

virus

BULLETIN

Covering the global threat landscape

VBSPAM EMAIL SECURITY COMPARATIVE REVIEW JUNE 2024

Ionuț Răileanu & Adrian Luca

In the Q2 2024 VBSpam test – which forms part of Virus Bulletin’s continuously running security product test suite – we measured the performance of a number of email security solutions against various streams of wanted, unwanted and malicious emails. One third of the solutions we tested opted to be included in the public test, the rest opting for private testing (all details and results remaining unpublished). The solutions tested publicly were ten full email security solutions, one custom configured solution¹ and one open-source solution.

¹ *Spamhaus Data Query Service (DQS) + SpamAssassin* is a custom solution built on top of the *SpamAssassin* open-source anti-spam platform.

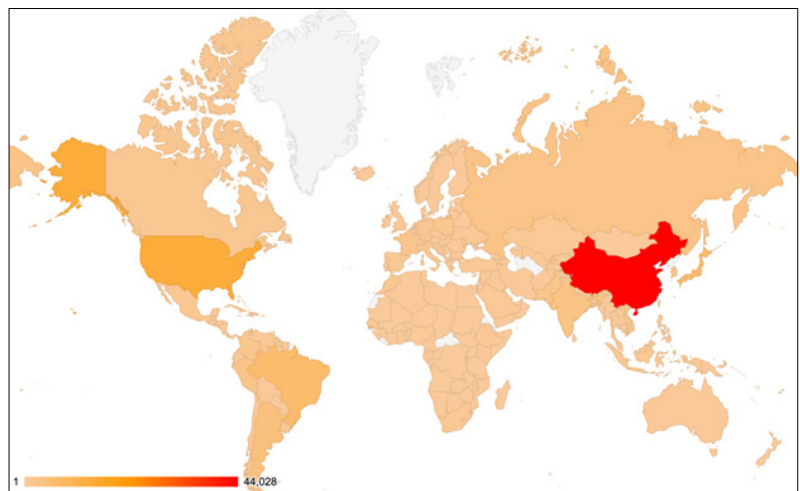
The test highlighted a critical challenge for all participants: the timely blocking of attacks that leverage legitimate services such as email marketing solutions and web pages with unsanitized input. These vectors, often overlooked due to their benign origins, present a significant risk as they can be exploited to bypass traditional security measures. Our findings underscore the necessity for advanced detection mechanisms capable of identifying and neutralizing such threats swiftly to maintain robust email security.

For some additional background to this report, the table and map below show the geographical distribution (based on sender IP address) of the spam emails seen in the test². *(Note: these statistics are relevant only to the spam samples we received during the test period.)*

² For 9,033 spam samples (6.33%) we were not able to find geographical location data based on IP address.

#	Sender's IP country	Percentage of spam
1	China	30.84%
2	United States	9.56%
3	Japan	4.73%
4	Brazil	4.62%
5	Argentina	2.97%
6	India	2.29%
7	Russian Federation	2.10%
8	Peru	1.82%
9	Republic of Korea	1.73%
10	Pakistan	1.42%

Top 10 countries from which spam was sent.



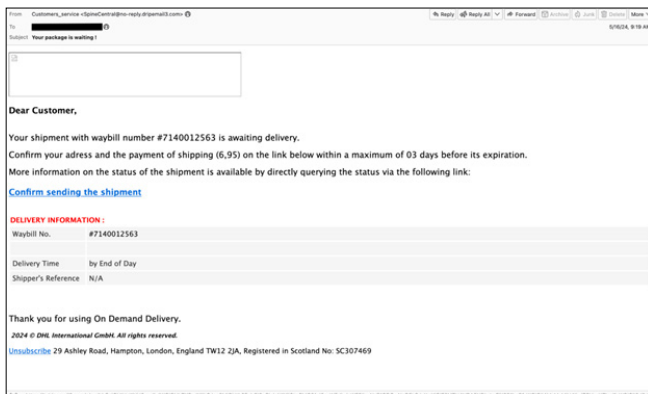
Geographical distribution of spam based on sender IP address.

HIGHLIGHTS

Phishing abuse of email marketing services

Among the samples received during the 16-day test period, we spotted a phishing campaign using an email marketing service platform. We observed the active campaign on 16 May, from 06:26 to 09:29 GMT.

At the time of our analysis the URLs leading to the phishing page were unavailable. The combination of the use of legitimate services and short-duration campaigns gives the attackers a window to send the phishing emails. We noted that the security solutions blocked these threats with a delay, compared to the blocking of a simple phishing campaign written in English.



Email marketing service phishing sample.



German phishing sample.



Dutch phishing sample.

Non-English phishing

We continue to note that most of the missed phishing emails are written in languages other than English. We highlight examples of German, Dutch and French phishing.

We noticed that these samples each contain special characters specific to the language they are written in.

Spam from unsanitized web page input

Spam emails generated from forms on unsanitized web pages represent a significant threat to cybersecurity. These forms, often found on websites lacking proper input validation, become easy targets for attackers. By exploiting these vulnerabilities, spammers can inject malicious scripts

or automated bots to submit bulk messages through these forms.

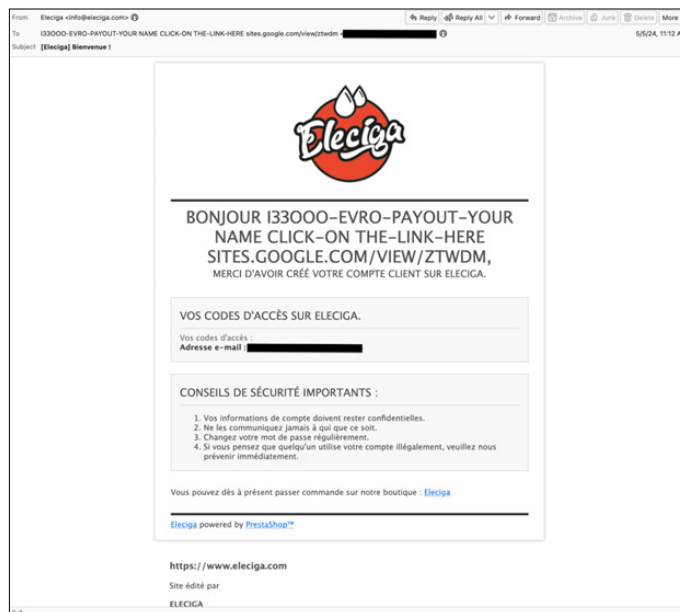
In this test these samples were the ones most commonly missed by the participating solutions.

RESULTS

Of the participating full solutions, three achieved a VBSpam award: *N-able Mail Assure*, *N-able SpamExperts* and *Zoho Mail*, as did the custom configured solution *Spamhaus DQS + SpamAssassin*, while seven – *Bitdefender GravityZone Premium*, *FortiMail*, *Mimecast*, *Net At Work NoSpamProxy*, *SEPPmail.cloud Filter*, *Sophos Email* and *SpamTitan* – were awarded a VBSpam+ certification.



French phishing sample.



Spam from unsanitized web page input.

(Note: Since, for a number of products, catch rates and/or final scores were very close to, whilst remaining a fraction below, 100%, we quote all the spam-related scores and final scores with three decimal places.)

Bitdefender GravityZone Premium

SC rate: 99.982%
 FP rate: 0.00%
 Final score: 99.982
 Malware catch rate: 99.610%
 Phishing catch rate: 99.990%
 Project Honey Pot SC rate: 100.000%
 Abusix SC rate: 99.971%
 MXMailData SC rate: 100.000%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Bitdefender executed a robust performance with a spam detection rate of 99.982%. With no false positives of any kind, and higher than 99% catch rates on the malware and phishing corpus, the product is awarded VBSpam+ certification, continuing its years-long uninterrupted record.

Fortinet FortiMail

SC rate: 99.962%
 FP rate: 0.00%
 Final score: 99.962
 Malware catch rate: 100.000%
 Phishing catch rate: 99.980%
 Project Honey Pot SC rate: 99.985%
 Abusix SC rate: 99.954%
 MXMailData SC rate: 99.810%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Fortinet's flagship solution in fighting email-based threats continues to show a solid performance in the VBSpam tests. Without misclassifying any ham or newsletter samples, while correctly blocking all the malware emails, it is awarded VBSpam+ certification.

Mimecast

SC rate: 99.699%
 FP rate: 0.00%
 Final score: 99.699
 Malware catch rate: 98.280%

Phishing catch rate: 99.950%
 Project Honey Pot SC rate: 99.466%
 Abusix SC rate: 99.875%
 MXMailData SC rate: 98.590%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



No false positives of any kind were recorded for Mimecast in this test. With a higher than 99.95% spam catch rate and very good labels on the speed test, the product is awarded VBSpam+ certification.

N-able Mail Assure

SC rate: 99.815%
 FP rate: 0.00%
 Final score: 99.623
 Malware catch rate: 95.500%
 Phishing catch rate: 99.930%
 Project Honey Pot SC rate: 99.955%
 Abusix SC rate: 99.833%
 MXMailData SC rate: 97.000%
 Newsletters FP rate: 8.1%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



N-able Mail Assure achieved higher than 99.90% catch rates on the overall spam corpus as well as on the malware and phishing subcategories. It is only due to an elevated newsletter false positive score that it misses out on a VBSpam+ award. Nevertheless, it easily earns VBSpam certification with an impressive final score.

N-able SpamExperts

SC rate: 99.815%
 FP rate: 0.00%
 Final score: 99.623
 Malware catch rate: 95.500%
 Phishing catch rate: 99.920%
 Project Honey Pot SC rate: 99.955%
 Abusix SC rate: 99.832%
 MXMailData SC rate: 97.000%
 Newsletters FP rate: 8.1%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



With almost identical scores to its sister product, N-able SpamExperts also narrowly misses out on a VBSpam+ award but easily earns VBSpam certification in this test.

Net At Work NoSpamProxy

SC rate: 99.959%
 FP rate: 0.00%
 Final score: 99.959
 Malware catch rate: 99.920%
 Phishing catch rate: 99.990%
 Project Honey Pot SC rate: 99.970%
 Abusix SC rate: 99.951%
 MXMailData SC rate: 100.000%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Net At Work's email security solution achieved higher than 99.95% catch rates on the spam corpus as well as on the malware and phishing subcategories. With no false positives of any kind, the product is awarded VBSpam+ certification.

Rspamd

SC rate: 91.039%
 FP rate: 0.58%
 Final score: 87.839
 Malware catch rate: 58.100%
 Phishing catch rate: 95.260%
 Project Honey Pot SC rate: 84.636%
 Abusix SC rate: 95.727%
 MXMailData SC rate: 65.800%
 Newsletters FP rate: 13.5%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Dealing with the malware samples was a challenge for the open-source *Rspamd*. However, we continue to see a decent performance from the solution on the overall spam corpus, in this case blocking more than 91% of the samples.

SEPPmail.cloud Filter

SC rate: 99.988%
 FP rate: 0.00%
 Final score: 99.988
 Malware catch rate: 100.000%
 Phishing catch rate: 99.970%
 Project Honey Pot SC rate: 99.967%
 Abusix SC rate: 100.000%
 MXMailData SC rate: 100.000%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



SEPPmail.cloud Filter performed admirably, recording the highest final score in this test. The product blocked 100% of

the malware samples and didn't miss any ham or newsletter samples, earning VBSpam+ certification with ease.

Sophos Email

SC rate: 99.977%
 FP rate: 0.00%
 Final score: 99.977
 Malware catch rate: 100.000%
 Phishing catch rate: 100.000%
 Project Honey Pot SC rate: 99.985%
 Abusix SC rate: 99.971%
 MXMailData SC rate: 100.000%
 Newsletters FP rate: 0.0%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Sophos marks its return after some years to the VBSpam test with an impressive performance, being the only solution in this test to block all the malware and phishing samples. The product also correctly classified all the ham and newsletter samples, and is awarded VBSpam+ certification.

Spamhaus DQS + SpamAssassin

SC rate: 99.315%
 FP rate: 0.00%
 Final score: 99.251
 Malware catch rate: 96.870%
 Phishing catch rate: 99.690%
 Project Honey Pot SC rate: 99.835%
 Abusix SC rate: 99.358%
 MXMailData SC rate: 89.490%
 Newsletters FP rate: 2.7%
 Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Spamhaus DQS + SpamAssassin is a custom-configured solution that integrates the *Spamhaus DQS* DNSBL service and the free open-source solution *SpamAssassin*. In this test no ham samples were blocked by the combined solution. With a final score of 99.251 the solution earns VBSpam certification.

SpamTitan

SC rate: 99.984%
 FP rate: 0.00%
 Final score: 99.984
 Malware catch rate: 100.000%
 Phishing catch rate: 99.990%
 Project Honey Pot SC rate: 99.994%

Abusix SC rate: 99.978%
MXMailData SC rate: 100.000%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

SpamTitan managed to block all the malware samples in the test and missed only one phishing sample. The product’s performance was further enhanced by a lack of false positives of any kind. With a final score of 99.984 – the second highest in this test – it earns VBSpam+ certification.



Zoho Mail

SC rate: 99.019%
FP rate: 0.00%
Final score: 99.019
Malware catch rate: 98.120%
Phishing catch rate: 99.660%
Project Honey Pot SC rate: 98.296%
Abusix SC rate: 99.493%
MXMailData SC rate: 97.730%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Zoho Mail put in a solid performance, achieving higher than 99% catch rates on the phishing samples and also on the overall spam corpus, while correctly classifying all the ham samples. The product is awarded VBSpam certification.



APPENDIX: SET-UP, METHODOLOGY AND EMAIL CORPORA

The full VBSpam test methodology can be found at <https://www.virusbulletin.com/testing/vbspam/vbspam-methodology/vbspam-methodology-ver20>.

The test ran for 16 days, from 12am on 4 May to 12am on 20 May 2024 (GMT).

The test corpus consisted of 144,348 emails. 142,756 of these were spam, 51,917 of which were provided by *Project Honey Pot*, with 87,710 provided by *Abusix* and the remaining 3,129 spam emails provided by *MXMailData*. There were 1,555 legitimate emails (‘ham’) and 37 newsletters, a category that includes various kinds of commercial and non-commercial opt-in mailings.

75 emails in the spam corpus were considered ‘unwanted’ (see the June 2018 report³) and were included with a weight

³ <https://www.virusbulletin.com/virusbulletin/2018/06/vbspam-comparative-review>.

of 0.2; this explains the non-integer numbers in some of the tables.

Moreover, 2,556 emails from the spam corpus were found to contain a malicious attachment while 14,991 contained a link to a phishing or malware site; though we report separate performance metrics on these corpora, 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.

For those products running in our lab, we all 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 positive to false negatives, we created a one-dimensional ‘Final score’ to compare products. This 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:

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

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:

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

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

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

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.

Head of Testing: Peter Karsai

Security Test Engineers: Adrian Luca, Csaba Mészáros, Ionuț Răileanu

Operations Manager: Bálint Tanos










Sales Executive: Allison Sketchley

Editorial Assistant: Helen Martin

© 2024 Virus Bulletin Ltd, Manor House - Office 6, Howbery Business Park,
Wallingford OX10 8BA, UK

Tel: +44 20 3920 6348 Email: editorial@virusbulletin.com

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

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	Final score	VBSpam
Bitdefender GravityZone Premium	1555	0	0.00%	25.8	142670.2	99.982%	99.982	
Fortinet FortiMail	1555	0	0.00%	54	142642	99.962%	99.962	
Mimecast	1555	0	0.00%	430	142266	99.699%	99.699	
N-able Mail Assure	1555	0	0.00%	263.4	142432.6	99.815%	99.623	
N-able SpamExperts	1555	0	0.00%	264.4	142431.6	99.815%	99.623	
Net At Work NoSpamProxy	1555	0	0.00%	59	142637	99.959%	99.959	
Rspamd	1546	9	0.58%	12786.6	129909.4	91.039%	87.839	
SEPPmail.cloud Filter	1555	0	0.00%	17	142679	99.988%	99.988	
Sophos Email	1555	0	0.00%	33.2	142662.8	99.977%	99.977	
Spamhaus DQS + SpamAssassin [‡]	1555	0	0.00%	977.8	141718.2	99.315%	99.251	
SpamTitan	1555	0	0.00%	22.4	142673.6	99.984%	99.984	
Zoho Mail	1555	0	0.00%	1399.2	141296.8	99.019%	99.019	

[‡]Spamhaus Data Query Service (DQS) + SpamAssassin is a fully configured solution that integrates Spamhaus DQS on top of SpamAssassin. Spamhaus DQS is not a stand-alone solution but rather a DNSBL service that can be added to MTAs and email security solutions such as SpamAssassin. The test set up reflects the real-life performance expected from this combined production deployment, not as individual product elements.

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

	Newsletters		Malware		Phishing		Project Honey Pot		Abusix		MXMailData		STDev [†]
	False positives	FP rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate	
Bitdefender GravityZone Premium	0	0.0%	10	99.610%	1	99.990%	0	100.000%	25.8	99.971%	0	100.000%	0.11
Fortinet FortiMail	0	0.0%	0	100.000%	3	99.980%	8	99.985%	40	99.954%	6	99.810%	0.21
Mimecast	0	0.0%	44	98.280%	8	99.950%	276.8	99.466%	109.2	99.875%	44	98.590%	0.68
N-able Mail Assure	3	8.1%	115	95.500%	11	99.930%	23.2	99.955%	146.2	99.833%	94	97.000%	0.54
N-able SpamExperts	3	8.1%	115	95.500%	12	99.920%	23.2	99.955%	147.2	99.832%	94	97.000%	0.54
Net At Work NoSpamProxy	0	0.0%	2	99.920%	1	99.990%	15.6	99.970%	43.4	99.951%	0	100.000%	0.15
Rspamd	5	13.5%	1071	58.100%	711	95.260%	7969.4	84.636%	3747.2	95.727%	1070	65.800%	6.61
SEPPmail.cloud Filter	0	0.0%	0	100.000%	4	99.970%	17	99.967%	0	100.000%	0	100.000%	0.10
Sophos Email	0	0.0%	0	100.000%	0	100.000%	8	99.985%	25.2	99.971%	0	100.000%	0.13
Spamhaus DQS + SpamAssassin [‡]	1	2.7%	80	96.870%	47	99.690%	85.4	99.835%	563.4	99.358%	329	89.490%	1.30
SpamTitan	0	0.0%	0	100.000%	1	99.990%	3	99.994%	19.4	99.978%	0	100.000%	0.09
Zoho Mail	0	0.0%	48	98.120%	51	99.660%	884	98.296%	444.2	99.493%	71	97.730%	1.07

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

[‡]Spamhaus Data Query Service (DQS) + SpamAssassin is a fully configured solution that integrates Spamhaus DQS on top of SpamAssassin. Spamhaus DQS is not a stand-alone solution but rather a DNSBL service that can be added to MTAs and email security solutions such as SpamAssassin. The test set up reflects the real-life performance expected from this combined production deployment, not as individual product elements.
(Please refer to the text for full product names and details.)

	Speed			
	10%	50%	95%	98%
Bitdefender GravityZone Premium	●	●	●	●
Fortinet FortiMail	●	●	●	●
Mimecast	●	●	●	●
N-able Mail Assure	●	●	●	●
N-able SpamExperts	●	●	●	●
Net At Work NoSpamProxy	●	●	●	●
Rspamd	●	●	●	●
SEPPmail.cloud Filter	●	●	●	●
Sophos Email	●	●	●	●
Spamhaus DQS + SpamAssassin‡	●	●	●	●
SpamTitan	●	●	●	●
Zoho Mail	●	●	●	●

● 0–30 seconds; ● 30 seconds to two minutes; ● two minutes to 10 minutes; ● more than 10 minutes.

Products ranked by final score	
SEPPmail.cloud Filter	99.988
SpamTitan	99.984
Bitdefender GravityZone Premium	99.982
Sophos Email	99.977
Fortinet FortiMail	99.962
Net At Work NoSpamProxy	99.959
Mimecast	99.699
N-able Mail Assure	99.623
N-able SpamExperts	99.623
Spamhaus DQS + SpamAssassin‡	99.251
Zoho Mail	99.019
Rspamd	87.839

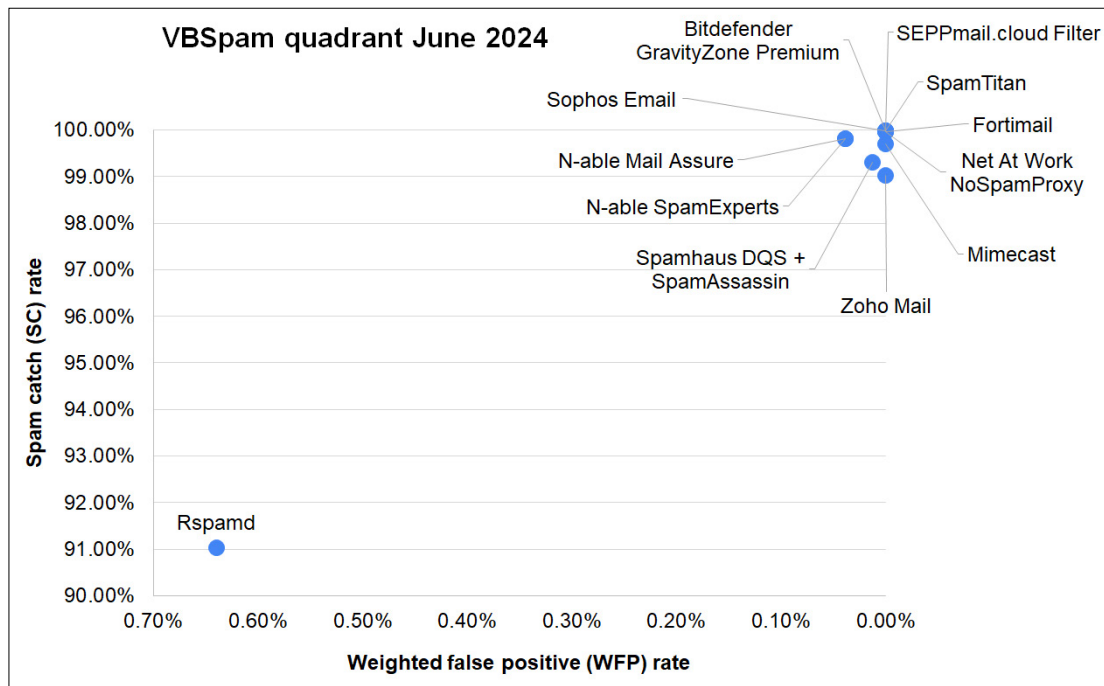
‡Spamhaus Data Query Service (DQS) + SpamAssassin is a fully configured solution that integrates Spamhaus DQS on top of SpamAssassin. Spamhaus DQS is not a stand-alone solution but rather a DNSBL service that can be added to MTAs and email security solutions such as SpamAssassin. The test set up reflects the real-life performance expected from this combined production deployment, not as individual product elements.

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

Hosted solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Multiple MX-records	Multiple locations
Mimecast	Mimecast		√	√	√	√	√
N-able Mail Assure	N-able Mail Assure	√	√	√	√		
N-able SpamExperts	SpamExperts	√	√	√	√		
Net At Work NoSpamProxy	32Guards & NoSpamProxy		√	√	√	√	√
SEPPmail.cloud Filter	SEPPmail	√	√	√	√	√	√
Sophos Email	Sophos	√	√	√	√	√	√
SpamTitan	SpamTitan	√	√	√	√	√	√
Zoho Mail	Zoho		√	√	√	√	√

Local solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Interface			
						CLI	GUI	Web GUI	API
Bitdefender GravityZone Premium	Bitdefender	√				√		√	√
Fortinet FortiMail	Fortinet	√	√	√	√	√		√	√
Rspamd	None					√			
Spamhaus DQS + SpamAssassin [‡]	Optional	√	√	√					√

[‡]Spamhaus Data Query Service (DQS) + SpamAssassin is a fully configured solution that integrates Spamhaus DQS on top of SpamAssassin. Spamhaus DQS is not a stand-alone solution but rather a DNSBL service that can be added to MTAs and email security solutions such as SpamAssassin. The test set up reflects the real-life performance expected from this combined production deployment, not as individual product elements.



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