

virus

BULLETIN

Covering the global threat landscape

VBSPAM EMAIL SECURITY COMPARATIVE REVIEW SEPTEMBER 2022

Ionuț Răileanu & Adrian Luca

In this test – which forms part of *Virus Bulletin's* continuously running security product test suite – seven full email security solutions, one custom configured solution¹, one open-source solution and one blocklist were assembled on the test bench to measure their performance against various streams of wanted, unwanted and malicious emails.

During the 16 days in August over which this test ran we saw fewer spam emails than in previous tests. This translated into fewer malware and phishing emails as well.

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

The tested solutions managed to block the majority of spam emails, the more significant challenge being the phishing emails, despite the lower number of these.

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 test. *(Note: these statistics are relevant only to the spam samples we received during the test period.)*

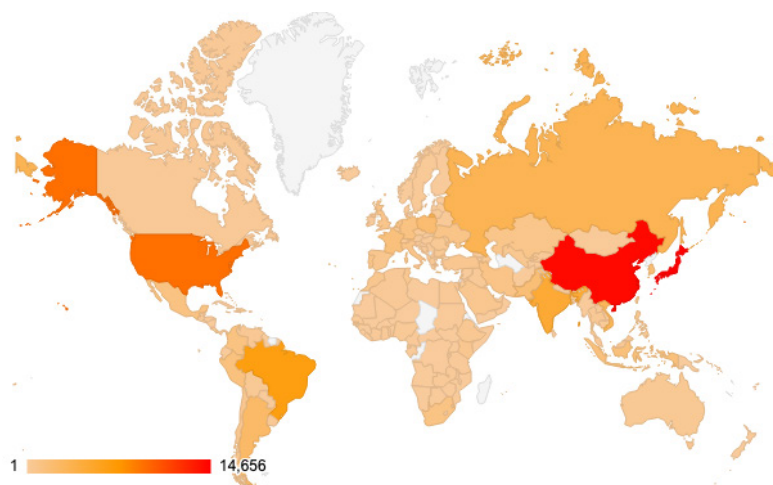
MALWARE AND PHISHING

The decrease in the number of all spam, malware and phishing samples seen during the test period translated into a silence among the campaigns linked to certain threat actors as well.

Although the majority of malware emails didn't pose much of a challenge to the tested solutions, the phishing emails

#	Sender's IP country	Percentage of spam
1	Japan	13.60%
2	China	13.19%
3	United States	8.66%
4	Brazil	6.04%
5	India	4.43%
6	Russian Federation	3.14%
7	Vietnam	2.89%
8	Argentina	2.26%
9	Poland	1.89%
10	Republic of Korea	1.65%

Top 10 countries from which spam was sent.



Geographical distribution of spam based on sender IP address.

were a different matter. No solution managed to block all the emails from the phishing corpus. We continue to see that most of the phishing emails that pass through the email filters are in languages other than English.

Here we describe those samples that managed to evade the detection of most of the tested solutions.

Romanian phishing emails

For both of these samples, the payload wasn't available at the time of our analysis. We mention these samples because most of the tested solutions missed them (eight out of 10 for Sample 1 and five out of 10 for Sample 2).

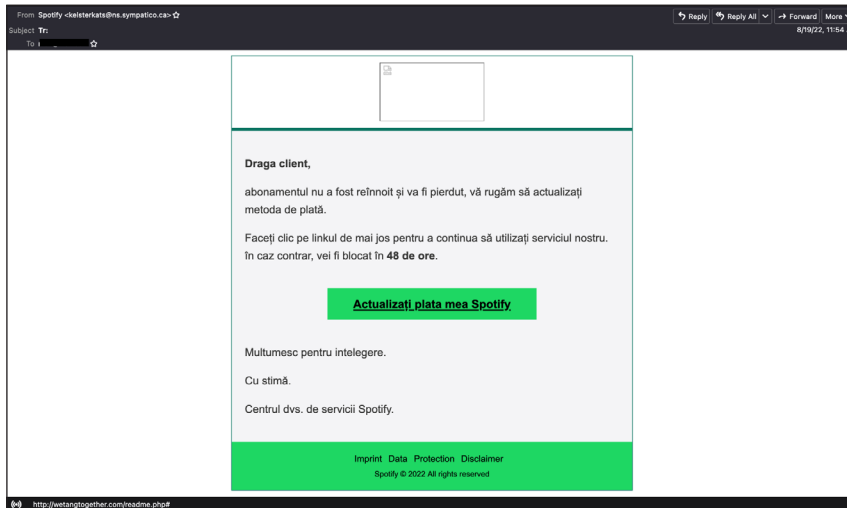
The following are the indicators of compromise for the two emails:

Sample 1

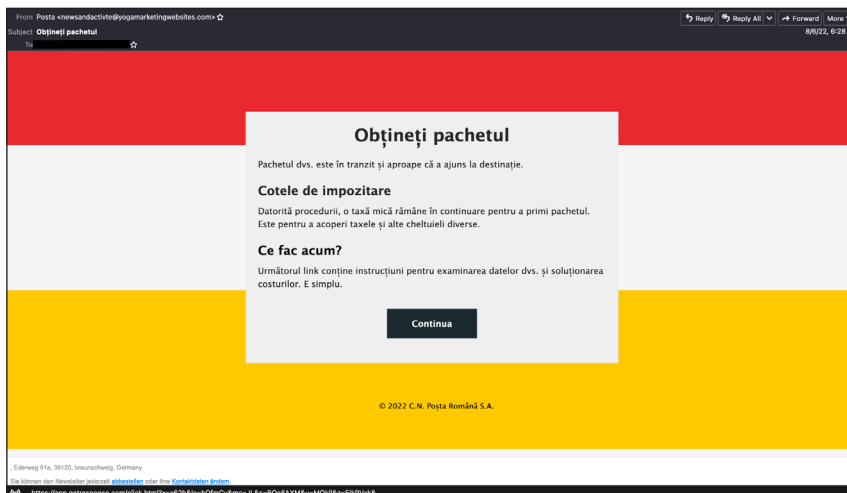
- Subject: Tr:
- From: Spotify <kelsterkats@ns.sympatico.ca>
- Sender IP address: 209.71.212.29
- URL from email's body: `hxxp://wetangtogether[.]com/readme[.]php#`

Sample 2

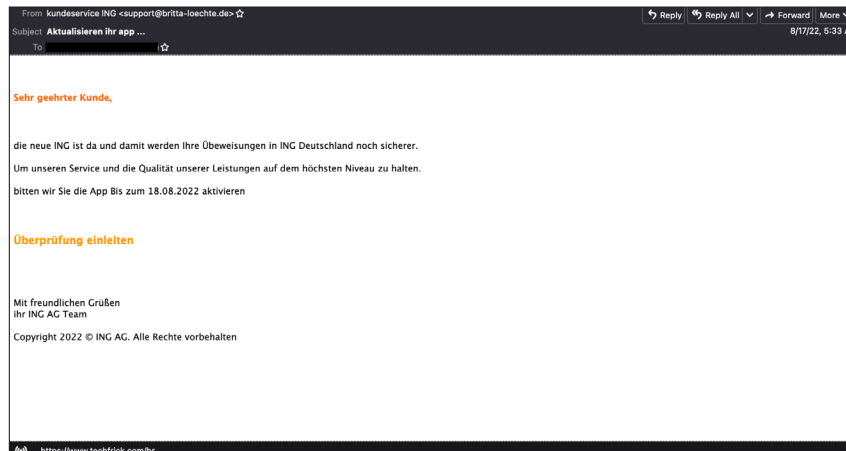
- Subject: Obțineți pachetul
- From: Posta <newsandactivite@yogamarketingwebsites.com>
- Sender IP address: 104.160.65.34
- URL domain from email's body: `app[.]getresponse[.]com`



Romanian phishing Sample 1.



Romanian phishing Sample 2.



German phishing sample.

German banking phishing

This spear-phishing sample was missed by more than half of the tested solutions (six out of 10). It is targeted to a German-speaking audience and we found it only once in the spam corpus, on 17 August.

Unfortunately, in our analysis we didn't get to a malicious payload. However, we considered it worth mentioning and here we list some of the indicators of this phishing email:

- Subject: Aktualisieren ihr app ...
- From: customer service lNG <support@britta-loechte.de>
- Sender IP address: 185.15.192.40
- URL domains from email's body: deref-gmx[.]net, techfrick[.]com, scc[.]rumbo[.]com

RESULTS

The majority of the tested solutions managed to achieve very good spam catch rates, with values exceeding 99%. A better comparison between the solutions can be made by looking at the malware and phishing catch rates, subsets of the spam corpus. Here we highlight the performance of *Bitdefender*, *N-able Mail Assure*, *SEPPmail* and *N-able SpamExperts*, all with 100% malware catch rate. No solution achieved a 100% catch rate on the phishing corpus, but *Bitdefender* deserves a mention for only having missed one sample of this kind.

Of the participating full solutions, three – *Cleanmail*, *SEPPmail* and *Zoho Mail* – achieved a VBSpam award, as did the custom configured solution *Spamhaus Data Query Service (DQS)* + *SpamAssassin*, while other four – *Bitdefender*, *Fortinet*, *N-able Mail Assure* and *N-able SpamExperts* – are awarded a VBSpam+ certification.

Bitdefender Security for Mail Servers 3.1.7

SC rate: 99.98%

FP rate: 0.00%

Final score: 99.98

Malware catch rate: 100.00%

Phishing catch rate: 99.96%

Project Honey Pot SC rate: 99.99%

Abusix SC rate: 99.98%

MXMailData SC rate: 100.00%

Newsletters FP rate: 0.0%

Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Bitdefender continues its run of VBSpam+ awards with an impressive performance in this test. No malware email passed through its filters, and the product achieved the best phishing catch rate, with only one missed sample. With no ham or newsletter false positives and speed values all in the green, *Bitdefender* earns another VBSpam+ award.

Cleanmail Domain Gateway

SC rate: 99.94%

FP rate: 0.05%

Final score: 99.71

Malware catch rate: 99.91%

Phishing catch rate: 98.89%

Project Honey Pot SC rate: 99.94%

Abusix SC rate: 99.94%

MXMailData SC rate: 99.87%

Newsletters FP rate: 0.0%

Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Cleanmail easily earns VBSpam certification in this test. The solution achieved higher than 99% spam and malware catch rates, while successfully detecting all the newsletters and missing only one ham email.

Fortinet FortiMail

SC rate: 99.97%
FP rate: 0.00%
Final score: 99.97
Malware catch rate: 99.73%
Phishing catch rate: 99.82%
Project Honey Pot SC rate: 99.95%
Abusix SC rate: 99.98%
MXMailData SC rate: 99.61%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



Another VBSpam+ certification is awarded to *Fortinet* in this test. The higher than 99% catch rates on all the spam, malware and phishing samples, and the lack of both ham and newsletter false positives show *Fortinet* to be a balanced and reliable solution.

N-able Mail Assure

SC rate: 99.82%
FP rate: 0.00%
Final score: 99.82
Malware catch rate: 100.00%
Phishing catch rate: 98.58%
Project Honey Pot SC rate: 99.61%
Abusix SC rate: 99.85%
MXMailData SC rate: 100.00%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●



The third test of 2022 brings *N-able Mail Assure* its third VBSpam+ certification. It is one of the four products in this test that managed to block all the malware samples. We also highlight the solution's high spam catch rate and the lack of false positives.

N-able SpamExperts

SC rate: 99.82%
FP rate: 0.00%
Final score: 99.82
Malware catch rate: 100.00%
Phishing catch rate: 98.58%



Project Honey Pot SC rate: 99.61%

Abusix SC rate: 99.85%

MXMailData SC rate: 100.00%

Newsletters FP rate: 0.0%

Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

SpamExperts – which is *N-able*'s solution for web hosts and ISPs – is a new entry in this test. On its debut it put in an excellent performance, checking all the boxes to earn a VBSpam+ award.

Rspamd

SC rate: 97.29%

FP rate: 0.46%

Final score: 94.86

Malware catch rate: 70.00%

Phishing catch rate: 89.28%

Project Honey Pot SC rate: 95.86%

Abusix SC rate: 98.11%

MXMailData SC rate: 62.78%

Newsletters FP rate: 4.1%

Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Even though *Rspamd*'s scores fall below the certification threshold, the open-source solution impresses once again in this test with a very decent spam catch rate. The malware samples were a challenge, but overall the results are promising.

SEPPmail.cloud Filter

SC rate: 99.98%

FP rate: 0.05%

Final score: 99.61

Malware catch rate: 100.00%

Phishing catch rate: 99.87%

Project Honey Pot SC rate: 99.83%

Abusix SC rate: 100.00%

MXMailData SC rate: 100.00%

Newsletters FP rate: 3.1%

Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

In this test we saw *SEPPmail* scoring the highest spam catch rate and blocking all the malware samples. Only three phishing emails evaded the product's filters and it earns a VBSpam award with ease.



Spamhaus Data Query Service (DQS) + SpamAssassin

SC rate: 99.61%

FP rate: 0.05%

Final score: 99.38

Malware catch rate: 89.39%

Phishing catch rate: 99.69%

Project Honey Pot SC rate: 99.31%

Abusix SC rate: 99.90%

MXMailData SC rate: 85.24%

Newsletters FP rate: 0.0%

Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Spamhaus Data Query Service + SpamAssassin is a custom configured solution that integrates the *Spamhaus DQS DNSBL* service and the free open-source solution *SpamAssassin*. In this test the solution showed a balanced performance and is awarded a VBSpam certification.



Zoho Mail

SC rate: 99.17%

FP rate: 0.18%

Final score: 98.14

Malware catch rate: 87.71%

Phishing catch rate: 98.76%

Project Honey Pot SC rate: 99.48%

Abusix SC rate: 99.40%

MXMailData SC rate: 83.04%

Newsletters FP rate: 3.1%

Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

In this test *Zoho Mail* earns a VBSpam certification. The solution scored well on the overall spam catch rate, higher than 99%. We continue to see a good performance on the phishing samples as well, with a 98.76% catch rate this time.



Abusix Mail Intelligence

SC rate: 98.69%

FP rate: 0.14%

Final score: 98.01

Malware catch rate: 72.37%

Phishing catch rate: 97.82%

Project Honey Pot SC rate: 97.27%

Abusix SC rate: 99.51%

MXMailData SC rate: 63.43%

Newsletters FP rate: 0.0%

Abusix Mail Intelligence is a set of blocklists that is tested as a partial solution because it has access only to parts of the emails (IP addresses, domains, URLs), which are queried to their DNS zones. With this setup, a spam catch rate of 98.69% and only one ham false positive is very impressive.

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 6 August to 12am on 22 August 2022 (GMT).

The test corpus consisted of 110,057 emails. 107,763 of these were spam, 14,798 of which were provided by *Project Honey Pot*, 91,420 were provided by *Abusix*, with the remaining 1,545 spam emails provided by *MXMailData*. There were 2,197 legitimate emails ('ham') and 97 newsletters, a category that includes various kinds of commercial and non-commercial opt-in mailings.

55 emails in the spam corpus were considered 'unwanted' (see the June 2018 report²) and were included with a weight of 0.2; this explains the non-integer numbers in some of the tables.

Moreover, 2,197 emails from the spam corpus were found to contain a malicious attachment while 2,249 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 command³.

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.

² <https://www.virusbulletin.com/virusbulletin/2018/06/vbspam-comparative-review>.

³ http://www.postfix.org/XCLIENT_README.html

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:

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

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.

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

© 2022 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	2197	0	0.00%	24.2	107694.8	99.98%	99.98	
Cleanmail Domain Gateway	2196	1	0.05%	69.4	107649.6	99.94%	99.71	
FortiMail	2197	0	0.00%	31.2	107687.8	99.97%	99.97	
N-able Mail Assure	2197	0	0.00%	197.4	107521.6	99.82%	99.82	
N-able SpamExperts	2197	0	0.00%	198.4	107520.6	99.82%	99.82	
Rspamd	2187	10	0.46%	2914.6	104804.4	97.29%	94.86	
SEPPmail.cloud Filter	2196	1	0.05%	26.6	107692.4	99.98%	99.61	
Spamhaus Data Query Service (DQS) + SpamAssassin [‡]	2196	1	0.05%	420	107299	99.61%	99.38	
Zoho Mail	2193	4	0.18%	889.2	106829.8	99.17%	98.14	
Abusix Mail Intelligence*	2194	3	0.14%	1415.8	106303.2	98.69%	98.01	N/A

[‡]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.

*This product is a partial solutions and its performance should not be compared with that of other products.

(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	0	0.0%	0	100.00%	1	99.96%	2	99.99%	22.2	99.98%	0	100.00%	0.14
Cleanmail Domain Gateway	0	0.0%	2	99.91%	25	98.89%	8.6	99.94%	58.8	99.94%	2	99.87%	0.28
FortiMail	0	0.0%	6	99.73%	4	99.82%	7	99.95%	18.2	99.98%	6	99.61%	0.17
N-able Mail Assure	0	0.0%	0	100.00%	32	98.58%	58	99.61%	139.4	99.85%	0	100.00%	0.5
N-able SpamExperts	0	0.0%	0	100.00%	32	98.58%	58	99.61%	140.4	99.85%	0	100.00%	0.5
Rspamd	4	4.1%	659	70.00%	241	89.28%	611.4	95.86%	1728.2	98.11%	575	62.78%	3.15
SEPPmail.cloud Filter	3	3.1%	0	100.00%	3	99.87%	24.6	99.83%	2	99.998%	0	100.00%	0.17
Spamhaus Data Query Service (DQS) + SpamAssassin‡	0	0.0%	233	89.39%	7	99.69%	102	99.31%	90	99.90%	228	85.24%	0.97
Zoho Mail	3	3.1%	270	87.71%	28	98.76%	77	99.48%	550.2	99.40%	262	83.04%	1.58
Abusix Mail Intelligence*	0	0.0%	607	72.37%	49	97.82%	402.8	97.27%	448	99.51%	565	63.43%	2.28

† 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.

* This product is a partial solution and its performance should not be compared with that of other products. None of the queries to the IP blocklist included any information on the attachments; hence its performance on the malware corpus is added purely for information. (Please refer to the text for full product names and details.)

	Speed			
	10%	50%	95%	98%
Bitdefender	●	●	●	●
Cleanmail Domain Gateway	●	●	●	●
FortiMail	●	●	●	●
N-able Mail Assure	●	●	●	●
N-able SpamExperts	●	●	●	●
Rspamd	●	●	●	●
SEPPmail.cloud Filter	●	●	●	●
Spamhaus Data Query Service (DQS) + SpamAssassin [‡]	●	●	●	●
Zoho Mail	●	●	●	●

● 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.)

[‡]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.

Products ranked by final score	
Bitdefender	99.98
FortiMail	99.97
N-able Mail Assure	99.82
N-able SpamExperts	99.82
Cleanmail Domain Gateway	99.71
SEPPmail.cloud Filter	99.61
Spamhaus Data Query Service (DQS) + SpamAssassin [‡]	99.38
Zoho Mail	98.14
Abusix Mail Intelligence [*]	98.01
Rspamd	94.86

[‡]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.

^{*}This product is a partial solution and its performance should not be compared with that of other products.

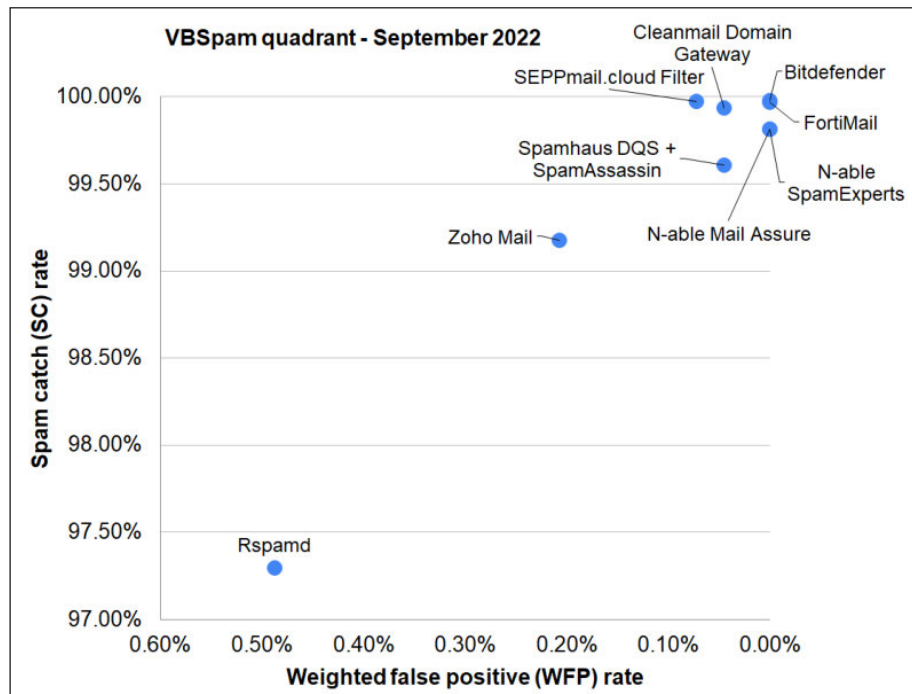
Hosted solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Multiple MX-records	Multiple locations
Cleanmail Domain Gateway	Cleanmail		√	√	√	√	
N-able Mail Assure	N-able Mail Assure	√	√	√	√		
N-able SpamExperts	SpamExperts	√	√	√	√		
SEPPmail.cloud Filter	SEPPmail	√	√	√	√	√	√
Zoho Mail	Zoho		√	√	√	√	√

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

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

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

[‡]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.)