

VBSPAM COMPARATIVE REVIEW SEPTEMBER 2016

Martijn Grooten & Ionuț Răileanu

Spam isn't that much of a problem these days – which may sound like an unusual statement coming from an organization that started testing spam filters precisely because it *was* such a problem. Yet it is no secret that there are many products that help to mitigate the spam problem; the VBSpam tests have been testament to that.

However, 'not much of a problem' isn't the same as *no* problem. The problems that remain with email exist mostly in the margins: phishing emails and, especially, emails with malicious attachments. These get blocked in the vast majority of cases, but are those block rates good enough? After all, it takes just one malicious attachment to be opened by the user to get infected with ransomware¹.

In these tests we have always focused on spam as a problem of volume – and this should remain an important focus for any product in the email security market: it's still not reasonable to expect anyone to use email without their inbox being protected by a spam filter, it probably never will be.

However, we now plan also to focus on the explicitly malicious aspect of spam. In this test report, we will give a sneak preview of how we will be doing this; in future test reports, we will report on the ability of email security products to block malicious attachments.

A total of 17 full email security (or anti-spam) solutions took part in this test, all of which achieved VBSpam certification. Seven of them performed well enough to earn the VBSpam+ accolade. We also tested five DNS-based blocklists.

¹ Which is why we, like most security experts, recommend running an endpoint security product next to an email security product.

THE TEST SET-UP

The VBSpam test methodology can be found at <https://www.virusbulletin.com/testing/vbspam/vbspam-methodology/>. As usual, emails were sent to the products in parallel and in real time, and products were given the option to block email pre-DATA (that is, based on the SMTP envelope and before the actual email was sent). However, on this occasion no products chose to make use of this option.

For those products running on our equipment, we use *Dell PowerEdge* machines. As different products have different hardware requirements – not to mention those running on their own hardware, or those running in the cloud – there is little point comparing the memory, processing power or hardware the products were provided with; we followed the developers' requirements and note that the amount of email we receive is representative of that received by a small organization.

To compare the products, we calculate a 'final score', which is defined as the spam catch (SC) rate minus five times the weighted false positive (WFP) rate. The WFP rate is defined as the false positive rate of the ham and newsletter corpora taken together, with emails from the latter corpus having a weight of 0.2:

$$\text{WFP rate} = (\# \text{false positives} + 0.2 * \min(\# \text{newsletter false positives}, 0.2 * \# \text{newsletters})) / (\# \text{ham} + 0.2 * \# \text{newsletters})$$

$$\text{Final score} = \text{SC} - (5 * \text{WFP})$$

In addition, for each product, we measure how long it takes to deliver emails from the ham corpus (excluding false positives) and, after ordering these emails by this time, we colour-code the emails at the 10th, 50th, 95th and 98th percentiles:

- (green) = up to 30 seconds
- (yellow) = 30 seconds to two minutes
- (orange) = two to ten minutes
- (red) = more than ten minutes

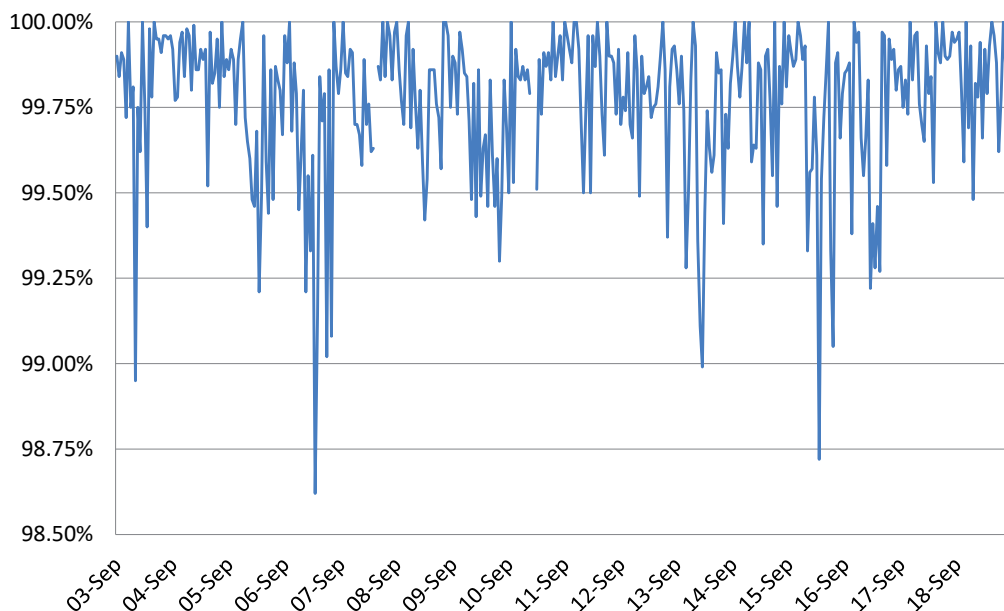


Figure 1: Spam catch rate of all full solutions throughout the test period.

Products earn VBSpam certification if the value of the final score is at least 98 and the ‘delivery speed colours’ at 10 and 50 per cent are green or yellow and that at 95 per cent is green, yellow or orange.

Meanwhile, products that combine a spam catch rate of 99.5% or higher with a lack of false positives, no more than 2.5% false positives among the newsletters and ‘delivery speed colours’ of green at 10 and 50 per cent and green or yellow at 95 and 98 per cent earn a VBSpam+ award.

THE EMAIL CORPUS

The test ran for 16 days, from 12am on 3 September to 12am on 19 September 2016.

The test corpus consisted of 81,796 emails. 73,710 of these were spam, 64,384 of which were provided by *Project Honey Pot*, with the remaining 9,326 spam emails provided by *spamfeed.me*, a product from *Abusix*. They were all relayed in real time, as were the 7,772 legitimate emails (‘ham’) and 314 newsletters.

Figure 1 shows the catch rate of all full solutions throughout the test. To avoid the average being skewed by poorly performing products, the highest and lowest catch rates have been excluded for each hour.

Compared to the last test, which ran in July, the average spam catch rate dropped by a probably insignificant 0.02%, the most important point of note of which is that

catch rates remain lower than they were in the first months of the year.

The most difficult to filter spam emails were, unsurprisingly, those that came from what are likely to be legitimate companies making promises that seem only a little bit too good to be true, and are probably a nuisance at worst. Still, none of these messages were missed by every participating product, which demonstrates that there was something in each of them that could be used to block them.

There were more false positives than in the last test, though this was caused mainly by two outlying products.

EMAILS WITH MALICIOUS ATTACHMENTS

Among the emails in our spam feed, 2,076, or a little under three per cent, contained a malicious attachment².

Spam has long been a delivery mechanism for malware. Initially, malicious executables were attached directly to the emails, which made them relatively easy to block. These days, however, the attachments are more often than not malware downloaders that come in a variety of formats, from JavaScript files to *Office* documents containing macros, the latter being a file format few organizations can afford to block.

The particular malware that ends up being downloaded often isn’t determined by the downloader alone, and the

² Spam is notoriously volatile. This ratio of malicious spam could be many times higher during different periods, or for other recipients.

same downloader could lead to different kinds of malware (and sometimes no malware at all) being downloaded. Still, most of the downloaders we saw were those commonly associated with ransomware, in particular Locky, once again confirming that this is the most important threat at the moment.

Thankfully, most of the emails were blocked by the spam filters in our tests. However, the block rates for messages containing malware were lower than for the overall spam corpus: while five full solutions blocked all 2,076 emails, four others missed significantly more than one per cent of the emails. For a small organization, this would have meant a few dozen malicious emails making it to users' inboxes. There is certainly room for improvement here.

Interestingly, while ransomware downloaders were among the malicious emails that some products missed, the most difficult to filter email contained the Adwind RAT³, a relatively rarely seen remote access trojan, written in Java. This emphasizes the obvious point that malware is harder to block when it is seen less often.

Note: Vendors have not received feedback on malicious spam in particular; and thus have not been able to contest our claims. We therefore do not feel it would be fair to report on the performance of individual products against malicious spam on this occasion. Moreover, some developers may want to adjust their products' settings as malicious spam becomes more of a focus in these tests.

RESULTS

Two products, *OnlyMyEmail* and *ESET*, stood out for missing just two and four emails from the spam corpus respectively. Neither product blocked any legitimate emails, earning them each VBSpam+ awards. VBSpam+ awards were also earned by *Bitdefender*, *Fortinet*, *IBM*, *Libra Esva* and *Trustwave*. 'Clean sheets' – in which no legitimate emails were blocked either in the ham corpus or in the newsletter feed – were achieved by *OnlyMyEmail* and *Libra Esva*.

Axway MailGate 5.5.1

SC rate: 99.62%
FP rate: 0.05%
Final score: 99.26
Project Honey Pot SC rate: 99.57%
Abusix SC rate: 99.94%
Newsletters FP rate: 2.5%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



³ <https://virustotal.com/en/file/504da9f2866c1b78c71237a4e-190354340c0801fb34a790baa4b00dedcd46475/analysis/>

Bitdefender Security for Mail Servers 3.1.2

SC rate: 99.86%
FP rate: 0.00%
Final score: 99.85
Project Honey Pot SC rate: 99.84%
Abusix SC rate: 99.98%
Newsletters FP rate: 0.3%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



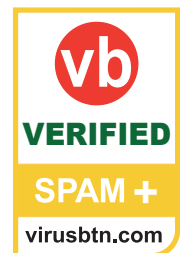
Egedian Mail Security

SC rate: 99.19%
FP rate: 0.00%
Final score: 99.17
Project Honey Pot SC rate: 99.07%
Abusix SC rate: 99.98%
Newsletters FP rate: 0.3%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



ESET Mail Security for Microsoft Exchange Server

SC rate: 99.99%
FP rate: 0.00%
Final score: 99.98
Project Honey Pot SC rate: 99.995%
Abusix SC rate: 99.989%
Newsletters FP rate: 0.3%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Fortinet FortiMail

SC rate: 99.97%
FP rate: 0.00%
Final score: 99.94
Project Honey Pot SC rate: 99.97%
Abusix SC rate: 99.99%
Newsletters FP rate: 0.6%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



GFI MailEssentials

SC rate: 99.55%
 FP rate: 0.48%
 Final score: 97.04
 Project Honey Pot SC rate: 99.52%
 Abusix SC rate: 99.73%
 Newsletters FP rate: 3.8%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Libra Esva 3.7.0.0

SC rate: 99.96%
 FP rate: 0.00%
 Final score: 99.96
 Project Honey Pot SC rate: 99.96%
 Abusix SC rate: 99.99%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



IBM Lotus Protector for Mail Security

SC rate: 99.97%
 FP rate: 0.00%
 Final score: 99.95
 Project Honey Pot SC rate: 99.97%
 Abusix SC rate: 99.98%
 Newsletters FP rate: 0.6%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



OnlyMyEmail's Corporate MX-Defender

SC rate: 99.997%
 FP rate: 0.00%
 Final score: 99.997
 Project Honey Pot SC rate: 99.997%
 Abusix SC rate: 100.00%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Kaspersky Linux Mail Security 8.0

SC rate: 99.70%
 FP rate: 0.01%
 Final score: 99.64
 Project Honey Pot SC rate: 99.68%
 Abusix SC rate: 99.85%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Scrollout F1

SC rate: 99.90%
 FP rate: 0.26%
 Final score: 98.44
 Project Honey Pot SC rate: 99.88%
 Abusix SC rate: 99.99%
 Newsletters FP rate: 4.5%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Kaspersky Secure Mail Gateway

SC rate: 99.62%
 FP rate: 0.01%
 Final score: 99.56
 Project Honey Pot SC rate: 99.59%
 Abusix SC rate: 99.81%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Sophos Email Appliance

SC rate: 99.51%
 FP rate: 0.10%
 Final score: 99.00
 Project Honey Pot SC rate: 99.46%
 Abusix SC rate: 99.85%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



SpamTitan 6.00**SC rate:** 98.59%**FP rate:** 0.00%**Final score:** 98.57**Project Honey Pot SC rate:** 98.47%**Abusix SC rate:** 99.45%**Newsletters FP rate:** 0.6%**Speed:** 10%: ●; 50%: ●; 95%: ●; 98%: ●**Trustwave Secure Email Gateway****SC rate:** 99.88%**FP rate:** 0.00%**Final score:** 99.79**Project Honey Pot SC rate:** 99.86%**Abusix SC rate:** 99.99%**Newsletters FP rate:** 2.2%**Speed:** 10%: ●; 50%: ●; 95%: ●; 98%: ●**Vade Retro MailCube****SC rate:** 99.17%**FP rate:** 0.00%**Final score:** 99.14**Project Honey Pot SC rate:** 99.05%**Abusix SC rate:** 99.99%**Newsletters FP rate:** 0.6%**Speed:** 10%: ●; 50%: ●; 95%: ●; 98%: ●**ZEROSPAM****SC rate:** 99.92%**FP rate:** 0.03%**Final score:** 99.70**Project Honey Pot SC rate:** 99.91%**Abusix SC rate:** 99.96%**Newsletters FP rate:** 2.2%**Speed:** 10%: ●; 50%: ●; 95%: ●; 98%: ●**PARTIAL SOLUTIONS**

The products listed below are 'partial solutions', which means they only have access to part of the emails and/or SMTP transaction, and are intended to be used as part of a full spam solution. As such, their performance should neither be compared with those of the full solutions listed previously, nor necessarily with each other's.

New to the test this month is *URIBL*, a DNS-based blocklist which, as its name suggests, is used to check URLs (or, more precisely, domain names) found in the body of emails. It is thus comparable with *Spamhaus DBL*, though it should be noted that no two blocklists have the same use case.

Its spam catch rate was close to 73%, which is certainly impressive, though this may in part have been a consequence of its use of a 'grey' list containing domains found in unsolicited, but not necessarily illegal, bulk emails, which the product itself warns could cause false positives⁴. Indeed, it 'blocked' 30 per cent of the emails in our newsletter feed.

IBM XForce API**SC rate:** 94.41%**FP rate:** 0.00%**Final score:** 94.34**Project Honey Pot SC rate:** 93.86%**Abusix SC rate:** 98.19%**Newsletters FP rate:** 1.6%**Spamhaus DBL****SC rate:** 32.14%**FP rate:** 0.00%**Final score:** 32.14**Project Honey Pot SC rate:** 36.25%**Abusix SC rate:** 3.73%**Newsletters FP rate:** 0.0%**Spamhaus ZEN****SC rate:** 91.52%**FP rate:** 0.00%**Final score:** 91.52**Project Honey Pot SC rate:** 90.36%**Abusix SC rate:** 99.56%**Newsletters FP rate:** 0.0%⁴<http://uribl.com/about.shtml>

Spamhaus ZEN+DBL

SC rate: 93.68%
FP rate: 0.00%
Final score: 93.68
Project Honey Pot SC rate: 92.83%
Abusix SC rate: 99.56%
Newsletters FP rate: 0.0%

URIBL

SC rate: 72.91%
FP rate: 0.00%
Final score: 72.18
Project Honey Pot SC rate: 73.36%
Abusix SC rate: 69.80%
Newsletters FP rate: 30.6%

CONCLUSION









Spam remains a well mitigated security problem. However, as this test now clearly shows, when it comes to malicious attachments, there is certainly some room for improvement, especially since this is an area where spam is far more than a nuisance.

We are already looking forward to the next test – to be published mid-December – when we will report in more detail on this aspect. Those interested in submitting a product should contact martijn.grooten@virusbulletin.com.

Product	Final score
OnlyMyEmail	99.997
ESET	99.98
Libra Esva	99.96
IBM	99.95
FortiMail	99.94
Bitdefender	99.85
Trustwave	99.79
ZEROSPAM	99.70
Kaspersky LMS	99.64
Kaspersky SMG	99.56
Axway	99.26
Egedian	99.17
Vade Retro MailCube	99.14
Sophos	99.00
SpamTitan	98.57
Scrollout	98.44
GFI MailEssentials	97.04

(Please refer to the text for full product names and details.)

Editor: Martijn Grooten
Chief of Operations: John Hawes
Security Test Engineers: Scott James, Tony Oliveira, Adrian Luca, Ionuț Răileanu, Chris Stock
Sales Executive: Allison Sketchley
Editorial Assistant: Helen Martin
Developer: Lian Sebe
Consultant Technical Editor: Dr Morton Swimmer
 © 2016 Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England
 Tel: +44 (0)1235 555139 Fax: +44 (0)1865 543153
 Email: editorial@virusbtl.com Web: <https://www.virusbulletin.com/>

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	VBSpam	Final score
Axway	7768	4	0.05%	280	73430	99.62%		99.26
Bitdefender	7772	0	0.00%	104	73606	99.86%		99.85
Egedian	7772	0	0.00%	599	73111	99.19%		99.17
ESET	7772	0	0.00%	4	73706	99.99%		99.98
FortiMail	7772	0	0.00%	23	73687	99.97%		99.94
GFI MailEssentials	7735	37	0.48%	332	73378	99.55%		97.04
IBM	7772	0	0.00%	21	73689	99.97%		99.95
Kaspersky LMS	7771	1	0.01%	218	73492	99.70%		99.64
Kaspersky SMG	7771	1	0.01%	279	73431	99.62%		99.56
Libra Esva	7772	0	0.00%	28	73682	99.96%		99.96
OnlyMyEmail	7772	0	0.00%	2	73708	99.997%		99.997
Scrollout	7752	20	0.26%	77	73633	99.90%		98.44
Sophos	7764	8	0.10%	361	73349	99.51%		99.00
SpamTitan	7772	0	0.00%	1037	72673	98.59%		98.57
Trustwave	7772	0	0.00%	91	73619	99.88%		99.79
Vade Retro MailCube	7772	0	0.00%	612	73098	99.17%		99.14
ZEROSPAM	7770	2	0.03%	61	73649	99.92%		99.70
IBM X-Force*	7772	0	0.00%	4124	69586	94.41%	N/A	94.34
Spamhaus DBL*	7772	0	0.00%	50022	23688	32.14%	N/A	32.14
Spamhaus ZEN*	7772	0	0.00%	6250	67460	91.52%	N/A	91.52
Spamhaus ZEN+DBL*	7772	0	0.00%	4656	69054	93.68%	N/A	93.68
URIBL*	7772	0	0.00%	19965	53745	72.91%	N/A	72.18

*The Spamhaus products, IBM X-Force and URIBL are partial solutions and their performance should not be compared with that of other products.

(Please refer to the text for full product names and details.)

	Newsletters		Project Honey Pot		Abusix		STDev†	Speed			
	False positives	FP rate	False negatives	SC rate	False negatives	SC rate		10%	50%	95%	98%
Axway	8	2.5%	274	99.57%	6	99.94%	0.51	●	●	●	●
Bitdefender	1	0.3%	102	99.84%	2	99.98%	0.05	●	●	●	●
Egedian	1	0.3%	597	99.07%	2	99.98%	1.05	●	●	●	●
ESET	1	0.3%	3	99.995%	1	99.989%	0.17	●	●	●	●
FortiMail	2	0.6%	22	99.97%	1	99.99%	0.07	●	●	●	●
GFI MailEssentials	12	3.8%	307	99.52%	25	99.73%	0.54	●	●	●	●
IBM	2	0.6%	19	99.97%	2	99.98%	0.18	●	●	●	●
Kaspersky LMS	0	0.0%	204	99.68%	14	99.85%	0.33	●	●	●	●
Kaspersky SMG	0	0.0%	261	99.59%	18	99.81%	0.36	●	●	●	●
Libra Esva	0	0.0%	27	99.96%	1	99.99%	0.10	●	●	●	●
OnlyMyEmail	0	0.0%	2	99.997%	0	100.00%	0.00	●	●	●	●
Scrollout	14	4.5%	76	99.88%	1	99.99%	0.28	●	●	●	●
Sophos	0	0.0%	347	99.46%	14	99.85%	0.72	●	●	●	●
SpamTitan	2	0.6%	986	98.47%	51	99.45%	0.94	●	●	●	●
Trustwave	7	2.2%	90	99.86%	1	99.99%	0.24	●	●	●	●
Vade Retro MailCube	2	0.6%	611	99.05%	1	99.99%	0.51	●	●	●	●
ZEROSPAM	7	2.2%	57	99.91%	4	99.96%	0.13	●	●	●	●
IBM X-Force*	5	1.6%	3955	93.86%	169	98.19%	2.07	N/A	N/A	N/A	N/A
Spamhaus DBL*	0	0.0%	41044	36.25%	8978	3.73%	5.97	N/A	N/A	N/A	N/A
Spamhaus ZEN*	0	0.0%	6209	90.36%	41	99.56%	3.03	N/A	N/A	N/A	N/A
Spamhaus ZEN+DBL*	0	0.0%	4615	92.83%	41	99.56%	2.36	N/A	N/A	N/A	N/A
URIBL*	96	30.6%	17149	73.36%	2816	69.80%	27.43	N/A	N/A	N/A	N/A

* The Spamhaus products, IBM X-Force and URIBL are partial solutions and their performance should not be compared with that of other products.

† The standard deviation of a product is calculated using the set of its hourly spam catch rates.

● 0–30 seconds; ● 30 seconds to two minutes; ● two minutes to 10 minutes; ● more than 10 minutes.
(Please refer to the text for full product names.)

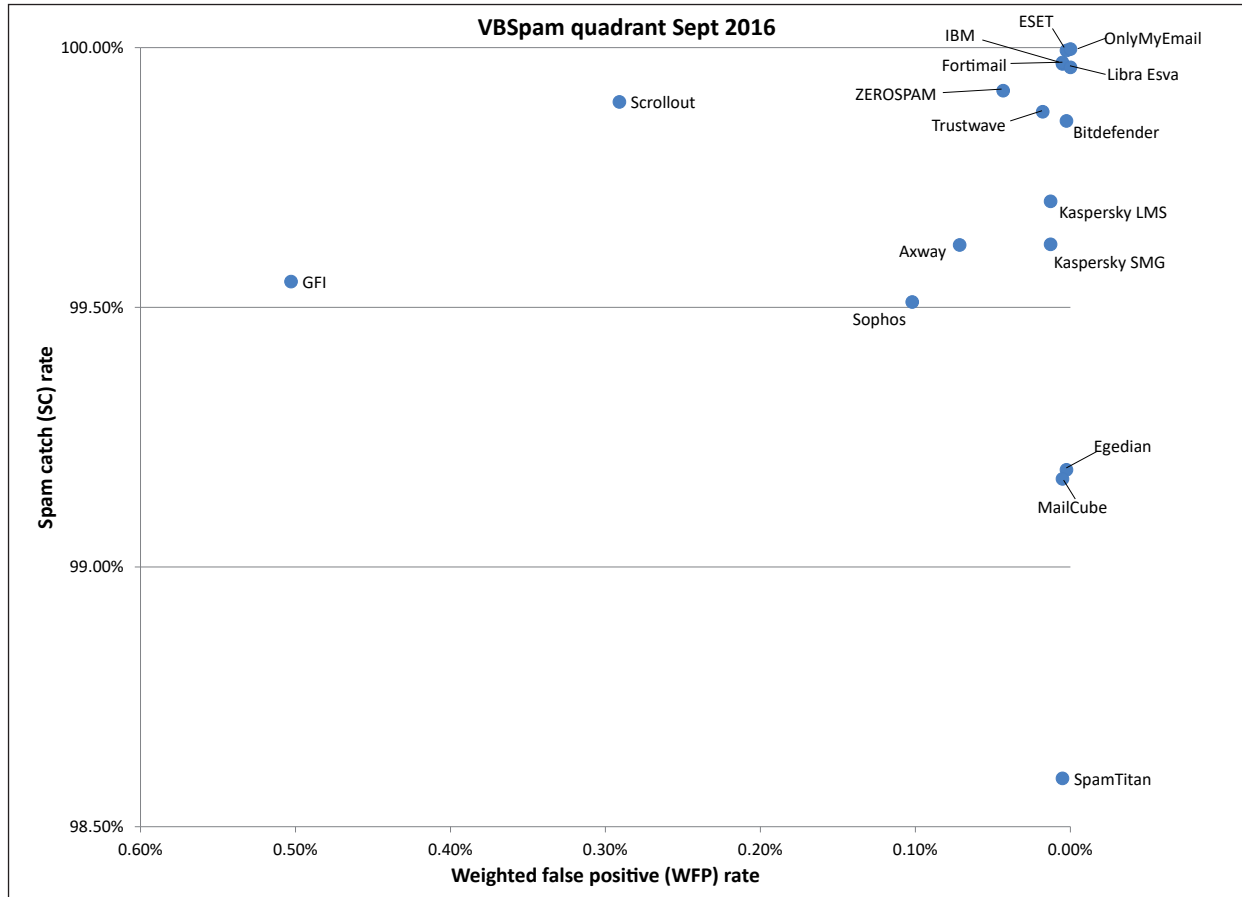
Hosted solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Multiple MX-records	Multiple locations
OnlyMyEmail	Proprietary (optional)		√	√	*	√	√
Vade Retro MailCube	DrWeb; proprietary	√	√	√		√	√
ZEROSPAM	ClamAV			√		√	√

* OnlyMyEmail verifies DMARC status but doesn't provide feedback at the moment.

(Please refer to the text for full product names.)

Local solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Interface			
						CLI	GUI	Web GUI	API
Axway MailGate	Kaspersky, McAfee	√	√	√				√	
Bitdefender	Bitdefender	√				√		√	√
Egedian	Bitdefender, ClamAV	√				√		√	√
ESET	ESET Threatsense	√	√	√	√	√	√		
FortiMail	Fortinet	√	√	√		√		√	
GFI	Five anti-virus engines	√		√				√	
IBM	Sophos; IBM Remote Malware Detection			√		√		√	
Kaspersky LMS	Kaspersky Lab	√		√		√		√	
Kaspersky SMG	Kaspersky Lab	√		√		√		√	
Libra Esva	ClamAV; others optional		√	√		√		√	
Scrollout	ClamAV			√		√		√	√
Sophos	Sophos		√	√				√	
SpamTitan	Kaspersky; ClamAV	√	√	√		√		√	√
Trustwave	Support for multiple third-party engines	√	√	√		√	√	√	

(Please refer to the text for full product names.)



(Please refer to the text for full product names.)