MARCH 2023

virus BULLETIN

Covering the global threat landscape

VBSPAM EMAIL SECURITY COMPARATIVE REVIEW MARCH 2023

Ionuţ Răileanu & Adrian Luca

In the Q1 2023 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tested opted to be included in the public test, the rest opting for private testing (all details and results remaining unpublished).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: eight full email security solutions, one custom configured solution[1], one open-source solution and one blocklist.

For the majority of the solutions we tested, more than 99% of spam emails didn't pose any challenge. The difference came in the ability of the filters to be fine-tuned in order to avoid false positives.

While threat actors continue to take advantage of legitimate public services such as social media URL shortenings and unusual malicious *OneNote* attachments, we saw quick response times from the security solutions in blocking these threats.

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.)*

[1] *Spamhaus DQS* is a custom solution built on top of the *SpamAssassin* open-source anti-spam platform.

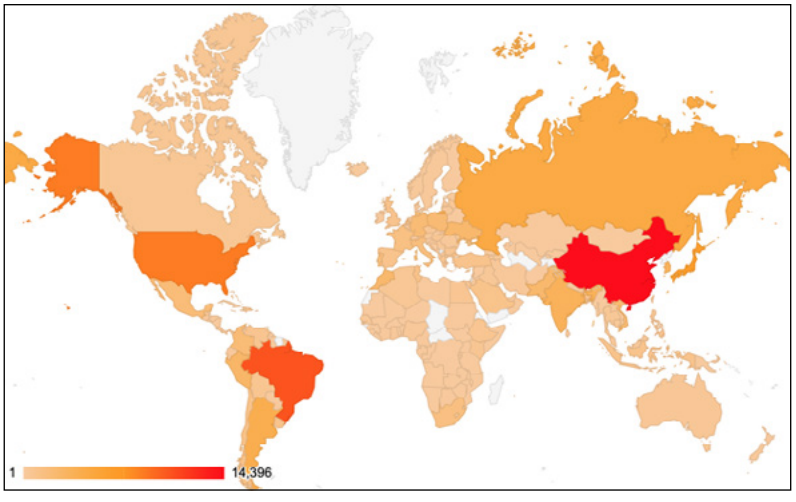
HIGHLIGHTS

OneNote malware campaign

In this quarter, and during the time the test ran, we observed an active malicious campaign of emails with .one files attached. Whilst both the number and variation of these

#	Sender's IP country	Percentage of spam
1	China	12.00%
2	Brazil	8.72%
3	United States	7.13%
4	Japan	5.43%
5	Russian Federation	3.84%
6	Argentina	3.33%
7	India	2.85%
8	Republic of Korea	2.69%
9	Peru	2.25%
10	Morocco	2.04%

Top 10 countries from which spam was sent.

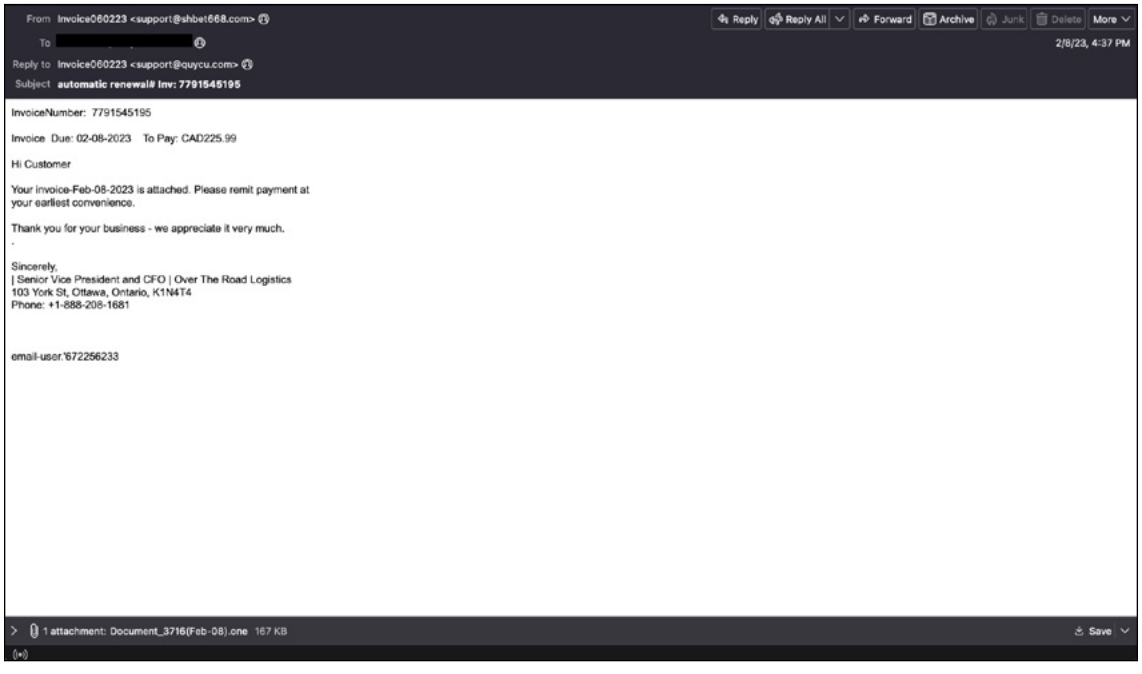


Geographical distribution of spam based on sender IP address.

ISSN 1749-7027

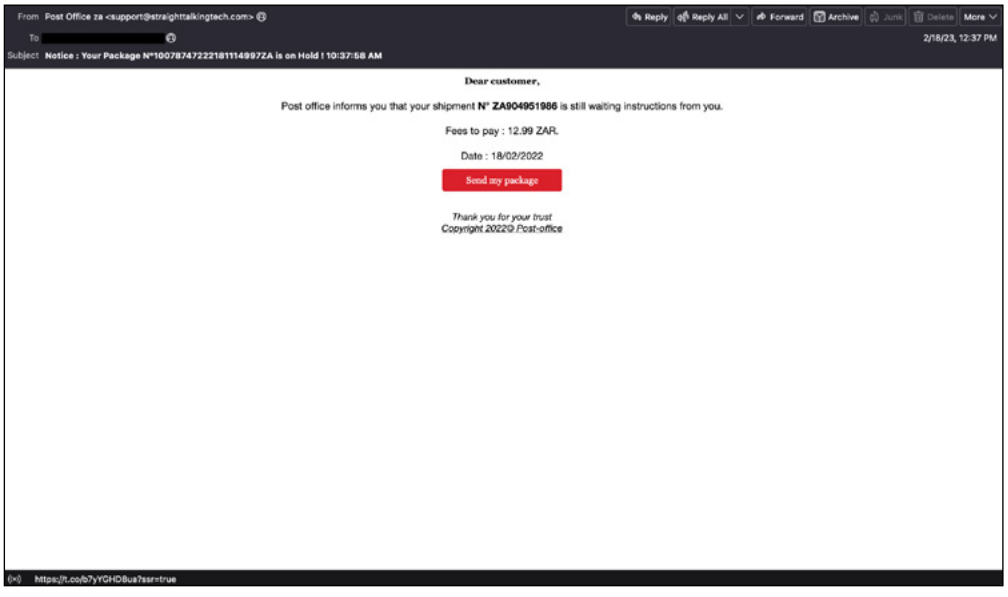
samples were unusual, the way the user was tricked into accessing the malicious payload was always the same: an image overlaying links to different kinds of executables, shortcut (LNK) files, or script files such as HTML application (HTA) or Windows script files (WSF).

For the solutions participating in the test this was the most challenging malware campaign encountered during the whole of the test period. However, the challenge came only at the beginning of the campaign, after which the products became more adept at blocking it.



Malspam email with a malicious .one file attached.

OneNote file with the .hta files hidden under an overlaid image resembling a button.



Phishing email using social media shortening URL.

Social media URL shortening phishing

We have seen this kind of phishing campaign before, but the use of social media shortening URLs continues to make it challenging for the filters to block an email before it reaches the user's inbox.

We saw a few samples of this kind, each coming from a different IP address. We were unable to find a link between this campaign and any particular threat actor. However, it is highlighted here because it was the most commonly missed phish in this test.

- **Subjects**:
  `Notice : Your Package N<U+FFFD>10078747222181114997ZA is on Hold ! 10:37:58 AM`
  `Notice : Your Package N<U+FFFD>53784568613487413211ZA is on Hold ! 02:17:49 AM`
- **From**:
  `Post Office za <support@straighttalkingtech[.]com>`
  `Customer Support <techsupport@ask4key[.]com>`
- **Email URLs**:
  `hxxps://t[.]co/b7yYGHD8ua?ssr=true`
  `hxxps://t[.]co/kVolpyNxzB?ssr=true`
- **Landing URLs**:
  `https://postofficce[.]page[.]link/XktS`
  `https://postofficesouthafrican[.]page[.]link/rniX`

RESULTS

The majority of the tested solutions managed to achieve spam catch rates of over 99%. A better comparison between the products can be made by analysing their malware and phishing catch rates, both of which are subsets of the spam corpus. Here we highlight the performance of *Fortinet*, *Mimecast*, *N-able Mail Assure*, *N-able SpamExperts* and *SEPPmail*, all of which achieved a 100% malware catch rate, and *Fortinet* blocked 100% of phishing samples as well.

Of the participating full solutions, two – *SEPPmail.cloud Filter* and *Zoho Mail* – achieved a VBSpam award, while six – *Bitdefender GravityZone Premium*, *Cleanmail Domain Gateway*, *FortiMail*, *Mimecast*, *N-able Mail Assure* and *N-Able SpamExperts* – plus the custom configured solution *Spamhaus DQS + SpamAssassin* were awarded VBSpam+ certification.

Bitdefender GravityZone Premium

SC rate: 99.97%
FP rate: 0.00%
Final score: 99.97
Malware catch rate: 99.88%
Phishing catch rate: 99.98%
Project Honey Pot SC rate: 100.00%
Abusix SC rate: 99.97%
MXMailData SC rate: 99.88%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

It was another great performance from *Bitdefender*, this time with the version of the solution for *Exchange* servers. The lack of false positives and a final score of 99.97 easily secures the product a VBSpam+ certification.

Cleanmail Domain Gateway

SC rate: 99.81%
FP rate: 0.00%
Final score: 99.81
Malware catch rate: 98.39%
Phishing catch rate: 98.83%
Project Honey Pot SC rate: 99.91%
Abusix SC rate: 99.86%
MXMailData SC rate: 96.34%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Cleanmail kicks off the 2023 VBSpam testing series with a VBSpam+ award. A solid 99.81% spam catch rate and no false positives of any kind confirms that the Swiss-based solution can be considered a reliable one.

Fortinet FortiMail

SC rate: 99.98%
FP rate: 0.00%
Final score: 99.98
Malware catch rate: 100.00%
Phishing catch rate: 100.00%
Project Honey Pot SC rate: 99.90%
Abusix SC rate: 99.99%
MXMailData SC rate: 100.00%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

It was another impressive performance from *Fortinet*. With no malware or phishing samples missed, no false positives, and a 99.98% spam catch rate, a VBSpam+ award was earned with ease.

Mimecast

SC rate: 99.88%
FP rate: 0.00%
Final score: 99.85
Malware catch rate: 100.00%
Phishing catch rate: 99.93%
Project Honey Pot SC rate: 99.64%
Abusix SC rate: 99.91%
MXMailData SC rate: 100.00%
Newsletters FP rate: 1.2%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Not a single malware email passed *Mimecast*'s filters in this test. Combined with a 99.88% spam catch rate and no false positives, the product earns a VBSpam+ award.

N-able Mail Assure

SC rate: 99.90%
FP rate: 0.00%
Final score: 99.90
Malware catch rate: 100.00%
Phishing catch rate: 99.74%
Project Honey Pot SC rate: 99.91%
Abusix SC rate: 99.89%
MXMailData SC rate: 100.00%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

It was another great performance by *N-able Mail Assure* in the Q1 2023 test. With a 100% malware catch rate, higher than 99% phishing catch rate and no ham or newsletter samples blocked, *N-able Mail Assure* is awarded a VBSpam+ certification.

N-able SpamExperts

SC rate: 99.90%
FP rate: 0.00%
Final score: 99.90
Malware catch rate: 100.00%
Phishing catch rate: 99.74%
Project Honey Pot SC rate: 99.91%
Abusix SC rate: 99.89%
MXMailData SC rate: 100.00%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

It was the same story for *N-able*'s second entry in this test, *SpamExperts*: a 100% malware catch rate, higher than 99% phishing catch rate, no ham or newsletter samples blocked, and another VBSpam+ certification awarded.

Rspamd

SC rate: 96.02%
FP rate: 0.47%
Final score: 93.47
Malware catch rate: 74.87%

Phishing catch rate: 94.43%
Project Honey Pot SC rate: 91.95%
Abusix SC rate: 96.93%
MXMailData SC rate: 72.46%
Newsletters FP rate: 7.3%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Rspamd achieved a higher than 95% spam catch rate while blocking more than 90% of the phishing samples. The open-source solution was challenged by the malware samples but we saw an improvement in the product's overall performance since the last test.

SEPPmail.cloud Filter

SC rate: 99.99%
FP rate: 0.11%
Final score: 99.31
Malware catch rate: 100.00%
Phishing catch rate: 99.98%
Project Honey Pot SC rate: 99.96%
Abusix SC rate: 99.998%
MXMailData SC rate: 100.00%
Newsletters FP rate: 4.9%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

SEPPmail's solution achieved the highest spam catch rate in this test, with only seven samples missed. Some false positives brought the final score down a little, but the product earns a VBSpam award with ease.

Spamhaus Data Query Service + SpamAssassin

SC rate: 99.74%
FP rate: 0.00%
Final score: 99.74
Malware catch rate: 98.43%
Phishing catch rate: 99.70%
Project Honey Pot SC rate: 99.95%
Abusix SC rate: 99.74%
MXMailData SC rate: 98.23%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Spamhaus SpamAssassin Data Query Service (*DQS*) is a custom configured solution that integrates the *Spamhaus DQS DNSBL* service and the free open-source solution *SpamAssassin*. In this test no ham or newsletter sample was blocked by the combined solution. With a final score of 99.74 the product easily earns a VBSpam+ certification.

Zoho Mail

SC rate: 99.54%
FP rate: 0.00%
Final score: 99.40
Malware catch rate: 99.76%
Phishing catch rate: 98.69%
Project Honey Pot SC rate: 99.00%
Abusix SC rate: 99.61%
MXMailData SC rate: 99.59%
Newsletters FP rate: 4.9%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Zoho Mail scored well on the overall spam catch rate. We saw a strong performance on the malware corpus, with 99.76% of samples blocked, and a lack of ham false positives. The product earns a VBSpam award.

Abusix Mail Intelligence

SC rate: 98.45%
FP rate: 0.00%
Final score: 98.42
Malware catch rate: 76.96%
Phishing catch rate: 98.23%
Project Honey Pot SC rate: 91.76%
Abusix SC rate: 99.80%
MXMailData SC rate: 68.57%
Newsletters FP rate: 1.2%

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, the solution's 98.45% spam catch rate and lack of ham false positives is commendable.

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 February to 12am on 20 February 2023 (GMT).

The test corpus consisted of 122,862 emails. 120,012 of these were spam, 13,581 of which were provided by *Project Honey Pot*, 104,735 were provided by *Abusix* with the remaining 1,696 spam emails provided by *MXMailData*. There were 2,768 legitimate emails ('ham') and 82

newsletters, a category that includes various kinds of commercial and non-commercial opt-in mailings.

61 emails in the spam corpus were considered 'unwanted' (see the June 2018 report[2]) and were included with a weight of 0.2; this explains the non-integer numbers in some of the tables.

Moreover, 2,483 emails from the spam corpus were found to contain a malicious attachment while 4,290 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 command[3].

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:

WFP rate = (#false positives + 0.2 * min(#newsletter false positives , 0.2 * #newsletters)) / (#ham + 0.2 * #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:

Final score = SC - (5 x 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.

[2] https://www.virusbulletin.com/virusbulletin/2018/06/vbspam-comparative-review.

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

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

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	2768	0	0.00%	37	119926.2	99.97%	99.97	SPAM + Verified
Cleanmail Domain Gateway	2768	0	0.00%	225	119738.2	99.81%	99.81	SPAM + Verified
Fortinet FortiMail	2768	0	0.00%	25	119938.2	99.98%	99.98	SPAM + Verified
Mimecast	2768	0	0.00%	141.2	119822	99.88%	99.85	SPAM + Verified
N-able Mail Assure	2768	0	0.00%	124.2	119839	99.90%	99.90	SPAM + Verified
N-able SpamExperts	2768	0	0.00%	124.2	119839	99.90%	99.90	SPAM + Verified
Rspamd	2755	13	0.47%	4773.2	115190	96.02%	93.47	
SEPPmail.cloud Filter	2765	3	0.11%	7	119956.2	99.99%	99.31	SPAM Verified
Spamhaus DQS + SpamAssassin‡	2768	0	0.00%	307.4	119655.8	99.74%	99.74	SPAM + Verified
Zoho Mail	2768	0	0.00%	552	119411.2	99.54%	99.40	SPAM Verified
Abusix Mail Intelligence*	2768	0	0.00%	1853.8	118109.4	98.45%	98.42	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 SpamAssasssin. 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.*

(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%	3	99.88%	1	99.98%	0	100.00%	35	99.97%	2	99.88%	0.21
Cleanmail Domain Gateway	0	0.0%	40	98.39%	50	98.83%	12	99.91%	151	99.86%	62	96.34%	1.59
Fortinet FortiMail	0	0.0%	0	100.00%	0	100.00%	14	99.90%	11	99.99%	0	100.00%	0.21
Mimecast	1	1.2%	0	100.00%	3	99.93%	49.2	99.64%	92	99.91%	0	100.00%	0.78
N-able Mail Assure	0	0.0%	0	100.00%	11	99.74%	12	99.91%	112.2	99.89%	0	100.00%	0.66
N-able SpamExperts	0	0.0%	0	100.00%	11	99.74%	12	99.91%	112.2	99.89%	0	100.00%	0.66
Rspamd	6	7.3%	624	74.87%	239	94.43%	1090.8	91.95%	3215.4	96.93%	467	72.46%	5.83
SEPPmail.cloud Filter	4	4.9%	0	100.00%	1	99.98%	5	99.96%	2	99.998%	0	100.00%	0.14
Spamhaus DQS + SpamAssassin‡	0	0.0%	39	98.43%	13	99.70%	7.2	99.95%	270.2	99.74%	30	98.23%	0.77
Zoho Mail	4	4.9%	6	99.76%	56	98.69%	135.4	99.00%	409.6	99.61%	7	99.59%	1.33
Abusix Mail Intelligence*	1	1.2%	572	76.96%	76	98.23%	1115.8	91.76%	205	99.80%	533	68.57%	3.66

† *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 SpamAssasssin. 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 GravityZone Premium	🟢	🟢	🟢	🟢
Cleanmail Domain Gateway	🟢	🟢	🟢	🟢
Fortinet FortiMail	🟢	🟢	🟢	🟢
Mimecast	🟢	🟢	🟢	🟢
N-able Mail Assure	🟢	🟢	🟢	🟢
N-able SpamExperts	🟢	🟢	🟢	🟢
Rspamd	🟢	🟢	🟢	🟢
SEPPmail.cloud Filter	🟢	🟢	🟢	🟡
Spamhaus 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 SpamAssasssin. 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	
Fortinet FortiMail	99.98
Bitdefender GravityZone Premium	99.97
N-able Mail Assure	99.90
N-able SpamExperts	99.90
Mimecast	99.85
Cleanmail Domain Gateway	99.81
Spamhaus DQS + SpamAssassin‡	99.74
Zoho Mail	99.40
SEPPmail.cloud Filter	99.31
Rspamd	93.47

‡*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 SpamAssasssin. The test set up reflects the real-life performance expected from this combined production deployment, not as individual product elements.*

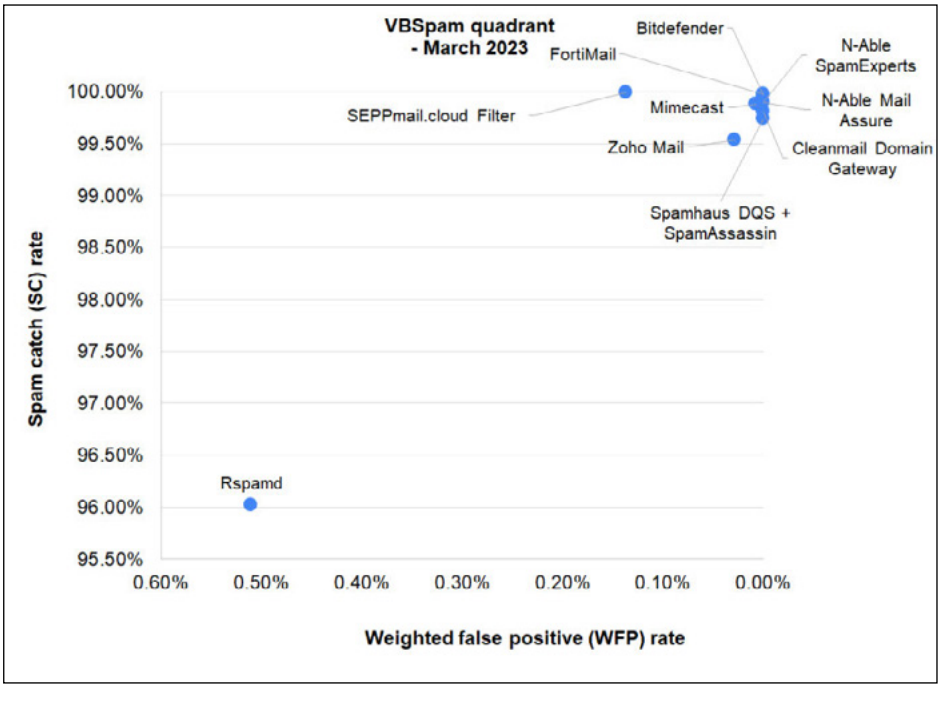
Hosted solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Multiple MX-records	Multiple locations
Cleanmail Domain Gateway	Cleanmail		√	√	√	√	
Mimecast	Mimecast		√	√	√	√	√
N-able Mail Assure	N-able Mail Assure	√	√	√	√		
N-able SpamExperts	SpamExperts	√	√	√	√		
SEPPmail.cloud Filter	SEPPmail	√	√	√	√	√	√
Zoho Mail	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 GravityZone Premium	Bitdefender	√				√		√	√
FortiMail	Fortinet	√	√	√	√	√		√	√
Rspamd	None					√			
Spamhaus 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 SpamAssasssin. 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.)