.00%	4161	94.84%		2
Fortinet FortiClient	0	100.00%	844	95.85%	30	99.15%	11183	86.13%		
Frisk F-PROT	0	100.00%	2964	85.44%	0	100.00%	28869	64.18%	1	
F-Secure PSB Server Security	0	100.00%	519	97.45%	0	100.00%	5112	93.66%		
G DATA AntiVirus	0	100.00%	83	99.59%	0	100.00%	570	99.29%		
Hauri ViRobot	96	85.00%	6526	67.93%	2996	96.43%	38502	52.23%	1	1
Kaspersky Anti-virus 6	0	100.00%	647	96.82%	0	100.00%	5580	93.08%		
Kaspersky Anti-virus 8	0	100.00%	623	96.94%	0	100.00%	5294	93.43%		3
Keniu Antivirus	0	100.00%	1231	93.95%	0	100.00%	4649	94.23%		3
Kingsoft Internet Security	32	99.998%	10372	49.04%	4828	58.64%	73536	8.76%		
Microsoft Forefront Client Security	0	100.00%	608	97.01%	6	99.74%	9111	88.70%		
Norman Endpoint Protection	0	100.00%	4766	76.58%	295	83.78%	24872	69.14%		
Qihoo 360 Antivirus	0	100.00%	401	98.03%	0	100.00%	5482	93.20%		
Quick Heal Anti-Virus 2011	0	100.00%	1742	91.44%	0	100.00%	16814	79.14%		
Returnil System Safe 2011	8	98.71%	2881	85.84%	0	100.00%	27995	65.27%	1	
SGA SGA-VC	10	99.03%	283	98.61%	0	100.00%	4307	94.66%		
Sophos Endpoint Security and Control	0	100.00%	1939	90.47%	0	100.00%	9387	88.35%		1
VirusBuster for Windows Servers	0	100.00%	2541	87.51%	191	89.49%	28296	64.89%		1

Please refer to text for full product names.

vb Oct 2010 100 VIRUS virusbtn.com



Agnitum's *Outpost* suite has become a familiar and always welcome participant in our comparatives, and once again it put in a solid showing.

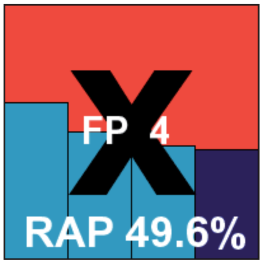
The set-up process is longer than some, thanks mainly to the suite's multiple modules including the company's well-respected firewall and also the need to install C++ components. Even with the required reboot, however, the whole process was completed in just a few minutes. The interface has had a minor overhaul recently, looking shiny and clean with an efficient and easy-to-navigate layout. A decent number of configuration options are available, although the anti-malware component is only given limited space among the other modules; scheduling is particularly simplistic. Nevertheless, all our tests ran through without problems, taking time but not too much effort – scanning speeds were fairly sluggish, with similarly heavy on-access overheads and fairly high use of system memory.

Detection rates were fairly decent, at least in the standard sets, with a RAP showing which left something to be desired. The WildList test set was handled without issues however, and the clean sets yielded nothing more than a warning of a file encrypted with the *Themida* packer. *Agnitum* gets this month's comparative off to a good start by earning a VB100 award.

AhnLab V3Net for Windows Servers 7.7.6.4

ItW	100.00%	**Polymorphic**	99.60%
ItW (o/a)	100.00%	**Trojans**	59.88%
Worms & bots	79.51%	**False positives**	4

AhnLab's server product seems like something of a step backwards after some recent improvements to the company's desktop solution, continuing the rather



anachronistic practice of separating the scanning for viruses and spyware. The installation process is uncomplicated, with no reboot needed. The interface is fairly clear and usable, though some settings are not where they might be expected to be. Running the tests proved reasonably straightforward, after some initial exploration, with good stability in the infected sets but some issues with logging – which seemed to lose track of what had been spotted when asked to work hard.

Scanning speeds were medium, with on-access lag times and RAM usage similarly middle-of-the-road, while CPU use while busy was somewhat higher than average. Detection rates were a little tricky to measure as the logging facility once again proved unreliable, dropping chunks of data off the end of lists after lengthy ‘refresh’ periods, but in the end we got some results thanks to multiple smaller scans. The results looked pretty reasonable in general, showing an alarming drop in detection of polymorphic items on access compared to on demand, and RAP scores dropped away fairly sharply after the earliest week. No problems emerged in the WildList set, but in the clean sets a couple of items were alerted on as containing malicious exploits. With the items originating from major software houses including *Microsoft* and *IBM*, which would make the issues rather serious in a business environment, there was no hesitation in denying *AhnLab* a VB100 award this month.

ArcaBit ArcaVir 2010 10.8.3204.0

ItW	99.99%	**Polymorphic**	83.14%
ItW (o/a)	99.99%	**Trojans**	63.51%
Worms & bots	68.87%	**False positives**	0

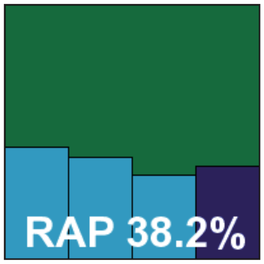
ArcaVir remains unchanged since its last appearance in our comparatives, with the 2010 edition installing in a reasonably straightforward manner (albeit with some rather unsettling pauses during which no activity registered for some time). When the process finally started up and got through its simple steps, a reboot was needed. The interface is a little quirky but generally simple to operate,

On-access tests	WildList viruses		Worms & bots		Polymorphic viruses		Trojans	
	Missed	%	Missed	%	Missed	%	Missed	%
Agnitum Outpost Security Suite Pro	0	100.00%	2598	87.23%	191	89.49%	28895	64.15%
AhnLab V3Net	0	100.00%	4279	78.98%	731	77.99%	33417	58.54%
ArcaBit ArcaVir	4	99.9997%	6355	68.77%	1854	83.14%	29538	63.35%
Avast Software avast!	0	100.00%	1731	91.49%	9	99.40%	4596	94.30%
Avertive VirusTect	22	96.61%	3393	83.33%	191	89.49%	31019	61.51%
AVG Internet Security	0	100.00%	2424	88.09%	51	97.71%	3666	95.45%
Avira AntiVir	0	100.00%	220	98.92%	0	100.00%	1745	97.83%
BitDefender Security	0	100.00%	275	98.65%	0	100.00%	4053	94.97%
Bkis BKAV	0	100.00%	1236	93.93%	1601	64.29%	7783	90.34%
Bullguard Antivirus	0	100.00%	347	98.30%	0	100.00%	5023	93.77%
CA Threat Manager	0	100.00%	5018	75.34%	3469	92.34%	44680	44.57%
Central Command Vexira	0	100.00%	2543	87.50%	191	89.49%	28484	64.66%
Commtouch Command	2	99.68%	3046	85.03%	3	99.86%	30311	62.39%
Comodo AntiVirus	7	99.03%	2996	85.28%	5185	60.69%	20741	74.27%
Comodo Internet Security	7	99.03%	2987	85.32%	5128	60.96%	20645	74.39%
Coranti 2010	0	100.00%	139	99.32%	0	100.00%	2130	97.36%
Defenx Security Suite Pro	0	100.00%	2598	87.23%	191	89.49%	28895	64.15%
Digital Defender AntiVirus	22	96.61%	3493	82.84%	191	89.49%	32298	59.93%
Emsisoft Anti-Malware	0	100.00%	419	97.94%	1314	80.08%	8799	89.08%

Please refer to text for full product names.

On-access tests contd.	WildList viruses		Worms & bots		Polymorphic viruses		Trojans	
	Missed	%	Missed	%	Missed	%	Missed	%
eScan Internet Security	0	100.00%	338	98.34%	0	100.00%	4970	93.83%
ESET NOD32	0	100.00%	674	96.69%	0	100.00%	5480	93.20%
Fortinet FortiClient	0	100.00%	844	95.85%	30	99.15%	11183	86.13%
Frisk F-PROT	0	100.00%	3007	85.23%	0	100.00%	29568	63.31%
F-Secure PSB Server Security	0	100.00%	542	97.34%	0	100.00%	5090	93.68%
G DATA AntiVirus	0	100.00%	83	99.59%	0	100.00%	570	99.29%
Hauri ViRobot	3607	67.68%	11082	45.55%	7138	49.17%	62160	22.88%
Kaspersky Anti-Virus 6	0	100.00%	797	96.08%	0	100.00%	7253	91.00%
Kaspersky Anti-Virus 8	0	100.00%	707	96.53%	0	100.00%	5988	92.57%
Keniu Antivirus	0	100.00%	18615	8.53%	0	100.00%	4649	94.23%
Kingsoft Internet Security	32	99.998%	10385	48.97%	4828	58.64%	73687	8.58%
Microsoft Forefront Client Security	0	100.00%	746	96.33%	6	99.74%	9956	87.65%
Norman Endpoint Protection	0	100.00%	5030	75.28%	343	82.65%	26550	67.06%
Qihoo 360 Antivirus	0	100.00%	493	97.58%	0	100.00%	7059	91.24%
Quick Heal Anti-Virus 2011	0	100.00%	6566	67.74%	0	100.00%	20027	75.15%
Returnil System Safe 2011	8	98.71%	3018	85.17%	0	100.00%	29699	63.15%
SGA SGA-VC	-	-	-	-	-	-	-	-
Sophos Endpoint Security and Control	0	100.00%	659	96.76%	0	100.00%	6593	91.82%
VirusBuster for Windows Servers	0	100.00%	2599	87.23%	191	89.49%	28997	64.02%

Please refer to text for full product names.



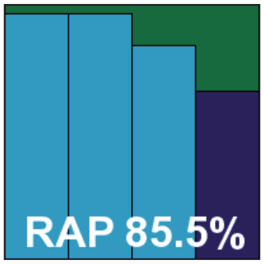
and it provides a basic level of configuration. Tests ran through without major issues. Scanning speeds and overheads did not challenge the leaders and CPU and RAM use was rather higher than many this month.

Detection rates were average in the main sets, a little underwhelming in the RAP sets, and a handful of fairly minor items in the clean sets were flagged. More seriously, however, one of the Virut variants in the WildList was not fully covered, and no VB100 award can be granted to *ArcaBit* this month.

Avast Software avast! 4.8.114

ItW	100.00%	**Polymorphic**	99.40%
ItW (o/a)	100.00%	**Trojans**	94.05%
Worms & bots	90.12%	**False positives**	0

vb 100 Oct 2010 VIRUS virusbtn.com



Once again *Avast* has made us wait to see its new server version, providing us with the aging 4.8 edition for what is almost certainly the final time. It still has the agility and toughness to outmatch many in this month's field, with a standard set of install steps followed by a reboot to get going. The GUI is a little clunky and awkward, especially compared to the delights of the new desktop edition, but it offers a comprehensive level of controls and is reasonably clear and accessible. Running through the tests was rapid and painless, with splendid scanning speeds, minimal overheads and low resource consumption.

The infected sets were brushed aside effortlessly, dealt with far faster than any other product this month, with

Reactive and Proactive (RAP) detection scores		Reactive			Reactive average	Proactive	Overall average
		week -3	week -2	week -1		week +1	
Agnitum Outpost Security Suite Pro	VIRUS 100	68.21%	54.62%	49.55%	57.46%	49.25%	55.41%
AhnLab V3Net		61.45%	49.97%	44.37%	51.93%	42.60%	49.60%
ArcaBit ArcaVir		43.83%	39.77%	32.66%	38.75%	36.50%	38.19%
Avast Software avast!	VIRUS 100	96.30%	96.12%	83.58%	92.00%	65.93%	85.48%
Avertive VirusTect		67.09%	53.38%	48.53%	56.34%	48.10%	54.28%
AVG Internet Security	VIRUS 100	95.52%	93.37%	89.12%	92.67%	69.72%	86.93%
Avira AntiVir	VIRUS 100	95.76%	86.85%	85.76%	89.46%	74.00%	85.59%
BitDefender Security	VIRUS 100	92.66%	89.07%	84.04%	88.59%	77.82%	85.90%
Bkis BKAV	VIRUS 100	71.14%	69.18%	71.19%	70.50%	71.58%	70.77%
Bullguard Antivirus	VIRUS 100	90.94%	86.33%	78.31%	85.19%	71.09%	81.66%
CA Threat Manager	VIRUS 100	52.16%	49.71%	49.19%	50.35%	53.77%	51.21%
Central Command Vexira	VIRUS 100	68.50%	55.13%	50.69%	58.11%	50.03%	56.09%
Commtouch Command		68.46%	58.04%	62.21%	62.91%	66.89%	63.90%
Comodo AntiVirus		66.70%	60.30%	54.91%	60.64%	53.99%	58.98%
Comodo Internet Security		66.72%	60.53%	54.99%	60.75%	54.04%	59.07%
Coranti 2010		95.49%	88.57%	84.68%	89.58%	84.00%	88.19%
Defenx Security Suite Pro	VIRUS 100	67.83%	54.23%	49.10%	57.05%	48.73%	54.97%
Digital Defender AntiVirus		66.03%	52.83%	51.78%	56.88%	47.98%	54.66%
Emsisoft Anti-Malware		93.93%	90.21%	86.41%	90.19%	71.23%	85.45%

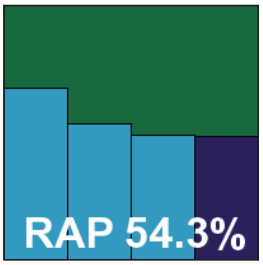
Please refer to text for full product names.

scores similarly excellent. The RAP sets were particularly well covered, albeit with a fair drop in the proactive week. The main sets and clean sets were handled splendidly, and a VB100 award is comfortably earned; we eagerly look forward to the upcoming new version.

Avertive VirusTect 1.1.8

ItW	100.00%	**Polymorphic**	89.49%
ItW (o/a)	96.61%	**Trojans**	64.00%
Worms & bots	87.05%	**False positives**	0

A newcomer this month, *Avertive* is another member of a growing stable of solutions based on an SDK and interface overlaid on the *VirusBuster* engine. These are generally made available through ISPs. The surprise last-minute submission of this product meant an online update was required on the deadline day, but the set-up process was fairly painless and all done within under a minute with no reboot needed. The interface is simple and colourful – instantly familiar from several others we have seen recently and hence easy to navigate. Controls are provided in reasonable depth, and easy to find.



Scanning speeds were not the fastest, showing no sign of smart caching of previous results, but performance measures were decent and the infected sets were managed with good stability. Detection rates were not overwhelming, but not too bad, with a single item in the clean set alerted on as being packed with *Themida* but no false alarms. The WildList was covered comfortably on demand, but strangely on access a handful of items were missed. The result was so surprising we repeated the scan multiple times but got identical results, and as a result *Avertive* doesn't quite earn its first VB100 award.

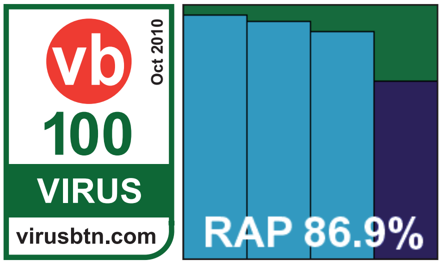
Reactive and Proactive (RAP) detection scores contd.		Reactive			Reactive average	Proactive	Overall average
		week -3	week -2	week -1		week +1	
eScan Internet Security	VIRUS 100	91.91%	87.56%	81.15%	86.87%	72.20%	83.20%
ESET NOD32	VIRUS 100	96.68%	96.77%	93.70%	95.71%	79.43%	91.64%
Fortinet FortiClient	VIRUS 100	83.67%	57.67%	43.31%	61.55%	36.43%	55.27%
Frisk F-PROT		67.92%	53.74%	60.00%	60.55%	65.27%	61.73%
F-Secure PSB Server Security	VIRUS 100	93.34%	82.93%	67.67%	81.31%	66.70%	77.66%
G DATA AntiVirus	VIRUS 100	99.55%	98.00%	91.53%	96.36%	77.29%	91.59%
Hauri ViRobot		50.44%	48.74%	41.29%	46.82%	41.26%	45.43%
Kaspersky Anti-Virus 6	VIRUS 100	93.50%	91.15%	83.47%	89.38%	65.70%	83.46%
Kaspersky Anti-Virus 8	VIRUS 100	93.86%	91.39%	85.32%	90.19%	71.51%	85.52%
Keniu Antivirus	VIRUS 100	91.64%	89.73%	81.45%	87.61%	67.98%	82.70%
Kingsoft Internet Security		16.22%	14.53%	14.59%	15.11%	22.25%	16.90%
Microsoft Forefront Client Security	VIRUS 100	91.68%	87.10%	78.89%	85.89%	63.62%	80.32%
Norman Endpoint Protection	VIRUS 100	46.62%	37.83%	40.23%	41.56%	49.77%	43.61%
Qihoo 360 Antivirus	VIRUS 100	90.34%	81.16%	70.42%	80.64%	67.51%	77.36%
Quick Heal Anti-Virus 2011	VIRUS 100	74.80%	63.85%	51.41%	63.35%	50.89%	60.24%
Returnil System Safe 2011		68.37%	53.47%	57.95%	59.93%	65.44%	61.31%
SGA SGA-VC		92.23%	88.35%	83.47%	88.01%	74.07%	84.53%
Sophos Endpoint Security and Control	VIRUS 100	88.86%	84.54%	76.33%	83.24%	68.52%	79.56%
VirusBuster for Windows Servers	VIRUS 100	68.11%	54.61%	49.50%	57.41%	49.22%	55.36%

Please refer to text for full product names.

AVG Internet Security Business Edition 9.0.851

ItW	100.00%	**Polymorphic**	97.71%
ItW (o/a)	100.00%	**Trojans**	96.37%
Worms & bots	88.49%	**False positives**	0

AVG's corporate version is barely different from the company's standard desktop suite solution, with a simple installation process which offers an impressive range of languages including two varieties of Bahasa. The set-up completes without needing a reboot and provides a rather cluttered interface covering the multiple modules included. Controls are offered in splendid depth, perfectly suited to a business environment, and running our various jobs proved no problem for it.

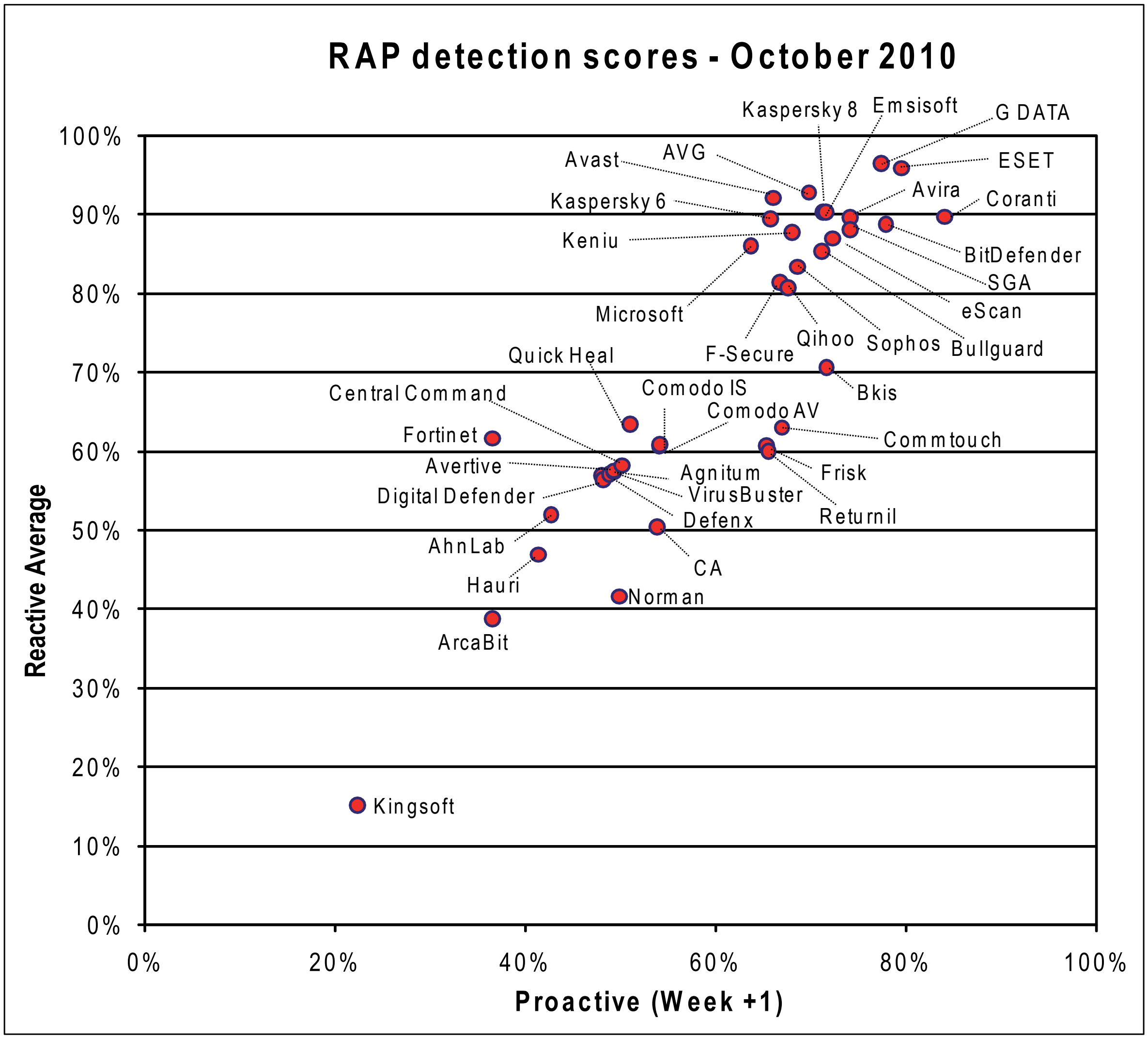


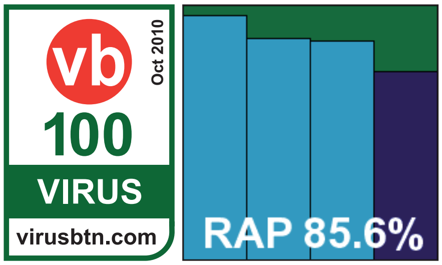
Scanning speeds were rather sluggish, and resource usage fairly high, although on-access overheads were not too bad. Detection rates were solid though, with good levels across all sets, and with no problems in the core certification areas *AVG* easily earns another VB100 award.

Avira AntiVir Server 10.00.06.00

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	98.16%
Worms & bots	99.02%	**False positives**	0

One of our most consistent participants and a reliable performer, *Avira*'s server edition is a proper business product but installs fairly rapidly, with most of the brief set-up time taken up by the installation of C++ components.





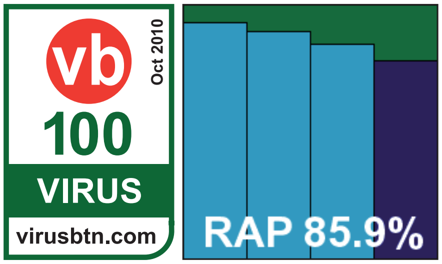
The interface makes good use of the MMC system, with a logical and easily navigable layout, and provides a full set of configuration controls to satisfy the most demanding administrator.

Scanning speeds were good, with fairly low overheads and resource drain. The infected sets were handled fairly well too, with a couple of files apparently snagging the scanner and having to be removed to keeps things moving along, but some superb detection scores. The proactive week of the RAP sets was particularly well handled. With nothing much to complain about anywhere, *Avira* earns a VB100 award with minimum fuss.

BitDefender Security for File Servers 3.4.141

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	95.42%
Worms & bots	98.88%	**False positives**	0

BitDefender's server solution is another fully fledged business product, again using the MMC console for its control system but installing rapidly, with user interaction



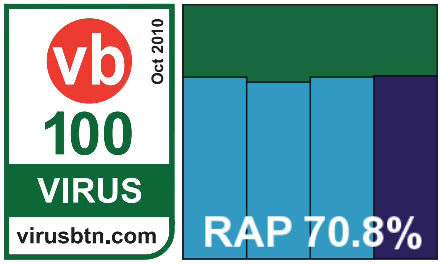
kept to a minimum and no need to reboot. The layout is good, making good use of the console base to provide complete and rational access to configuration and control. Scanning speeds were decent on the initial runs, and remarkable on repeat visits to known files, with excellent use of smart caching techniques. CPU use was very low, probably thanks to the same techniques, while memory use was perhaps a little above average.

In the infected sets, we had a few problems with scans apparently completing but presenting only a blank, unresponsive screen. Retrying the scans in smaller batches yielded better results, implying that the logging system is easily overwhelmed by large numbers of detections – admittedly not something that most real-world users are likely to encounter. Further investigation showed that in some cases we may have been a little hasty, giving up on the logging system after only half an hour or so, as some logs did later emerge after huge periods of unresponsiveness.

In the end, we managed to gather all the information needed, which showed solid scores in the infected sets and no problems in the clean sets; *BitDefender* thus earns a VB100 award, having put us through considerable pains to get there.

Bkis BKAV Gateway Scan 2910

ItW	100.00%	**Polymorphic**	64.29%
ItW (o/a)	100.00%	**Trojans**	90.34%
Worms & bots	93.93%	**False positives**	0

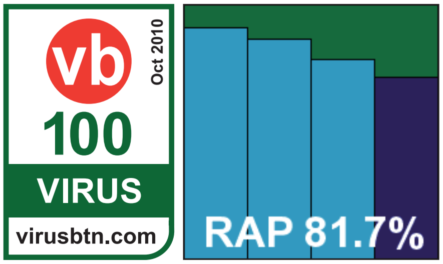


Bkis has become a familiar name in our tests in the last few months, and has shown steady improvement throughout its run of appearances. The product itself has a remarkably rapid installation process, with only a single click and no reboot needed, and the interface provides a basic level of controls with very little fuss. No archive scanning is provided as far as we could tell, so the archive set was scanned very rapidly, but other sets were very slow to get through, with on-access overheads rather high to match. Memory consumption was fairly low however, although CPU use was high.

The infected sets were handled without problems, and showed some very impressive scores indeed – a huge step up from previous performances. The WildList presented no problems, and with the clean sets covered without issues *Bkis* is a worthy winner of a VB100 award.

Bullguard Antivirus 9.0

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	93.77%
Worms & bots	98.30%	**False positives**	0



Bullguard's solution is clearly designed more for the home-user market than for business, but nevertheless operates perfectly well on this month's platform. It installs easily in very few steps and with no reboot needed, and offers online back-up as part of its line-up. The interface is bright and colourful, with large buttons which seem designed with the clumsiest of users in mind. Navigation is not completely straightforward, but after some poking around we found a basic set of options provided, and ran through the scans with no major problems other than the log access buttons being rather surprisingly buried at the bottom of the results lists.

Once the logs were found and converted into usable format, detection rates proved to be excellent, with a steady decline across the RAP sets but still a decent level even in the proactive week. With no issues in the WildList or clean sets, *Bullguard* easily earns a VB100 award this month.

CA Integrated Threat Manager 8.1.66.0.0

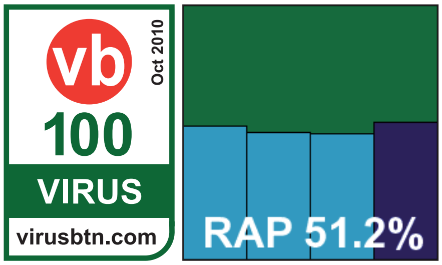
ItW	100.00%	**Polymorphic**	92.34%
ItW (o/a)	100.00%	**Trojans**	44.57%
Worms & bots	75.34%	**False positives**	0

After many years of prayer, and even begging, it looks like this could at last be the final appearance of this version of *CA*'s product, with a much-heralded new edition on the horizon. We have described the lengthy install process, with its multiple EULAs and data-gathering screens, and the

On-demand throughput (MB/s)	Archive files			Binaries and system files			Media and documents			Other file types		
	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files
Agnitum Outpost Security Suite Pro	1.85	26.43	1.85	23.46	289.77	23.46	8.91	35.89	8.91	9.02	120.22	9.02
AhnLab V3Net	4.90	5.29	4.90	17.41	36.76	17.41	22.47	24.79	22.47	21.22	22.54	21.22
ArcaBit ArcaVir	8.89	9.00	8.89	15.89	15.79	15.89	30.06	30.44	30.06	17.45	17.74	17.45
Avast Software avast!	290.69	415.28	7.86	47.83	52.41	41.05	33.87	50.09	35.89	45.08	60.11	24.59
Avertive VirusTect	5.17	5.18	N/A	31.38	32.84	31.38	16.58	17.18	16.58	16.39	16.39	16.39
AVG Internet Security	0.70	138.43	0.70	17.59	26.34	16.93	6.03	6.12	5.73	5.82	5.82	4.45
Avira AntiVir	6.81	6.78	6.81	65.68	59.35	65.68	24.29	28.63	24.29	21.22	22.54	21.22
BitDefender Security	4.36	242.24	4.36	22.09	289.77	22.09	10.15	89.06	10.15	7.21	56.95	7.21
Bkis BKAV	111.81	116.28	N/A	4.49	4.54	4.49	5.81	5.95	5.81	4.21	4.24	4.21
Bullguard Antivirus	8.52	8.81	8.52	44.38	46.04	44.38	22.26	24.05	22.26	19.67	20.81	20.42
CA Threat Manager	4.47	4.43	4.47	46.04	47.37	46.04	33.40	33.40	33.40	18.66	18.98	18.66
Central Command Vexira	11.96	14.32	4.07	30.41	44.38	28.98	22.26	31.23	17.30	20.04	23.52	15.46
Commtouch Command	9.32	9.38	9.32	19.55	19.63	19.55	27.02	27.32	27.02	16.91	16.39	16.91
Comodo AntiVirus	9.26	9.26	9.26	38.19	41.75	38.19	54.65	58.65	54.65	38.64	38.64	38.64
Comodo Internet Security	9.23	9.26	9.23	37.32	41.75	37.32	55.92	60.11	55.92	37.31	40.07	37.31
Coranti 2010	3.56	3.63	3.56	6.59	6.59	6.59	4.03	4.05	4.03	3.23	3.23	3.23
Defenx Security Suite Pro	1.87	26.43	1.87	22.91	273.67	22.91	8.62	35.89	8.62	9.09	135.25	9.09
Digital Defender AntiVirus	5.29	5.25	0.93	31.18	33.28	3.31	16.47	16.36	3.65	16.15	16.15	3.72
Emsisoft Anti-Malware	7.65	8.86	N/A	9.97	10.01	9.97	20.04	19.08	20.04	14.05	14.24	14.05

Please refer to text for full product names.

interface with its sluggish response times and lack of permanency of settings, more than enough times in these pages, but despite our complaints about the surface, underneath its ungainly covers *CA*'s scanning remains solid, reliable and quite remarkably rapid. To do this it uses a fair amount of RAM, but not too many processor cycles.



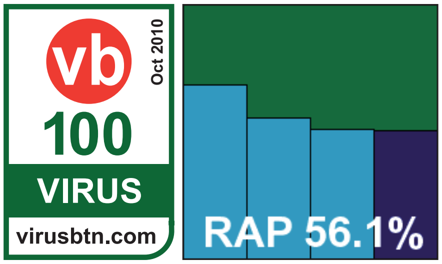
Detection rates were less than stellar, but not too disappointing, and the WildList presented no problems. With the clean set also handled nicely, *CA* earns another VB100 award – perhaps the last with this particular product version; we look forward greatly to the refreshed edition.

Central Command Vexira Antivirus for Servers 6.3.14

ItW	100.00%	**Polymorphic**	89.49%
ItW (o/a)	100.00%	**Trojans**	65.53%
Worms & bots	87.79%	**False positives**	0

On-demand throughput (MB/s) contd.	Archive files			Binaries and system files			Media and documents			Other file types		
	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files
eScan Internet Security	12.42	484.49	12.42	10.09	46.92	10.09	1.62	20.38	1.62	7.57	27.05	7.57
ESET NOD32	4.87	4.86	4.87	56.62	56.62	56.62	14.31	14.66	14.31	14.82	0.85	14.82
Fortinet FortiClient	7.00	8.12	7.00	9.79	10.59	9.79	12.59	14.06	12.59	16.65	18.34	16.65
Frisk F-PROT	11.05	11.18	11.05	18.73	19.09	18.73	16.58	19.24	16.58	23.52	30.06	23.52
F-Secure PSB Server Security	7.86	2906.94	7.86	25.66	1642.04	25.66	24.05	480.90	24.05	17.45	541.00	17.45
G DATA AntiVirus	4.26	2906.94	4.26	29.15	1642.04	29.15	20.21	601.13	20.21	15.46	360.67	15.46
Hauri ViRobot	2.25	2.31	N/A	13.10	13.61	13.10	3.70	3.67	3.70	3.00	2.98	3.00
Kaspersky Anti-Virus 6	6.20	1453.47	6.20	25.39	703.73	25.39	15.82	200.38	15.82	11.63	180.33	11.63
Kaspersky Anti-Virus 8	3.08	2906.94	3.08	16.59	821.02	16.59	9.58	240.45	9.58	6.56	180.33	6.56
Keniu Antivirus	3.13	1453.47	3.13	31.38	46.92	31.38	11.96	126.55	11.96	8.14	98.36	8.14
Kingsoft Internet Security	2.60	2.61	2.60	35.19	36.22	35.19	9.21	9.54	9.21	21.64	24.04	21.64
Microsoft Forefront Client Security	4.59	4.64	4.59	19.55	20.19	19.55	27.32	30.44	27.32	19.67	19.32	19.32
Norman Endpoint Protection	0.91	0.91	0.91	2.96	2.97	2.96	4.67	4.77	4.67	3.30	3.32	3.30
Qihoo 360 Antivirus	4.40	4.73	4.40	26.63	27.52	26.63	14.66	14.93	15.51	11.39	11.27	11.51
Quick Heal Anti-Virus 2011	4.60	6.37	3.30	60.82	61.58	60.82	68.70	68.70	12.46	120.22	51.52	12.44
Returnil System Safe 2011	6.71	6.81	6.71	17.28	17.22	17.28	8.10	8.18	8.10	13.20	13.20	13.20
SGA SGA-VC	4.95	5.22	4.95	10.16	10.64	10.16	6.68	6.79	6.68	6.08	6.08	6.15
Sophos Endpoint Security and Control	207.64	264.27	1.90	18.11	18.38	16.59	28.97	34.85	26.14	15.24	16.15	12.44
VirusBuster for Windows Servers	11.91	13.91	11.91	30.79	44.78	29.15	23.57	30.06	16.70	20.04	22.54	15.24

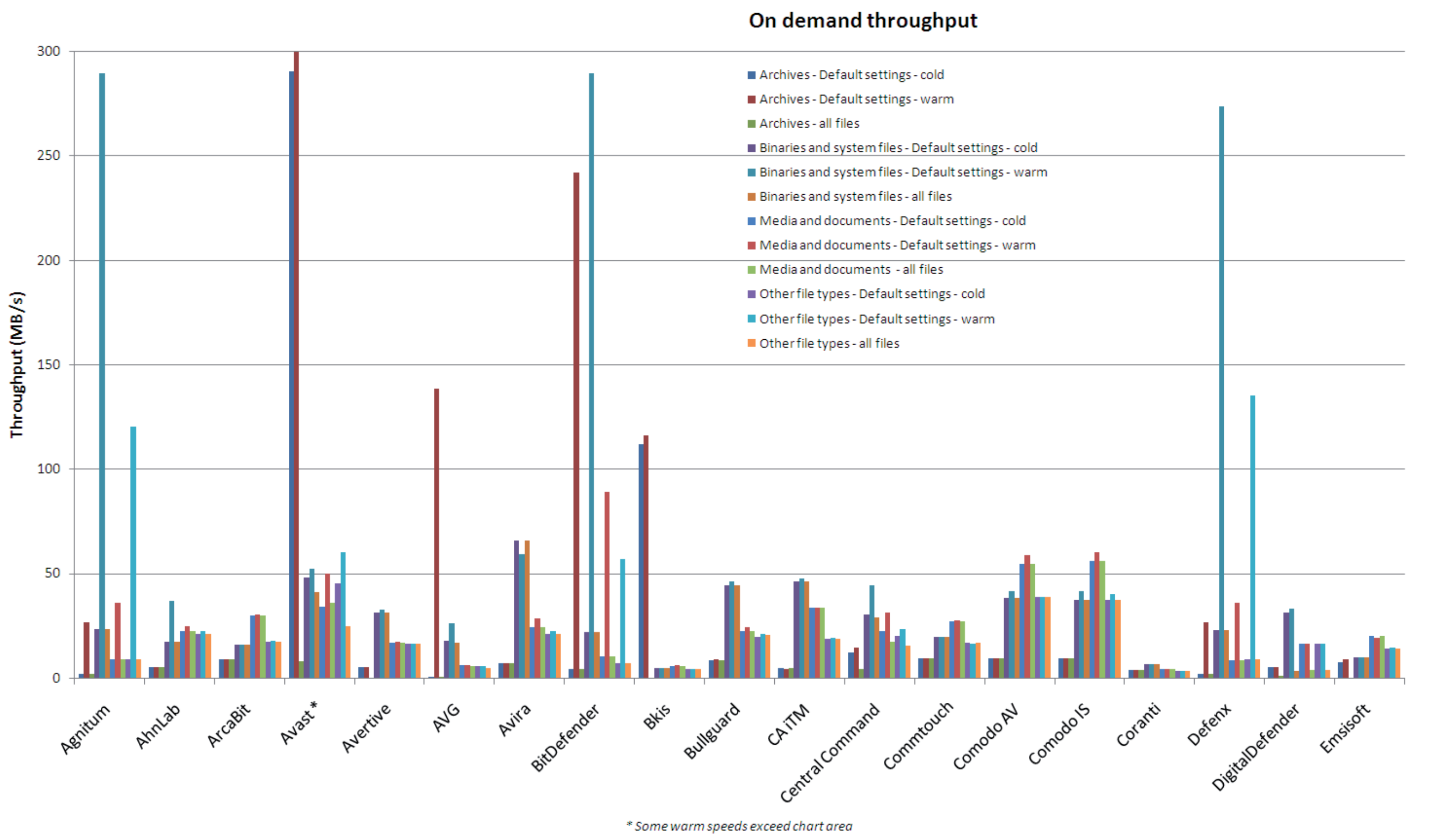
Please refer to text for full product names.



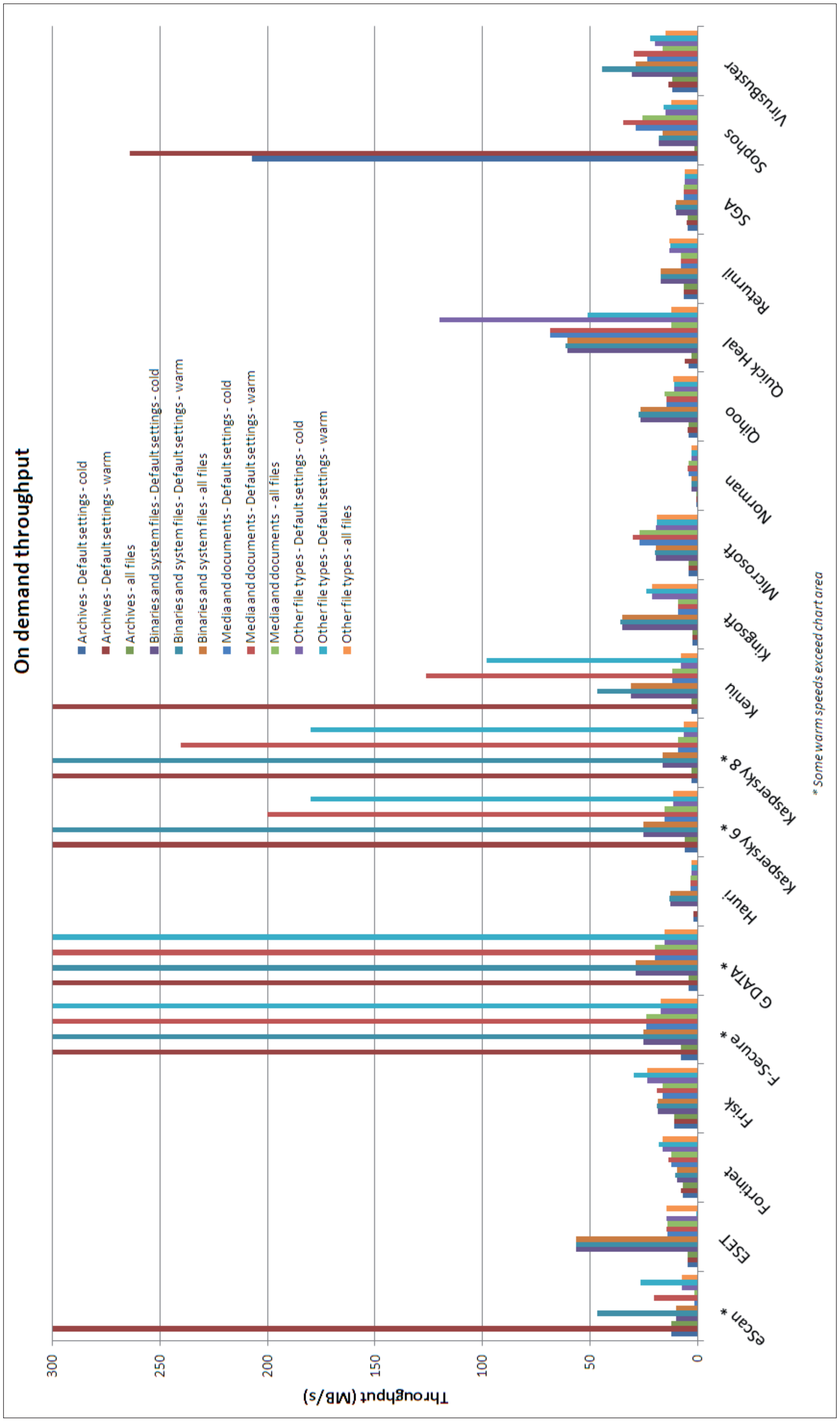
The server edition of *Vexira* has been seen many times in our tests, being very similar to that of another product.

It has a rather lengthy installation process in terms of stages, but it doesn't take too long, as long as the 'next' button is clicked with alacrity; no reboot is required to complete. The console is not a great example of implementation of the MMC system, being inconsistent and awkward, but with some practice it can be used with reasonable comfort. Some of the controls – notably the options for archive handling on-access – remain seemingly non-functional after many reports in these pages. The scheduler seemed a little unreliable too, with jobs set to run during the night failing to run at all, leaving a message merely informing us that 'the parameter was incorrect' – another identical scan set manually ran without issues.

Scanning speeds, overheads and resource usage were all fairly mid-range. Detection rates were somewhat more difficult to measure as the logs appeared to be deleted after a seemingly random interval, despite the options being set



Please refer to text for full product names.



Please refer to text for full product names.

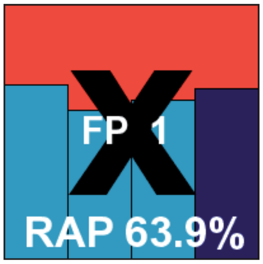
File access lag time (s/MB)	Archive files			Binaries and system files			Media and documents			Other file types		
	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files
Agnitum Outpost Security Suite Pro	0.008	0.001	N/A	0.035	0.001	0.035	0.087	0.013	0.087	0.111	0.011	0.111
AhnLab V3Net	0.010	0.011	N/A	0.017	0.016	N/A	0.038	0.036	N/A	0.039	0.036	N/A
ArcaBit ArcaVir	0.002	0.003	0.098	0.036	0.036	0.038	0.021	0.019	0.021	0.017	0.012	0.039
Avast Software avast!	0.014	0.001	0.130	0.022	0.001	0.026	0.035	0.003	0.036	0.038	0.003	0.039
Avertive VirusTect	0.001	0.002	N/A	0.031	0.031	N/A	0.008	0.003	N/A	0.013	0.007	N/A
AVG Internet Security	0.001	0.001	NA	0.037	0.008	0.005	0.062	0.032	0.029	0.088	0.034	0.038
Avira AntiVir	0.003	0.001	0.031	0.017	0.001	0.017	0.032	0.026	0.029	0.038	0.036	0.035
BitDefender Security	0.006	0.001	0.178	0.023	0.000	0.031	0.045	0.002	0.058	0.064	0.002	0.076
Bkis BKAV	0.005	0.005	N/A	0.158	0.158	0.158	0.100	0.099	0.100	0.137	0.136	0.136
Bullguard Antivirus	0.112	0.112	0.112	0.035	0.035	0.035	0.073	0.070	0.073	0.089	0.088	0.089
CA Threat Manager	0.007	0.005	N/A	0.017	0.017	0.017	0.026	0.022	0.026	0.045	0.044	0.045
Central Command Vexira	0.001	0.001	0.003	0.030	0.028	0.028	0.038	0.034	0.046	0.058	0.057	0.069
Commtouch Command	0.014	0.014	N/A	0.045	0.045	N/A	0.029	0.027	N/A	0.034	0.033	N/A
Comodo AntiVirus	0.001	0.001	N/A	0.036	0.036	0.036	0.019	0.019	0.019	0.029	0.029	0.029
Comodo Internet Security	0.001	0.000	NA	0.042	0.036	0.042	0.021	0.020	0.021	0.032	0.029	0.032
Coranti 2010	0.013	0.013	0.021	0.136	0.135	0.135	0.209	0.207	0.232	0.248	0.247	0.291
Defenx Security Suite Pro	0.009	0.001	N/A	0.035	0.000	0.035	0.088	0.013	0.088	0.111	0.011	0.111
Digital Defender AntiVirus	0.002	0.002	N/A	0.032	0.031	N/A	0.009	0.005	N/A	0.010	0.011	N/A
Emsisoft Anti-Malware	0.081	0.001	N/A	0.104	0.001	0.104	1.063	0.005	1.063	2.510	0.004	2.510

Please refer to text for full product names.

to store an unlimited amount of data for 15 days. Some closer analysis seemed to suggest that the 'unlimited' setting did not, in fact, mean that at all, but we could not determine whether it did set an arbitrary limit or simply dropped results when it felt like it. In the end we set it to the highest available number of records (somewhat less than half the number of items in our sets) and carefully watched as it ran through the scan multiple times, saving the log at judicious moments. The results showed some reasonable scores in the main sets, dropping below half in the later weeks of the RAPs. No problems were encountered in the clean sets, other than a warning that a file packed with *Themida* might be considered suspicious, and *Central Command* thus just about earns another VB100 award.

Commtouch Command Anti-Malware 5.1.0

ItW	100.00%	**Polymorphic**	99.86%
ItW (o/a)	99.68%	**Trojans**	64.68%
Worms & bots	85.97%	**False positives**	1



The company formerly known as *Authentium* was acquired by *Commtouch* in the weeks leading up to this month's comparative. The product remains unchanged however, with its usual fast and simple set-up process and pared-down interface; even activation of the 'advanced'

File access lag time (s/MB) contd.	Archive files			Binaries and system files			Media and documents			Other file types		
	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files
eScan Internet Security	0.001	0.001	0.062	0.020	0.001	0.002	0.041	0.002	0.008	0.015	0.002	0.024
ESET NOD32	0.001	0.001	N/A	0.007	0.006	0.007	0.062	0.061	0.063	0.049	0.048	0.050
Fortinet FortiClient	0.110	0.001	0.110	0.093	0.001	0.093	0.045	0.003	0.045	0.069	0.004	0.069
Frisk F-PROT	0.004	0.004	N/A	0.043	0.043	0.043	0.016	0.013	0.016	0.027	0.024	0.027
F-Secure PSB Server Security	0.001	0.001	0.618	0.059	0.000	0.077	0.066	0.002	0.134	0.104	0.002	0.197
G DATA AntiVirus	0.047	0.001	0.047	0.058	0.001	0.058	0.083	0.007	0.083	0.113	0.009	0.113
Hauri ViRobot	0.001	0.001	N/A	0.012	0.017	0.013	0.051	0.048	0.094	0.018	0.012	0.111
Kaspersky Anti-Virus 6	0.003	0.001	0.024	0.030	0.000	0.033	0.066	0.007	0.070	0.099	0.008	0.106
Kaspersky Anti-Virus 8	0.005	0.001	0.081	0.035	0.002	0.006	0.074	0.015	0.018	0.108	0.018	0.024
Keniu Antivirus	0.005	0.001	N/A	0.027	0.001	0.027	0.070	0.008	0.070	0.101	0.010	0.101
Kingsoft Internet Security	0.001	0.001	N/A	0.021	0.001	0.021	0.099	0.001	0.099	0.037	0.001	0.037
Microsoft Forefront Client Security	0.002	0.001	N/A	0.046	0.000	0.046	0.026	0.001	0.026	0.047	0.001	0.047
Norman Endpoint Protection	0.005	0.005	N/A	0.086	0.086	0.086	0.205	0.203	0.205	0.251	0.250	0.251
Qihoo 360 Antivirus	0.001	0.001	N/A	0.001	0.001	0.003	0.010	0.009	0.010	0.011	0.008	0.008
Quick Heal Anti-Virus 2011	0.026	0.006	N/A	0.014	0.004	0.014	0.070	0.031	0.070	0.068	0.067	0.068
Returnil System Safe 2011	0.020	0.020	N/A	0.050	0.051	0.050	0.111	0.109	0.111	0.050	0.048	0.050
SGA SGA-VC	0.000	0.001	N/A	0.003	0.001	N/A	0.018	0.003	N/A	0.017	0.003	N/A
Sophos Endpoint Security and Control	0.002	0.002	0.498	0.051	0.051	0.056	0.024	0.022	0.030	0.058	0.058	0.068
VirusBuster for Windows Servers	0.001	0.001	N/A	0.031	0.028	0.028	0.036	0.034	0.048	0.060	0.058	0.070

Please refer to text for full product names.

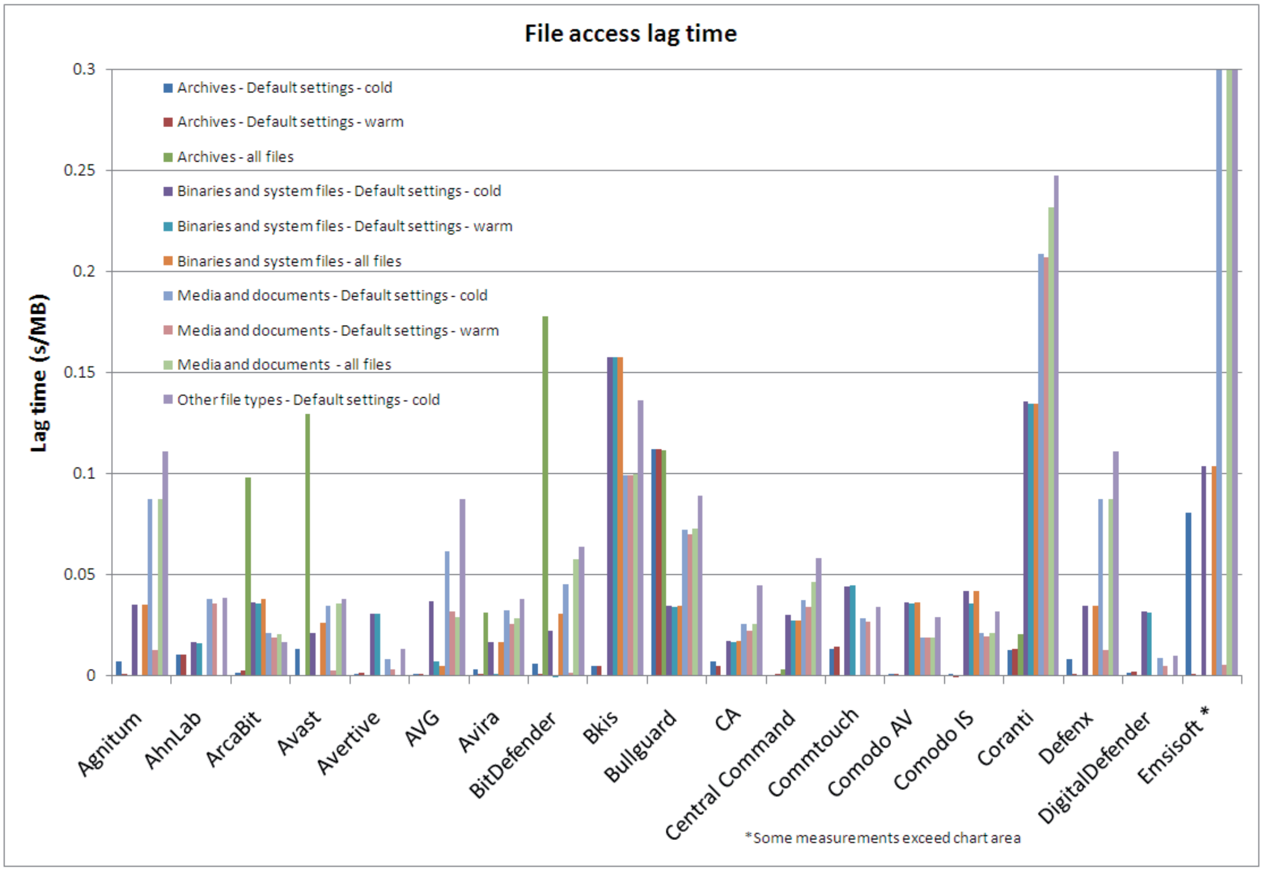
mode offers no more than the basic set of configuration options. Scanning speeds were decent, with fairly low overheads but notably high use of CPU cycles when heavily engaged in checking files.

Detection rates were not outstanding, with a rather surprising upturn in scores in the proactive week of the RAP sets. The core WildList set was handled ably on demand, but on access a pair of items seemed to go undetected. Consultation with the developers could not pin down the problem, which was not reproducible elsewhere, but multiple installs in our lab showed the same result. In the clean sets a single item was flagged with a generic malware alert; the item was the installer for a version of *Mozilla Firefox*. There was thus little choice but to deny *Commtouch* its first VB100 award under its new name, despite the false alarm having been fixed shortly after the products were submitted for testing.

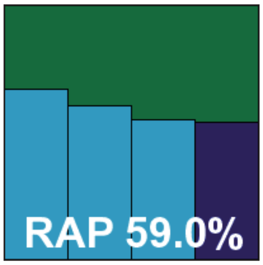
Comodo Antivirus 4.1.150349.920

ItW	99.03%	**Polymorphic**	60.96%
ItW (o/a)	99.03%	**Trojans**	75.43%
Worms & bots	86.01%	**False positives**	0

At long last, after many years of topping the list of products most requested by our readers to appear in our



Please refer to text for full product names.



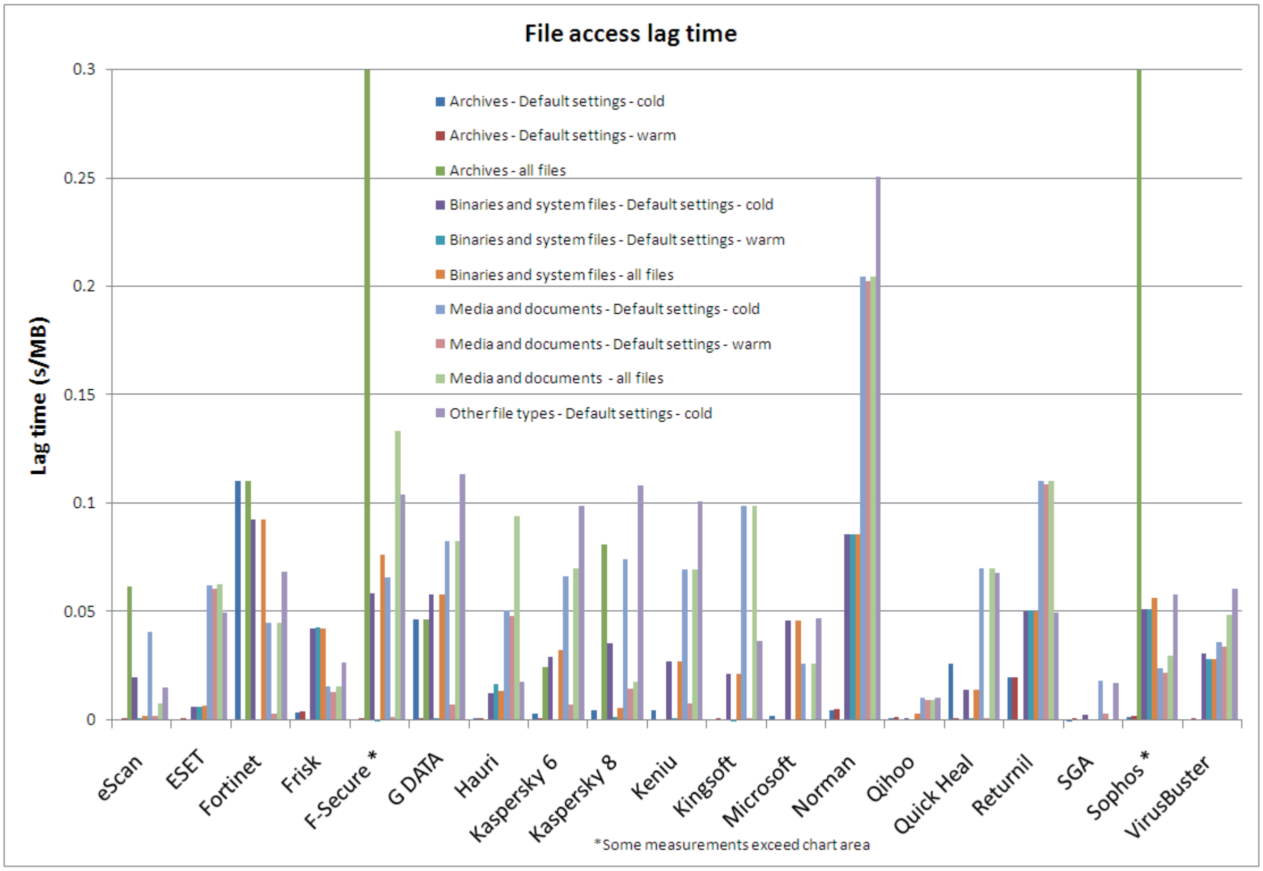
tests, *Comodo* has decided to make its first appearance, with two products included in this month's comparative. The first is a 'plain' AV solution, although it offers much more than the basics of static malware detection, with a range of extra layers including sandboxing of suspicious processes covered by the 'Defense+' modules. The installation process is fairly lengthy, enlivened by a lengthy list of available languages – many of the translations being provided by members of the company's large and active community of fans. A reboot is needed to complete the set-up.

The interface is clean and slick, with some clear, if rather wordy details of current status on the main page and a good level of fine-tuning under the surface – all of which is laid out in a sensible and usable way. We quickly zipped through the tests, with some excellent running times for on-demand scans and low overheads for file accessing; memory usage was mid-range, while CPU use was a little higher than average.

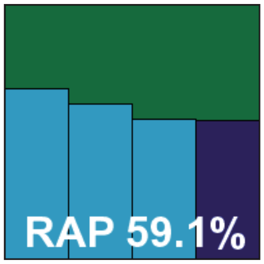
Gathering detection data proved no problem, with good stability under the heavy bombardment of our infected test sets. Detection scores were pretty decent in the main sets, with a reasonable showing in the RAP sets too. The clean set was a little more tricky, with a couple of files somewhere in the batch of sample packages from *Microsoft* getting the scanner into some deep water, from which only a hard reboot could recover things in some cases. In the end full data was gathered, with no false positives in our extended sets – an impressive achievement for a first-timer. In the WildList set however, a handful of more recent items were not covered, including a single sample from a set of 2,500 of one of the latest Virut strains. Although this means that *Comodo* does not manage to earn a VB100 award, an otherwise excellent performance is a sign of good things to come.

Comodo Internet Security Premium 4.1.150349.920

ItW	99.03%	**Polymorphic**	60.93%
ItW (o/a)	99.03%	**Trojans**	75.55%
Worms & bots	86.06%	**False positives**	0



Please refer to text for full product names.

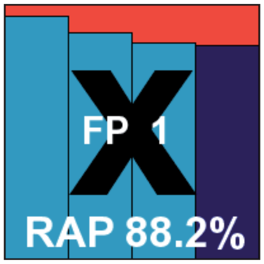


The second of *Comodo*'s offerings this month provides the same impressive selection of defences, plus more besides, including the company's highly regarded firewall. Despite the 'premium' of the title, the product appears to be available for free on the same terms as the standard product. The installation process is similarly straightforward, and the interface almost identical. Scanning speeds, overheads and resource usage were pretty closely matched too.

Detection rates were likewise hard to tell apart from the basic product, although a selection of items on the local system drive were alerted on as suspicious, all in the dll cache. The same set of WildList items were not covered, so no VB100 award can be granted this month, but the product looks very impressive and seems certain to put in some splendid performances in the near future.

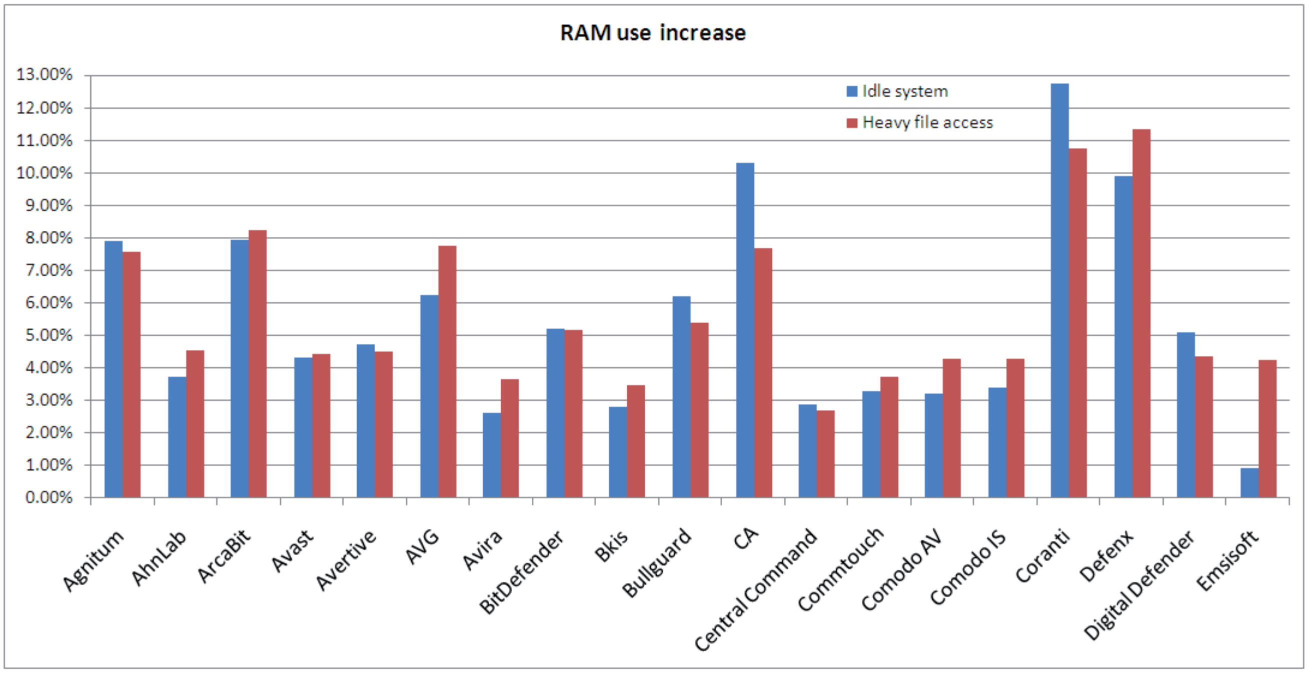
Coranti 2010 1.000.0044

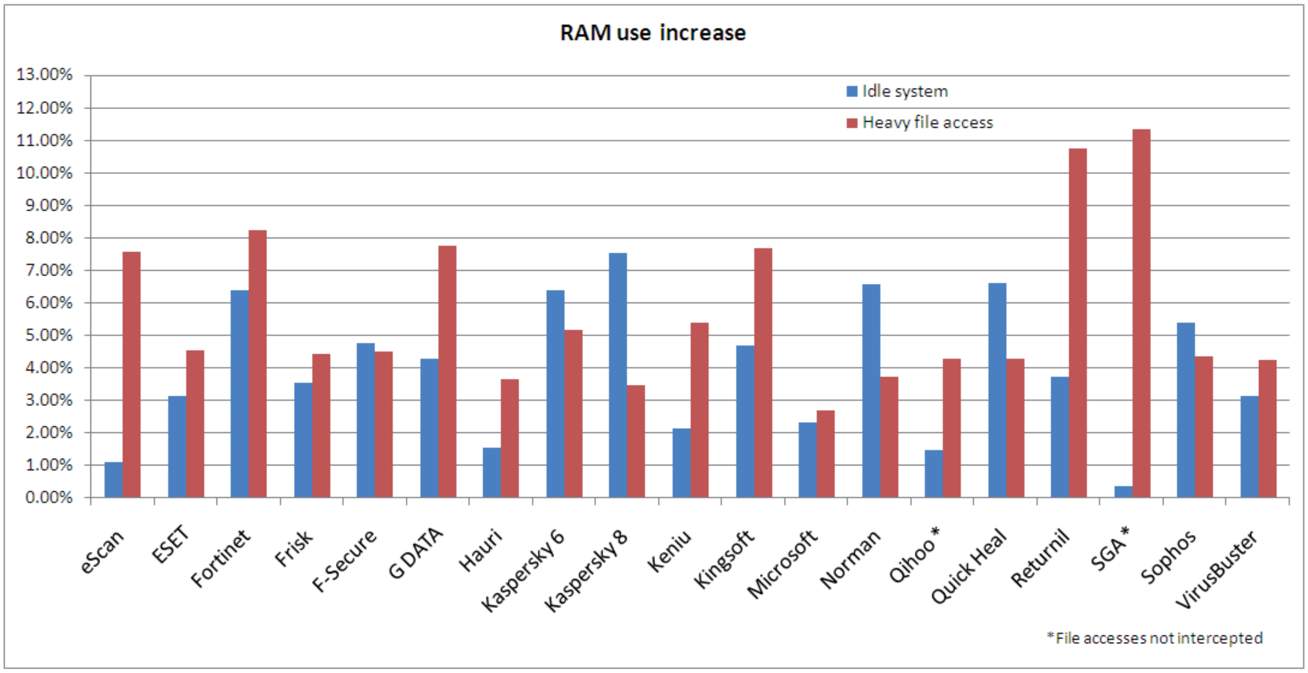
ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	97.36%
Worms & bots	99.32%	**False positives**	1



Coranti, we learned this month, is based in Japan, and its product seems to have dropped the earlier 'Multicore' name in favour of a simpler approach. The multi-engine technique remains unchanged, but the installer package provided for testing was far from the biggest this month, despite the multiple components, and the set-up process was fast and simple, with no need for a reboot to get protection in place.

The interface has an air of comprehensive solidity, without seeming overly grey and businesslike, and includes an





*File accesses not intercepted

Please refer to text for full product names.

excellent degree of configuration for the three main engines (provided by *BitDefender*, *Frisk* and *Norman*) plus the anti-spyware component from *Lavasoft*.

Operating and controlling the product is a pleasure, it being very responsive and simple to navigate, and while scanning times were far from the fastest they were not unbearably slow either. As might be anticipated, resource consumption is fairly high.

This heavy system impact is made up for by the excellent detection level, which proved splendid across the board,

Product	RAM use increase – idle system	RAM use increase – heavy file access	CPU use increase – heavy file access
Agnitum	7.90%	7.57%	94.47%
AhnLab	3.73%	4.55%	102.76%
ArcaBit	7.94%	8.23%	108.80%
Avast	4.31%	4.45%	67.96%
Avertive	4.74%	4.51%	65.90%
AVG	6.23%	7.77%	120.59%
Avira	2.62%	3.65%	71.40%
BitDefender	5.23%	5.16%	54.34%
Bkis	2.80%	3.48%	157.83%
Bullguard	6.21%	5.38%	121.82%
CA	10.31%	7.69%	77.09%
Central Command	2.88%	2.70%	90.58%
Commtouch	3.31%	3.73%	154.43%
Comodo AV	3.21%	4.27%	117.53%
Comodo IS	3.39%	4.30%	105.44%
Coranti	12.74%	10.74%	174.07%
Defenx	9.92%	11.34%	110.62%
Digital Defender	5.09%	4.36%	59.43%
Emsisoft	0.91%	4.23%	156.55%

Please refer to text for full product names.

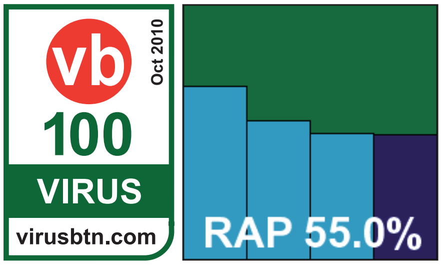
Product	RAM use increase – idle system	RAM use increase – heavy file access	CPU use increase – heavy file access
eScan	1.11%	2.00%	50.48%
ESET	3.15%	2.32%	104.31%
Fortinet	6.40%	6.60%	103.15%
Frisk	3.54%	3.64%	135.52%
F-Secure	4.75%	5.70%	89.13%
G DATA	4.28%	4.93%	122.34%
Hauri	1.54%	1.68%	93.29%
Kaspersky AV 6	6.41%	4.60%	74.42%
Kaspersky AV 8	7.55%	7.36%	95.01%
Keniu	2.15%	2.59%	96.39%
Kingsoft	4.70%	3.35%	64.86%
Microsoft	2.34%	3.10%	55.83%
Norman	6.59%	7.40%	199.69%
Qihoo	1.48%	2.55%	25.80%
Quick Heal	6.60%	9.16%	63.98%
Returnil	3.72%	3.74%	167.86%
SGA	0.38%	0.38%	70.66%
Sophos	5.40%	4.19%	119.89%
VirusBuster	4.33%	4.23%	63.56%

with one of the highest scores we've seen yet in the proactive week of the RAP sets. As sharp-eyed readers may have predicted of course, there is a flipside to the combination of multiple engines, and this month a single false positive already noted in another product using one of the engines included here denies *Coranti* a VB100 award, despite a perfect showing in the WildList set.

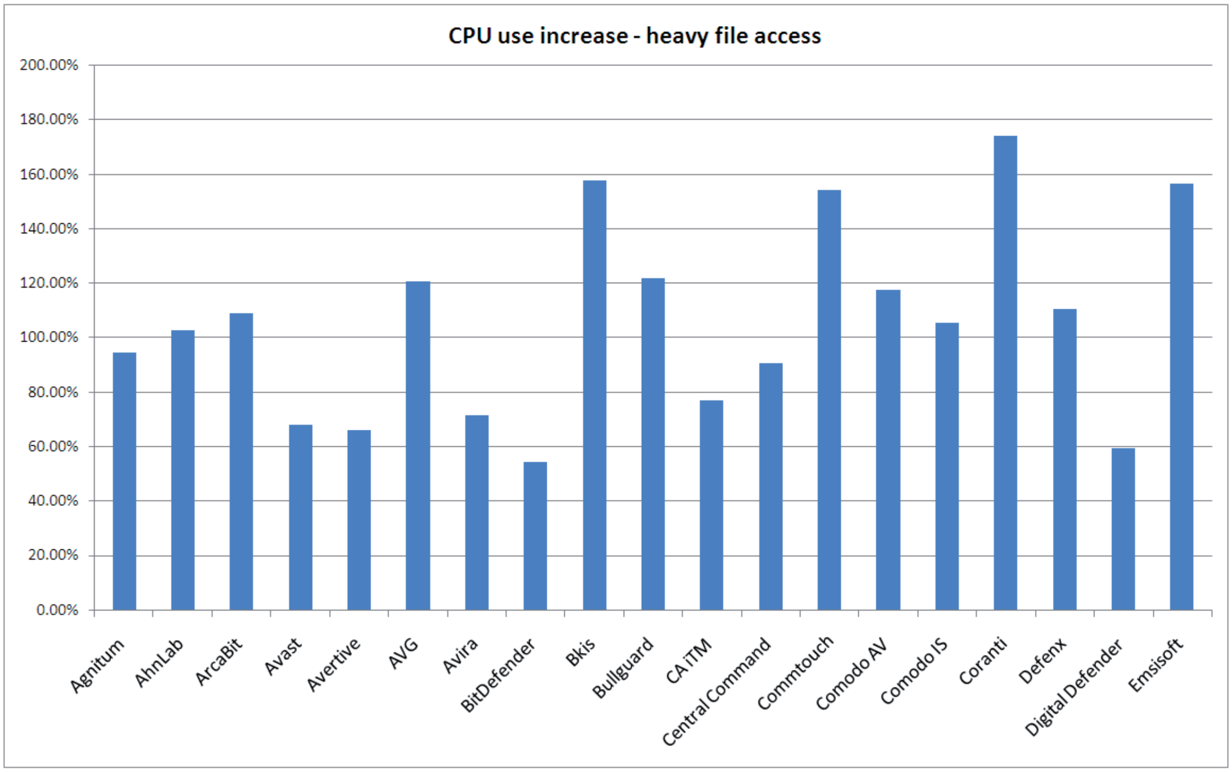
Defenx Security Suite Pro 2011 3387.517.1242

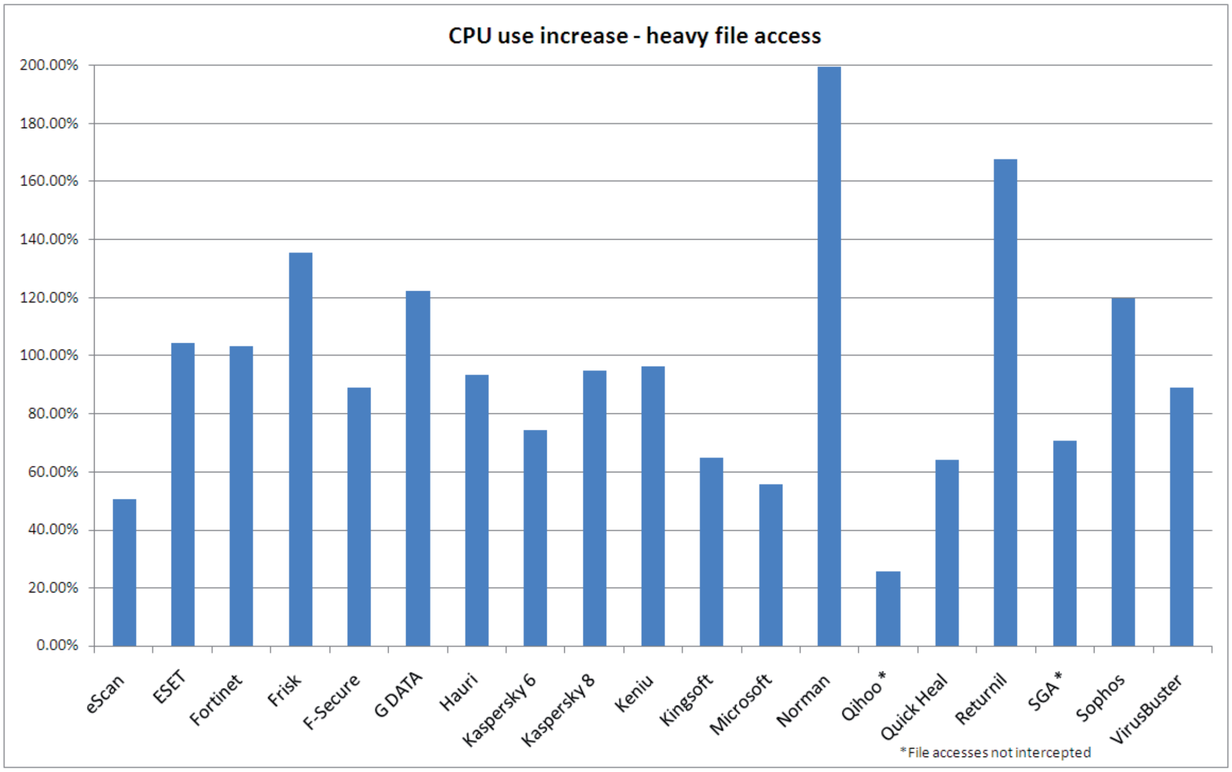
ItW	100.00%	**Polymorphic**	89.49%
ItW (o/a)	100.00%	**Trojans**	64.37%
Worms & bots	87.18%	**False positives**	0

The *Defenx* solution has become a regular VB100 entrant in recent months, and has already established a solid record of good performances. The installation process requires little interaction but takes longer than many, mainly thanks to the need for some extra C++ components and some setting up of trusted packages already installed in the local system. Like its progenitor *Agnitum*, the interface has been somewhat refreshed lately, and looks glossy and slick without losing its air of seriousness. Minimal space is given to the anti-malware component amongst the other modules, but there are still ample controls for most standard desktop requirements, and testing proceeded at a good pace.



Scanning speeds showed some signs of judicious use of smart caching, although resource usage remained fairly high. Detection rates were solid, as in several other implementations of the same engine this month, with none of the flakiness or issues in the WildList set seen elsewhere.



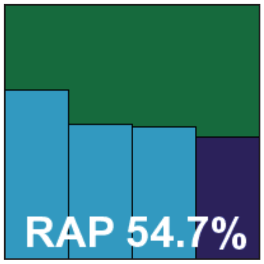


Please refer to text for full product names.

The clean set was once again enlivened only by a single suspicious alert on a *Themida*-packed file, and *Defenx* comfortably earns another VB100 award.

Digital Defender Server Antivirus 2.1.8

ItW	100.00%	**Polymorphic**	89.49%
ItW (o/a)	96.61%	**Trojans**	62.32%
Worms & bots	79.64%	**False positives**	0

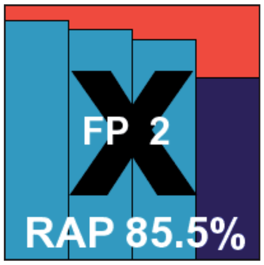


Digital Defender has the same straightforward installation process and simple interface as *Avertive*'s solution, differing only in colour scheme. Performance measures were also at the higher end of the mid-range, and scanning speeds similarly languorous in the infected sets. Logging was again somewhat traumatic, with detection data summarily thrown away after a fairly limited amount of disk space had been used up – surely no computer still running would find 20MB too much to dedicate to vital information on potential infections, and server admins would almost certainly find the lack of traceability a problem.

At the end of a lengthy testing period detection rates proved fairly reasonable, with just a single *Themida*-packed file alerted on in the clean sets, and in the WildList the same batch of items were again mysteriously missed on access, with no problems on demand. This was enough to deny *Digital Defender* a VB100 award this month, despite a fairly solid performance compared to some of the competition.

Emsisoft Anti-Malware 5.0.0.68

ItW	100.00%	**Polymorphic**	79.84%
ItW (o/a)	100.00%	**Trojans**	91.74%
Worms & bots	97.96%	**False positives**	2

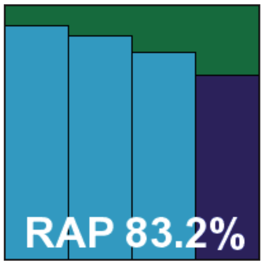


Since dropping the 'a-squared' name, *Emsisoft*'s solution has come on in leaps and bounds, leaving behind the stability issues of early appearances and living up to the excellent detection levels of *Ikarus*, provider of the scanning engine at the core of the product. The install is fast and easy, and the interface clean and clear, with a fair level of configuration for what is mainly a home-user product. One thing which was missing from our point of view was the option to simply prevent access to infected items without either prompting for user input or automatically trying to clean up, but this would be a minor issue for most users.

RAM usage was fairly low, but CPU drain fairly high, while scanning speeds were slowish and on-access overheads fairly high. Despite being slowed down by the need to quarantine every item spotted on access, there were no stability problems when running through the demanding infected sets, and in the end detection scores were as superb as we have come to expect, with excellent figures in all sets. In the clean sets, a pair of false positives emerged: one in some fairly obscure business software and the other in a utility from hardware manufacturer *Belkin*. This was enough to deny *Emsisoft* a VB100 award this month despite an otherwise very strong performance.

eScan Internet Security for Windows 11.0.1139.793

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	94.52%
Worms & bots	98.54%	**False positives**	0



We've been quite enjoying working with *eScan*'s latest version in recent tests. It installs quickly and simply, but does need a reboot, and the interface is colourful and fun-packed, with its shimmery *Mac*-style icon tray and windows that close with a swirling flourish. Under the stylish surface it continues to provide a wealth of fine-tuning controls, presented in a much more sober fashion, making it simple for the more demanding user to find the most detailed options. On-demand scanning times were initially on the slow side, particularly in our set of media files, but were considerably faster on repeat visits, while on-access overheads were fairly low to begin with and again improved later thanks to some smart caching of results. Both memory and processor usage were also fairly low, making for a very good set of performance results all round.

Detection results were also highly impressive across the board, with no problems in the core certification sets, and *eScan* comfortably earns another VB100 award for its splendid performance.

Archive scanning		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
Agnitum Outpost	Default	2	√	√	√	√	√	√	√	√	√	√
	All	X	X	X	X	X	X	X	X	X	X	√
AhnLab V3Net	Default	9	9	9	9	9	9	9	X	9	X	√
	All	X	X	X	X	X	X	X	X	X	X	√
ArcaBit ArcaVir	Default	2	√	√	√	√	√	√	√	√	1	√
	All	X	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/1	√
Avast Software avast!	Default	X/√	X/√	√	√	X/√	X/√	X/√	X/√	X/√	X/√	X/√
	All	X/√	X/√	√	√	X/√	X/√	X/√	X/√	X/√	X/√	√
Avertive VirusTect	Default	1	1	X	X	1	X	1	X	1	1	√
	All	1	1	X	X	X	X	X	X	1	X	X
AVG Internet Security	Default	√	√	√	√	√	√	√	√	√	√	X/√
	All	X	X	X	X	X	X	X	X	X	X	X/√
Avira AntiVir	Default	√	√	√	√	√	√	√	√	√	√	√
	All	X	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
BitDefender Security	Default	√	√	8	8	√	√	√	8	√	√	√
	All	X/√	X/√	X/√	X/√	8/√	X/√	X/√	X/√	1/√	1/√	√
Bkis BKAV	Default	X	X	X	X	X	X	X	X	X	X	√
	All	X	X	X	X	X	X	X	X	X	X	√
Bullguard Antivirus	Default	√	√	8	8	√	√	√	8	√	√	√
	All	√	√	8	8	√	√	√	8	√	√	√
CA Threat Manager	Default	X	√	X	X	√	√	√	√	√	X	√
	All	X	X	X	X	1	X	X	X	1	X	√
Central Command Vexira	Default	2	√	√	√	X/√	X	√	√	√	X/√	X/√
	All	X	X	X	X	X	X	X	X	X	X	X/√
Commtouch Command	Default	5	5	5	5	5	√	5	5	5	5	√
	All	X	X	X/4	X/4	X/4	X	X	X	X	X	X
Comodo AntiVirus	Default	X	5	5	5	5	5	5	2	5	X	√
	All	X	X	X	X	X	X	X	X	X	X	√
Comodo Internet Security	Default	X	5	5	5	5	5	5	2	5	X	√
	All	X	X	X	X	X	X	X	X	X	X	√
Coranti 2010	Default	√	√	8	8	√	√	√	8	√	√	√
	All	X	X	X	X	√	X	X	X	1	X/1	X/√
Defenx Security Suite Pro	Default	2	√	√	√	√	X	√	√	√	X	√
	All	X	X	X	X	X	X	X	X	X	X	√
Digital Defender AntiVirus	Default	1	1	X	X	1	X	1	X	1	1	√
	All	1	1	X	X	1	X	1	X	1	1	X
Emsisoft Anti-Malware	Default	2	2	2	2	2	2	2	3	2	2	√
	All	2	2	2	2	2	2	2	3	2	2	√

Please refer to text for full product names.

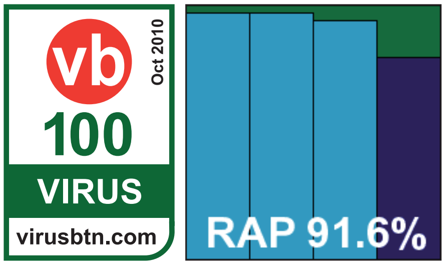
Archive scanning contd.		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
eScan Internet Security	Default	9	5	4	3	5	5	5	4	5	8	√
	All	X/√	X/√	X	X/1	X/√	X	X/√	X/√	X/√	X/√	√
ESET NOD32	Default	√	√	√	√	√	√	√	5	√	√	√
	All	X	X	X	X	X	X	X	X	X	X	√
Fortinet FortiClient	Default	X	√	√	√	√	√	√	√	4	1	√
	All	X	√	√	√	√	√	√	√	4	1	√
Frisk F-PROT	Default	√	√	√	√	√	√	√	√	√	√	√
	All	X	X	X	2	2	X	X	X	2	2	√
F-Secure PSB Server Security	Default	√	√	√	√	√	√	√	8	√	√	√
	All	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/8	X/√	X/√	X/√
G DATA AntiVirus	Default	√	√	√	√	√	√	√	√	√	√	√
	All	√	√	3	4	√	√	√	8	√	√	√
Hauri ViRobot	Default	X	1	1	1	√	1	X	X	X	1	√
	All	X	X	X	X	X	X	X	X	X	X	X/√
Kaspersky Anti-Virus 6	Default	√	√	√	√	√	√	√	√	√	√	√
	All	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
Kaspersky Anti-Virus 8	Default	√	√	√	√	√	√	√	√	√	√	√
	All	X/√	X/√	√	√	X/√	X/√	X/√	X/√	X/√	X/√	√
Keniu Antivirus	Default	√	√	X	X	√	√	√	√	√	√	√
	All	X	X	1	1	X	X	X	X	X	X	√
Kingsoft Internet Security	Default	X	√	√	X	√	√	√	√	√	1	√
	All	X	X	X	X	X	X	X	X	X	X	√
Microsoft Forefront Client Security	Default	√	√	√	√	2	2	2	√	√	√	√
	All	X	X	X	1	X	X	X	X	1	X	√
Norman Endpoint Protection	Default	X	√	√	1	√	√	√	√	√	1	√
	All	X	X	X	X	X	X	X	X	X	X	√
Qihoo 360 Antivirus	Default	X/√	X/√	X/8	X/8	X/√	X/√	X/√	X/8	X/√	X/√	√
	All	X	X	X	X	X	X	X	X	X	X	X/√
Quick Heal Anti-Virus 2011	Default	X/2	X/5	X	X	2/5	X	2/5	X/1	2/5	X	X/√
	All	2	X	X	X	1	X	X	X	1	X	√
Returnil System Safe 2011	Default	5	5	4	4	5	√	5	2	5	5	√
	All	X	X	X	X	X	X	X	X	X	X	√
SGA SGA-VC	Default	√	√	8	8	√	√	√	8	√	√	√
	All	X	X	8	8	X	X	X	X	X	X	X
Sophos Endpoint Security and Control	Default	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/√
	All	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/√
VirusBuster for Windows Servers	Default	1	1	X	X	1	X	1	X	1	1	√
	All	1	1	X	X	1	X	1	X	1	1	X

Please refer to text for full product names.

ESET NOD32 Antivirus 4 Business Edition 4.2.64.12

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	94.84%
Worms & bots	98.52%	**False positives**	0

Eset's renowned *NOD32* has stuck to the same slick and efficient design for a while now, installing simply, needing no reboot and presenting an interface which combines glossy good looks with easy access to a comprehensive range of controls. The one area which seemed awkward, and indeed we found ourselves unable to persuade to function, was the configuration of archive scanning on access – perhaps something of a specialist requirement, but much more likely to be required in a server environment than any other.

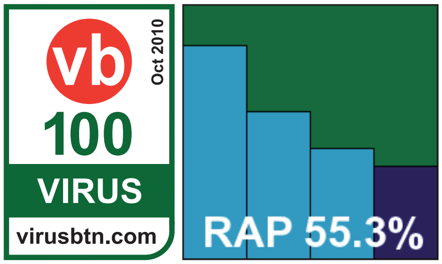


Tests proceeded rapidly, with some decent scanning speeds, overheads and CPU use, and very low memory consumption. Our main scan of infected sets was delayed somewhat thanks to the GUI sticking at 99% for some time, until we realized the scanning was complete but had failed to report this to the world. Harvesting results from the clear and reliable logging system showed the usual stratospheric scores across the board; a couple of adware items spotted in the clean sets do nothing to dent a sterling performance, easily earning *ESET* yet another VB100 award for its record collection.

Fortinet FortiClient 4.1.3143

ItW	100.00%	**Polymorphic**	99.15%
ItW (o/a)	100.00%	**Trojans**	86.13%
Worms & bots	95.85%	**False positives**	0

The *Fortinet* product is more business-focused than most, but nowadays includes a free option, presumably for home users. The set-up process is simple enough for any user type, and needs no reboot. The interface is serious and businesslike, but not intimidatingly so, and provides a decent level of controls in a sensible and unflashy manner. Speed tests ran through without problems, showing scanning speeds towards the lower end, slightly above average overheads, and fairly high memory usage.



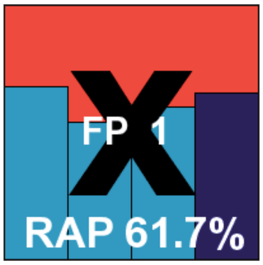
The detection tests have been somewhat more problematic for *Fortinet* for several months now, with many files seeming to snag the engine; this time many attempts at running over our large sets simply stopped scanning, either silently or with an unhelpful message reading 'interrupted'. After much careful coaxing, we managed to get a full set of results for the standard sets, but the RAP sets seemed altogether too much for it, and in the end we had to resort to gathering figures for on-access checking of the RAP sets. These may be somewhat lower than on-demand scores would have been, had it been possible to complete any scans.

The results we eventually obtained were pretty decent, at least for older items, with scores in the later RAP weeks declining to the lowish numbers we used to see from *Fortinet* before some drastic improvements in the past year. With the WildList covered and no false alarms in the clean sets, *Fortinet* scrapes through to achieve a VB100 award, despite some clear problems.

Frisk F-PROT Antivirus for Windows 6.0.9.4

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	64.18%
Worms & bots	85.44%	**False positives**	1

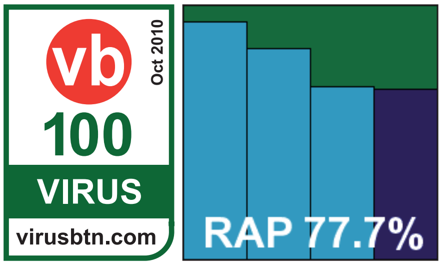
F-PROT has to be one of the most stable solutions to regularly take part in our tests – at least in terms of interface design, which seems to have remained unchanged for several years now. The set-up is simple but does require a reboot, and the GUI is plain and stark, with a bare minimum of controls available. It seems to operate quite nicely however, and performance times were mostly reasonable, with only CPU use noticeably above average for this month's field.



Detection tests ran fairly well too, with the usual error messages popping up to warn that the product had stopped working, which seem to have no effect on the actual running of scans or protection levels. Scores were decent, with a surprising upturn in the latter weeks of the RAP sets, and the WildList caused no problems. However, in the clean sets the same version of the *Firefox* installer that caused problems earlier was again misidentified as a trojan, and *Frisk* is thus denied a VB100 award this month. The false alarm was apparently fixed shortly after the product submission date.

F-Secure PSB Server Security 9.00 build 198

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	93.66%
Worms & bots	97.45%	**False positives**	0



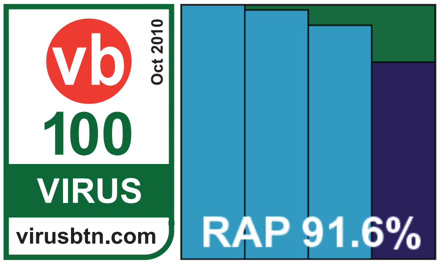
F-Secure's corporate solutions are grouped under the 'Protection Services for Business' title, and this one seems properly businesslike, with a web-based interface providing decent control levels for most requirements. The installation process is efficient – a conflict with some networking drivers was noted and resolved without the need for extra work on our part; a reboot is needed to complete. The GUI is fairly well laid out and responds quite nicely – something of a rarity with such approaches – but it does have a tendency to lose touch with its server side and requires frequent repeat logins.

Running through the tests proved reasonably straightforward. However, as in many recent tests, logging proved highly unreliable, with data on large scans not properly stored and often lost entirely. The problem seems to be caused by keeping results in memory during scanning – something which many solutions seem to do and which often causes problems when more than a handful of detections are recorded in a single scan. Apparently the developers have implemented a fix for this issue, which should be included in the product by now, but for this test (hopefully for the last time), we had to resort to using the command-line scanner included with the product.

This produced some good results, with excellent scores across the board, steadily declining in the RAP sets but starting high and ending up more than respectable in the 'week +1' set. No problems were observed in either the clean or WildList set, and *F-Secure* is judged worthy of a VB100 award this month.

G DATA AntiVirus 10.5.132.28

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	99.29%
Worms & bots	99.59%	**False positives**	0

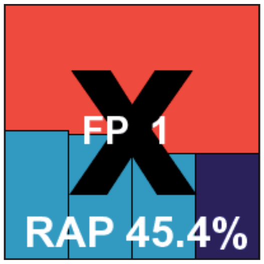


G DATA's server solution includes an administration suite and client-side protection, which is simple to roll out from the admin interface. This management tool installs fairly easily, resolving a dependency on the .NET framework with a copy bundled with the package, and needs no reboot to complete either its own set-up or that of the protection rolled out to the local system. The design is splendidly clear and provides excellent configuration, although to simplify things for ourselves we allowed control to be ceded to the client side and ran most jobs from there.

Scanning speeds were not bad and improved enormously on repeat attempts, and RAM usage was lower than many despite the dual-engine approach; CPU use was a little above average, but not excessive. Detection rates were almost impeccable, with very little missed anywhere. With no false alarms and the superb detection extending to the WildList set, *G DATA* easily earns a VB100 award this month.

Hauri ViRobot Windows Server 3.5

ItW	85.00%	**Polymorphic**	96.43%
ItW (o/a)	67.68%	**Trojans**	52.23%
Worms & bots	67.93%	**False positives**	1

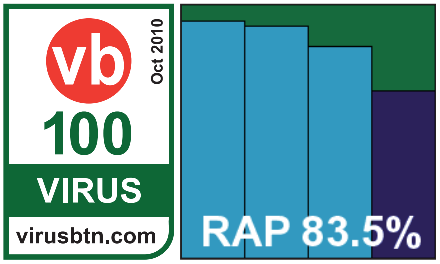


Returning after a lengthy absence from our tests, *Hauri* is another licensee of the popular *BitDefender* engine, with some additional technology and definitions of its own added to the mix. The installer is quite fast and simple, with no reboot needed, and the interface looks complete and businesslike, providing plenty of options in a good logical layout. It seemed to respond well to changes, although logging proved extremely slow to export for our larger jobs. On-demand scans were rather slow, and on-access overheads fairly high, but resource usage was quite light.

Detection rates were something of a surprise, with much lower scores than expected, including a fair number of samples missed in the WildList. We assumed that the submission had been provided without updates, although we do make our requirements as clear as possible when accepting products for test. In any case, in the on-access tests many more misses were evident, including the entire set of W32/Polip polymorphic samples, which are much older than most in the sets. With a handful of false alarms to add to its woes, *Hauri* fails to make the grade for a VB100 this month, although the product shows promise.

Kaspersky Anti-Virus 6 for Windows Servers 6.0.4.1424

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	93.08%
Worms & bots	96.82%	**False positives**	0



Kaspersky's version 6 product has a rather lengthy installation process, with multiple steps, but includes many components and protective layers so perhaps this is no surprise; no reboot is needed to complete. The interface is fairly similar to that of the standard desktop version, being an attractive affair in metallic green, with a wealth of controls and options all within easy reach. It ran through the tests in fine time, with some excellent caching of results making for lightning times in the speed tests and both RAM and CPU slightly above this month's averages.

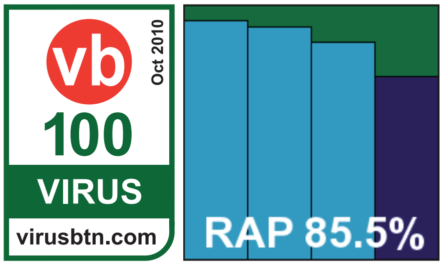
Detection scores were easily obtained, with the logging system reliable, and although somewhat slow to export it showed none of the issues observed in the desktop solutions in the last comparative. Scores were uniformly excellent, dropping off only in the final week of the RAP sets but still achieving a good score in the proactive week. No problems in the core sets means *Kaspersky* earns another VB100 award.

Kaspersky Anti-Virus 8 for Windows Servers Enterprise Edition 8.0.0.495

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	93.43%
Worms & bots	96.94%	**False positives**	0

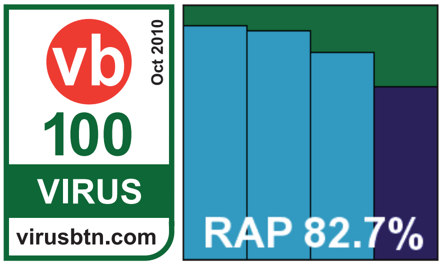
Version 8 from *Kaspersky* has a similarly lengthy installation process, split into numerous steps, and this time the interface uses the MMC system, doing so in a pretty stylish and efficient manner, making good use of colour and providing the full range of controls. Scanning speeds were again superb, with slightly higher resource usage than the version 6 edition.

Detection rates were also slightly higher in most areas, showing some good improvements in heuristics and so on in this latest edition, and scores were thus truly excellent. *Kaspersky* earns a second VB100 award this month, after a pair of splendid showings.



Keniu Antivirus 1.0.0.1062

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	94.23%
Worms & bots	93.95%	**False positives**	0



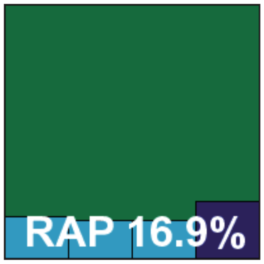
Keniu provides an OEM product based on the *Kaspersky* engine for the Chinese market, which is simple and basic but seems to work reasonably well. The install is fairly straightforward and rapid, but we were requested to update online on the deadline day, and found this took well over an hour to complete – presumably this would be considerably faster closer to home base. The GUI is minimalistic with large buttons and only a few options, but ran through our performance tests nicely, with unremarkable speeds and overheads, high-ish CPU consumption and low RAM usage.

Detection results were something of a pain to obtain, logging being once again somewhat broken – lines appear to be trimmed to an arbitrary length, dropping vital details of which items have been detected in many cases. After much effort, including re-running scans over sets doctored to shorten file paths as much as possible, we managed to obtain some results. These appeared reasonably comprehensive, closely approaching those of *Kaspersky*'s products, but it could well be that some items which were detected were not recognized thanks to the poor quality of the logging. The WildList results were more or less intact however, and showed full coverage, and no false alarms were noted in the clean sets, so *Keniu* just about earns a

VB100 award. Few server admins would find the product ready for production systems though.

Kingsoft Internet Security 2010 2008.11.6.65

ItW	99.99%	**Polymorphic**	58.64%
ItW (o/a)	99.99%	**Trojans**	8.76%
Worms & bots	49.04%	**False positives**	0

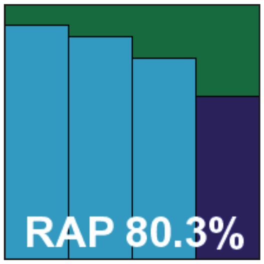


Unlike the last few tests there was just a single entry from *Kingsoft* this month. The standard *IS* version is nice and easy to install and needs no reboot to complete. The interface is not the prettiest, but is useable and provides for most of our needs; scanning speeds were fairly slow, but overheads and resource usage were fairly low.

Detection rates were frankly abysmal, with the trojans set handled particularly poorly and some astoundingly low scores in the RAP sets – implying that perhaps some vital component of the detection signatures had been missed out of the build submitted (a problem we have seen before). No problems were spotted in the clean sets, but in the WildList set a number of Virut samples went undetected, and *Kingsoft* is some way from the standard required to earn a VB100 award this month.

Microsoft Forefront Client Security 1.5.1981.0

ItW	100.00%	**Polymorphic**	99.74%
ItW (o/a)	100.00%	**Trojans**	88.70%
Worms & bots	97.01%	**False positives**	0

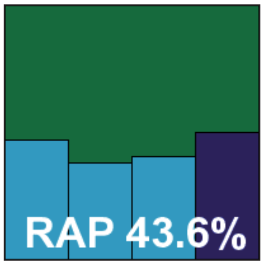


Microsoft's business product was provided as a special offline set-up, requiring three reboots to get everything in place – presumably this is not the case for regular users running proper management tools. The interface is slick but a little confusing in places, with a lot of verbiage which does not always make clear the purpose of the accompanying checkbox. Logging is also a little on the wordy side, but was rendered usable thanks to some insight from the developers.

Running through the tests proved fairly problem free, with neither scanning speeds nor lag times particularly good but very low resource consumption. Scanning the infected sets took an enormously long time – among the longest of all this month's products. The product is clearly recording massive amounts of data on each item spotted, and seems to keep it all in memory, only producing a log at the end of the scan – this made for a rather tense few days for us as we waited for it to complete. In the end, though, scores were very solid, with a steady decline across the RAP sets but starting from a very strong baseline, and with no issues in the core sets a VB100 award is comfortably earned.

Norman Endpoint Protection 7.20.0900

ItW	100.00%	**Polymorphic**	83.78%
ItW (o/a)	100.00%	**Trojans**	69.14%
Worms & bots	76.58%	**False positives**	0

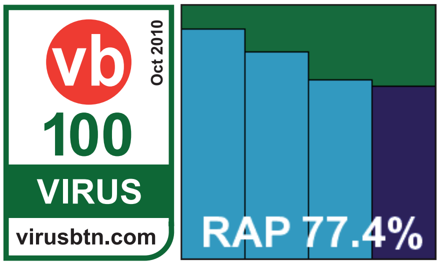


Norman's current product has been having some problems of late, with a run of bad luck in our tests. The installation process is fairly drawn out, with a fair few steps to click through, and at the end it warns that a reboot may be requested in a few minutes. Although no such request appeared, we felt it best to restart the system just in case. Opening the browser-based interface (which required some adjustments to the built-in browser security settings in *Server 2003*), we found it, as before, rather wobbly and lacking in reassurance, with anti-malware components missing on the initial few attempts. When they finally appeared, we found a basic level of controls which seemed to operate reasonably well, although our instructions not to delete any infected items seemed to go unheeded. We also noted the GUI apparently losing touch with its local server on several occasions, displaying instead a pretty picture of a crash test dummy doodling on a chalk board while we waited for service to be resumed.

Results were obtained without undue difficulty though, showing slow scanning times, and overheads and resource usage sky-high, mainly thanks to the in-depth investigations of the built-in sandbox system. Detection results were no more than reasonable in the main sets, deteriorating somewhat in the infected sets, with an odd rally in the proactive week. The WildList presented no problems though, despite the large number of polymorphic viruses in there, and with no repeat of previous issues in the clean sets, *Norman*'s run of bad luck comes to an end and a VB100 award is earned.

Qihoo 360 Antivirus 1.1.0.1312

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	93.20%
Worms & bots	98.03%	**False positives**	0

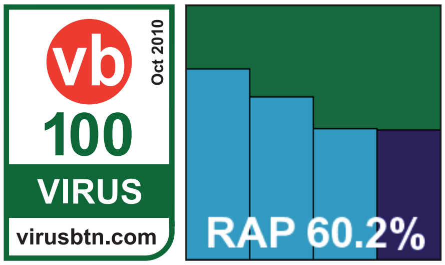


Another Chinese company, *Qihoo* licenses the *BitDefender* engine and squeezes it into a much simplified set-up. The installation process is short and sweet, and needs no reboot, and the interface offers large, clear buttons and minimal configuration options. Scanning speeds were mediocre, but overheads and resource usage very low indeed.

Detection tests proceeded without incident, although the on-access component did not seem to function as usual on-read, failing to block access to infected items when simply opened for reading (although its logs and pop-ups claim to have done so). It does at least note their presence however, providing nice, clear, reliable logging, and in final calculations scores were as high as expected – a very respectable showing in all sets. With no problems in the WildList or clean sets, *Qihoo* easily earns a VB100 award.

Quick Heal AntiVirus 2011 Server Edition 11.00 (4.0.0.4)

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	79.14%
Worms & bots	91.44%	**False positives**	0

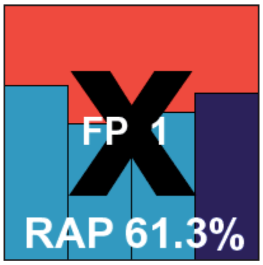


Quick Heal's products run a brief scan of vital areas prior to installation, but even with this the whole set-up process was over in under a minute, with no reboot and minimal user interaction. The interface is clean, simple and unfussy, providing a decent but not exhaustive level of configuration. Running was generally smooth and stable, although it seemed to do something odd to our performance measuring scripts, which frequently aborted with bizarre error messages and had to be run multiple times to obtain a complete set of results – and even then, it is possible that the recorded RAM usage (high-ish) and CPU drain (low-ish) are not entirely accurate.

Detection scores presented no such problems however, and they showed some fairly respectable levels across the main sets, dropping fairly sharply in the RAP sets. No issues were noted in the core sets, and a VB100 award is duly granted.

Returnil System Safe 2011 3.2.10143.501-REL2

ItW	98.71%	**Polymorphic**	100.00%
ItW (o/a)	98.71%	**Trojans**	65.27%
Worms & bots	85.84%	**False positives**	1

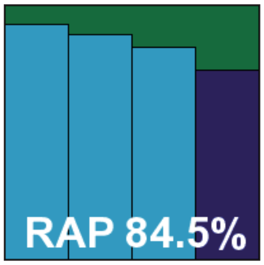


Returnil's product has been renamed since its last VB100 appearance, adopting the more universal '*System Safe*' title in place of the old 'Virtual System'. Installing is fairly simple and, rather surprisingly for a multi-level solution like this, no reboot is required. The interface is pleasant and clear, providing only minimal controls for the anti-virus protection module, which is based on the *Frisk* detection engine.

Running through the tests was a breeze, although scan times were slow and overheads high, with file access lags and CPU use both well above average for this month's field. Detection rates were decent though – in some areas a fraction higher than those of other products based on the same technology, implying some more aggressive settings. However, in the WildList a handful of items were not detected, hinting that perhaps slightly older updates had been used. In the clean sets the same false alarm we had been fearing reared its head once again, and *Returnil* doesn't quite make it to a second VB100 award this time.

SGA SGA-VC 2.0

ItW	99.03%	**Polymorphic**	100.00%
ItW (o/a)	N/A	**Trojans**	94.66%
Worms & bots	98.61%	**False positives**	0



SGA returns to the tests once more, with its product offering an extremely fast installation process which is all over in under 30 seconds and needs no reboot. The interface is a little unusual, not providing much in the way of fine-tuning, and what is available is quite hard to find. Scanning speeds were on the slow side, and performance measures reflect better on the product than others thanks to the rather odd approach to on-access scanning, which doesn't seem to actually intercept file access so much as note that an infected item has been opened and then, often some time later, take action.

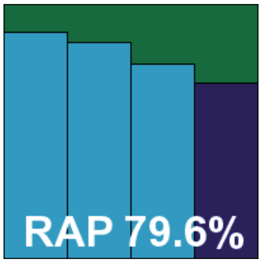
Detection rates in the on-demand scans were mostly quite impressive thanks to the *BitDefender* engine underlying the product, but a handful of items in the WildList sets were not picked up on due to the default extension list excluding some extensions commonly used by malware to propagate.

Running the on-access tests was rather more difficult, as the scanner's lack of blocking meant relying on the product's internal logs – which seemed rather hard to believe – and the actions taken when files were written to the system drive. Trying to piece together information on what was allowed to write and what was logged, over multiple installs and test runs, proved bewildering and inconclusive, with some of the data implying that the scanner regularly shut itself down when under heavy pressure. As a result, we recorded no on-access scores for *SGA* this month, and no VB100 award can be granted.

Sophos Endpoint Security and Control 9.5

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	88.35%
Worms & bots	90.47%	**False positives**	0

vb 100 VIRUS virusbtn.com Oct 2010



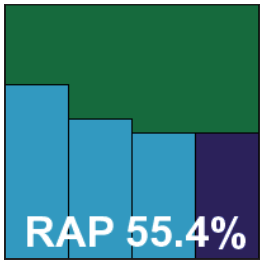
Sophos's latest business product is as businesslike as we have come to expect, with an efficient and zippy set-up which includes the fairly unusual offer to remove competitor products from the system. No reboot is needed to complete the set-up, but after some problems in the last test we restarted anyway, after disabling the new cloud-based protection layer, which is not covered by our testing methodology. The speed and performance tests ran through fine, with fairly fast scanning times and overheads and performance use somewhat above average.

The detection tests took much longer however, with each detection taking some time despite the live system being switched off. In the end, with time pressing urgently, we decided to abandon the GUI scan and re-run from the command line, using a tool provided with the product. This may have produced slightly lower scores than the product is capable of, even without its live system, but they were still very good indeed in the main sets, and pretty decent in the RAP sets too. No issues were observed in the core sets, and *Sophos* earns another VB100 award.

VirusBuster for Windows Servers 6.3.14

ItW	100.00%	**Polymorphic**	89.49%
ItW (o/a)	100.00%	**Trojans**	64.89%
Worms & bots	87.51%	**False positives**	0

vb 100 VIRUS virusbtn.com Oct 2010



Last up this month, *VirusBuster*'s product has already appeared in this report in another guise, and here the experience was pretty similar.

The set-up, though going through several stages, is untaxing and fairly speedy, no reboot being needed to complete, and the MMC-based interface is clunky and lacking in consistency, with some controls not fully functional. The biggest problem was once again logging, with the 'unlimited' option less than honest about its true nature, and scans had to be repeated to replace lost sections of information. Server admins would be less likely to run into these problems, unless dealing with a serious infestation on their network.

Scanning speeds were fairly good, but overheads a little heavy, while resource usage was unremarkable. Detection tests ran slowly but produced decent results once complete logs had been obtained, with a reasonable showing across the sets. No problems appeared in the WildList or clean sets, and *VirusBuster* also earns a VB100 award this month.

CONCLUSIONS

We had everything set up for this month's test good and early, with the aim of speeding testing along in what we knew would be a shorter than usual month, with the annual *VB* conference approaching fast. However, a combination of a pre-planned holiday and illness in the lab team left the lab unattended for a full week just as testing got underway, and some serious scrambling was required to get through testing in time. This hectic period was not helped by some further manifestations of instability, lack of resilience to tough challenges and general flakiness in a number of products, but in the end we got all the results needed for our report. We have done our utmost to ensure full coverage of our standard array of tests and measurements, and hope that our readers will forgive any minor errors or oversights contained in this report – as soon as we have time, we will of course ensure every 'i' is dotted, every 't' is crossed, and every surprising result is confirmed and double-checked.

It should also be noted that several other products were submitted for this month's test, all of them taking at least a few days of machine time and several installs before it was decided that no results could be obtained due to severe instability or failure to complete any scanning tasks. We saw many more incidents of scans failing to complete, logs being incompletely recorded, and even whole machine failures this month than in any previous test, making for more hair-tearing and nail-biting than ever before. In future we will be much quicker to reject any product which cannot be relied on to run smoothly, and may have to include blank scores for products which fail to record their activities accurately.

Of course it has not all been doom and gloom this month, with many products performing well, and some interesting newcomers joining our lists. Looking forward to the next test, on *Windows 7*, we expect to see another record-breaking haul of submissions, with many more new faces on the horizon. We can only hope those which have given us so much grief this month can up their game, put in the work required on proper development and QA procedures, and start delivering decent, reliable products in time.

Technical details:

All products were tested on identical systems with *AMD Phenom II X2 550* processors, 4 GB RAM, dual 80GB and 1TB hard drives, running *Microsoft Server 2003, R2, SP2, 32-bit Enterprise Edition.*

Any developers interested in submitting products for VB's comparative reviews should contact john.hawes@virusbtn.com. The current schedule for the publication of VB comparative reviews can be found at http://www.virusbtn.com/vb100/about/schedule.xml.