MARCH 2025

virus BULLETIN

Covering the global threat landscape

VBSPAM EMAIL SECURITY COMPARATIVE REVIEW MARCH 2025

Ionuţ Răileanu & Adrian Luca

In the Q1 2025 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tested opted to be included in the public test, the rest opting for private testing (all details and results remaining unpublished).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 – and included in this report – were 11 full email security solutions and one open-source solution.

The email security solutions assessed in this evaluation showed solid performance against spam and malware, with some minor disparities in their phishing detection efficacy. Although perfect phishing detection was not attained by any solution in the test, three of them exhibited near-flawless performance, each failing to detect only one sample. Phishing attacks – especially those directed at non-English-language demographics – remain a considerable challenge for the products.

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

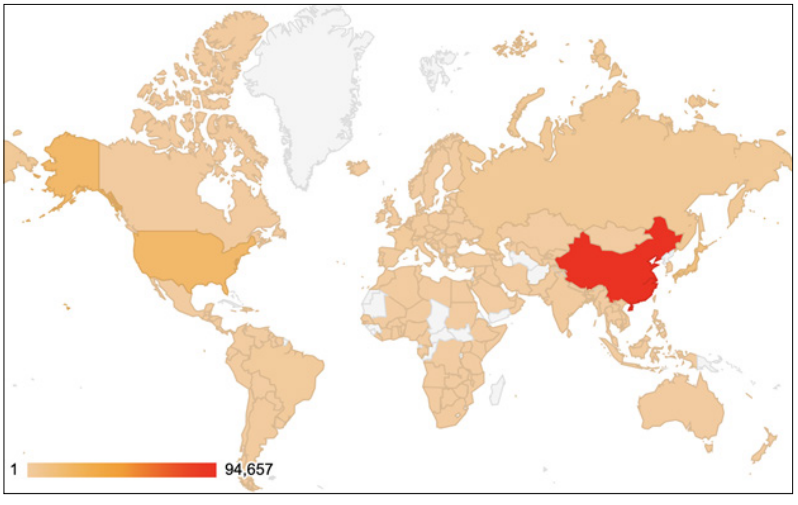
AMTSO STANDARD COMPLIANCE

This test was executed in accordance with the AMTSO Standard of the Anti-Malware Testing Standards Organization.

[1] For a number of samples (5,836 spam samples; 3.72% of the total) we were unable to find data about geographical location based on IP address.

#	Sender's IP country	Percentage of spam
1	China	60.30%
2	United States	12.63%
3	Japan	6.69%
4	Russian Federation	2.35%
5	France	1.14%
6	Brazil	1.12%
7	Argentina	0.73%
8	Germany	0.56%
9	India	0.56%
10	Vietnam	0.49%

Top 10 countries from which spam was sent.



Geographical distribution of spam based on sender IP address.

ISSN 1749-7027

The compliance status can be verified on the AMTSO website:

- **AMTSO Test ID**: AMTSO-LS1-TP139
- **Link**: https://www.amtso.org/tests/virus-bulletin-vbspam-q1-2025/

HIGHLIGHTS

Non-English phishing

Phishing emails that bypass security filters are predominantly written in languages other than English. These non-English phishing emails are found infrequently within the spam corpus, which makes it a significant challenge for the security solutions to detect and block them in a timely manner.

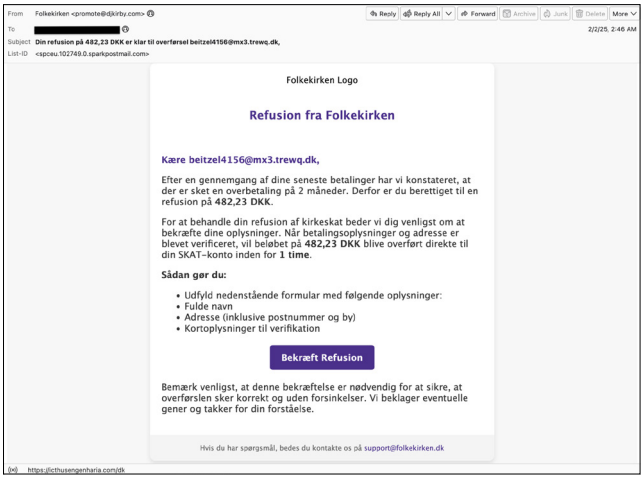
Some examples of the phishing emails that evaded most of the filters are shown below, targeting Danish, German, Italian and Portuguese speakers.

PureCrypter malware

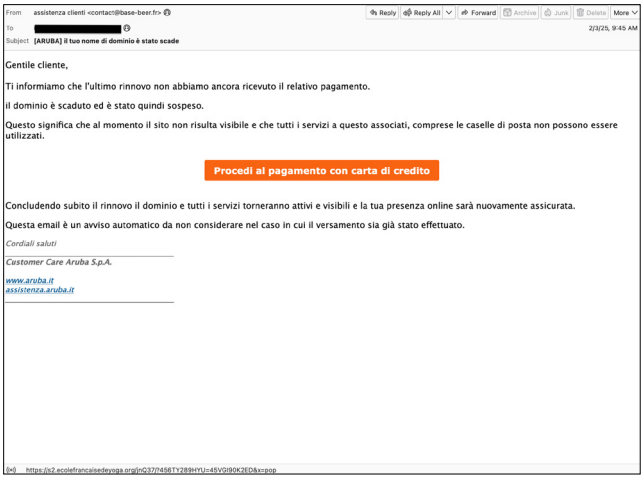
Two similar malware samples caught our attention because they were missed by most of the tested solutions. In this case the emails contain a little text in French, were spotted on 5 February in a half-hour time window, and have a TGZ archive attachment (SHA256: `931ee3bf862d74b6b9407a0579b0cb71c4c85b07ccb670fe2e826daf46be77b7`). When unpacked, a 100MB EXE file is extracted.

Our analysis showed this malware to have similarities with the PureCrypter[2] malware.

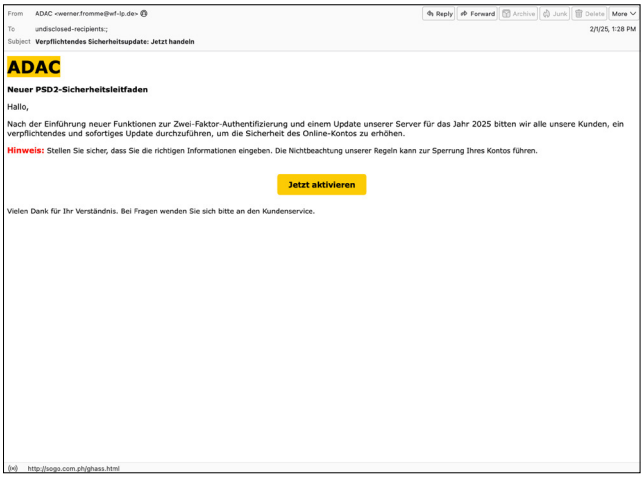
[2] https://any.run/malware-trends/purecrypter/



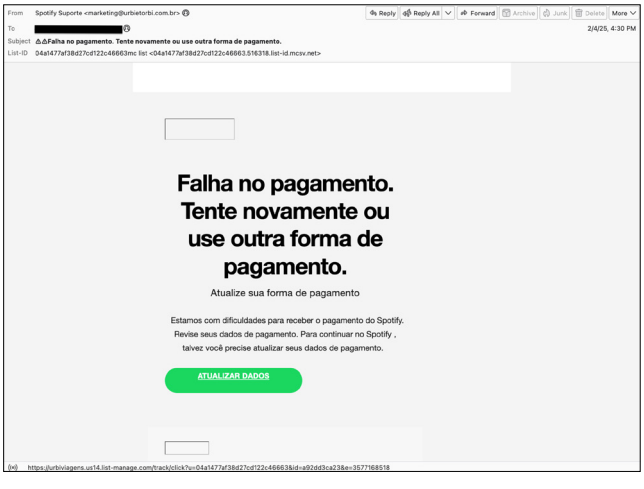
Danish phishing sample.



Italian phishing sample.



German phishing sample.



Portuguese phishing sample.

Email containing PureCrypter malware infected attachment.

Guloader malware

Another malware sample we observed during the test period targets Spanish-speaking users and contains a RAR attachment (SHA256: `f95652083ef6179f3342e53657a48ba88f57fc2bbc58fb77f7c2b927ecf3ec94`).

Our analysis showed that when unpacking the archive, an EXE file is extracted which further leads to Snake Keylogger.

Email containing Guloader malware infected attachment.

RESULTS

Of the participating full solutions, two achieved a VBSpam award: *SEPPmail.cloudfilter* and *Zoho Mail*, while eight – *Bitdefender GravityZone Premium*, *FortiMail*, *Mimecast*, *N-able Mail Assure*, *N-able SpamExperts*, *Net At Work NoSpamProxy*, *Sophos Email* and *SpamTitan* – were awarded VBSpam+ certification.

(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 with three decimal places.)

Bitdefender GravityZone Premium

SC rate: 99.998%

FP rate: 0.00%

Final score: 99.998

Malware catch rate: 100.000%

Phishing catch rate: 99.999%

Project Honey Pot SC rate: 99.998%

Abusix SC rate: 100.000%

MXMailData SC rate: 100.000%

Newsletters FP rate: 0.0%

Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Continuing its unbroken record, *Bitdefender* attained VBSpam+ certification, showing impressive efficacy in identifying malware and phishing attempts, and with a final score of 99.998 and an absence of false positives.

Fortinet FortiMail

SC rate: 99.962%

FP rate: 0.00%

Final score: 99.962

Malware catch rate: 100.000%

Phishing catch rate: 99.950%

Project Honey Pot SC rate: 99.965%

Abusix SC rate: 99.947%

MXMailData SC rate: 99.970%

Newsletters FP rate: 0.0%

Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Fortinet exhibited a flawless detection rate for malware samples and accurately filtered all the legitimate feeds. Achieving a spam catch rate of 99.962% and maintaining optimal speed values across all parameters, the product earns VBSpam+ certification.

Mimecast

SC rate: 99.719%

FP rate: 0.00%

Final score: 99.719

Malware catch rate: 100.000%

Phishing catch rate: 99.950%

Project Honey Pot SC rate: 99.666%

Abusix SC rate: 99.930%

MXMailData SC rate: 100.000%

Newsletters FP rate: 0.0%

Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Mimecast demonstrated exceptional performance in the VBSpam test, correctly blocking all malicious samples, and achieving an impressive 99.95% success rate in blocking phishing attempts. With a complete absence of false

positives and a final score of 99.719, *Mimecast* once again earns VBSpam+ certification.

N-able Mail Assure

SC rate: 99.929%
FP rate: 0.00%
Final score: 99.929
Malware catch rate: 99.910%
Phishing catch rate: 99.960%
Project Honey Pot SC rate: 99.988%
Abusix SC rate: 99.580%
MXMailData SC rate: 100.000%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

N-able Mail Assure earns VBSpam+ certification for its exceptional and well-rounded performance, which included a 99.929% spam detection rate and an absence of false positives.

N-able SpamExperts

SC rate: 99.925%
FP rate: 0.00%
Final score: 99.925
Malware catch rate: 99.910%
Phishing catch rate: 99.960%
Project Honey Pot SC rate: 99.988%
Abusix SC rate: 99.580%
MXMailData SC rate: 99.900%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

With almost identical scores to its sister product, *N-able SpamExperts* also easily earns VBSpam+ certification in this test.

Net At Work NoSpamProxy

SC rate: 99.992%
FP rate: 0.00%
Final score: 99.992
Malware catch rate: 100.000%
Phishing catch rate: 99.990%
Project Honey Pot SC rate: 99.993%
Abusix SC rate: 99.982%
MXMailData SC rate: 100.000%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

NoSpamProxy attained an impressive final score of 99.992, and with no false positive it earns VBSpam+ certification. It also successfully blocked all malware samples and 99.99% of phishing attempts.

Rspamd

SC rate: 91.353%
FP rate: 0.57%
Final score: 88.524
Malware catch rate: 57.160%
Phishing catch rate: 93.850%
Project Honey Pot SC rate: 93.106%
Abusix SC rate: 92.613%
MXMailData SC rate: 56.340%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

The open-source *Rspamd* found dealing with the malware samples a challenge. However, we continue to see good performances from the solution on the overall spam corpus, in this case blocking more than 91% of the samples.

Rspamd Premium 3.10.2

SC rate: 98.996%
FP rate: 0.68%
Final score: 95.601
Malware catch rate: 98.580%
Phishing catch rate: 99.590%
Project Honey Pot SC rate: 98.914%
Abusix SC rate: 99.343%
MXMailData SC rate: 99.330%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

The upgraded *Rspamd* configuration significantly outperformed the basic version, successfully blocking 98.996% of spam samples and achieving a final score of 95.601.

SEPPmail.cloudfilter

SC rate: 99.997%
FP rate: 0.06%
Final score: 99.714
Malware catch rate: 100.000%
Phishing catch rate: 99.990%
Project Honey Pot SC rate: 99.996%
Abusix SC rate: 100.000%

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

SEPPmail.cloudfilter achieved a spam catch rate exceeding 99.99% and blocked all malware samples in this test. A single false positive prevented the solution from gaining VBSpam+ certification, but a VBSpam award is easily earned.

Sophos Email

SC rate: 99.993%
FP rate: 0.00%
Final score: 99.993
Malware catch rate: 100.000%
Phishing catch rate: 99.999%
Project Honey Pot SC rate: 99.995%
Abusix SC rate: 99.977%
MXMailData SC rate: 100.000%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Sophos achieved VBSpam+ certification in this test, with a final score of 99.993 and zero false positives. It also successfully blocked all malware samples and only missed one phishing sample.

SpamTitan

SC rate: 99.997%
FP rate: 0.00%
Final score: 99.997
Malware catch rate: 100.000%
Phishing catch rate: 99.999%
Project Honey Pot SC rate: 99.998%
Abusix SC rate: 99.996%
MXMailData SC rate: 100.000%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

SpamTitan demonstrated exceptional efficacy with only four misclassifications, one of which was a phishing attempt. The product's outstanding performance earns it VBSpam+ certification.

Zoho Mail

SC rate: 99.299%
FP rate: 0.00%
Final score: 99.299
Malware catch rate: 99.910%
Phishing catch rate: 99.690%
Project Honey Pot SC rate: 99.371%
Abusix SC rate: 98.739%
MXMailData SC rate: 99.800%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Zoho Mail demonstrated good performance across all test sets and exhibited no false positives. However, due to a spam catch rate falling short of 99.95% the solution misses out on VBSpam+ certification, but a VBSpam award is easily earned.

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-ver30/.

The test ran for 16 days, from 12am on 1 February to 12am on 17 February 2025 (GMT).

The test corpus consisted of 158,770 emails. 156,973 of these were spam, 126,950 of which were provided by *Project Honey Pot*, 22,845 were provided by *Abusix* with the remaining 7,178 spam emails provided by *MXMailData*. There were 1,760 legitimate emails ('ham') and 37 newsletters, a category that includes various kinds of commercial and non-commercial opt-in mailings.

13 emails in the spam corpus were considered 'unwanted' (see the June 2018 report[3]) and were included with a weight of 0.2; this explains the non-integer numbers in some of the tables.

Moreover, 1,055 emails from the spam corpus were found to contain a malicious attachment while 34,513 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[4].

[3] https://www.virusbulletin.com/virusbulletin/2018/06/vbspam-comparative-review
[4] http://www.postfix.org/XCLIENT_README.html

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.

Head of Testing: Peter Karsai
Security Test Engineers: Adrian Luca, Csaba Mészáros, Ionuţ Răileanu
Operations Manager: Bálint Tanos
Sales Executive: Allison Sketchley
Marketing: David Kelemen
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	1760	0	0.00%	3	156959.6	99.998%	99.998	SPAM + Verified
FortiMail	1760	0	0.00%	59	156903.6	99.962%	99.962	SPAM + Verified
Mimecast	1760	0	0.00%	440.6	156522	99.719%	99.719	SPAM + Verified
N-able Mail Assure	1760	0	0.00%	111	156851.6	99.929%	99.929	SPAM + Verified
N-able SpamExperts	1760	0	0.00%	118	156844.6	99.925%	99.925	SPAM + Verified
Net At Work NoSpamProxy	1760	0	0.00%	13	156949.6	99.992%	99.992	SPAM + Verified
Rspamd	1750	10	0.57%	13572.6	143390	91.353%	88.524	
Rspamd Premium	1748	12	0.68%	1576.6	155386	98.996%	95.601	
SEPPmail.cloudfilter	1759	1	0.06%	5	156957.6	99.997%	99.714	SPAM Verified
Sophos Email	1760	0	0.00%	11.2	156951.4	99.993%	99.993	SPAM + Verified
SpamTitan	1760	0	0.00%	4	156958.6	99.997%	99.997	SPAM + Verified
Zoho Mail	1760	0	0.00%	1100.6	155862	99.299%	99.299	SPAM Verified

	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	0.00%	0	100.000%	1	99.999%	3	99.998%	0	100.000%	0	100.000%	0.06
FortiMail	0	0.00%	0	100.000%	17	99.950%	45	99.965%	12	99.947%	2	99.970%	0.6
Mimecast	0	0.00%	0	100.000%	18	99.950%	424.6	99.666%	16	99.930%	0	100.000%	1
N-able Mail Assure	0	0.00%	1	99.910%	13	99.960%	15	99.988%	96	99.580%	0	100.000%	0.42
N-able SpamExperts	0	0.00%	1	99.910%	13	99.960%	15	99.988%	96	99.580%	7	99.900%	0.43
Net At Work NoSpamProxy	0	0.00%	0	100.000%	3	99.990%	9	99.993%	4	99.982%	0	100.000%	0.07
Rspamd	0	0.00%	452	57.160%	2121	93.850%	8751.6	93.106%	1687	92.613%	3134	56.340%	7.47
Rspamd Premium	0	0.00%	15	98.580%	141	99.590%	1378.6	98.914%	150	99.343%	48	99.330%	1.4
SEPPmail.cloudfilter	0	0.00%	0	100.000%	3	99.990%	5	99.996%	0	100.000%	0	100.000%	0.05
Sophos Email	0	0.00%	0	100.000%	1	99.999%	6	99.995%	5.2	99.977%	0	100.000%	0.11
SpamTitan	0	0.00%	0	100.000%	1	99.9990%	3	99.998%	1	99.996%	0	100.000%	0.06
Zoho Mail	0	0.00%	1	99.910%	106	99.690%	798.6	99.371%	288	98.739%	14	99.800%	3.09

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

	Speed			
	10%	**50%**	**95%**	**98%**
Bitdefender GravityZone Premium	●	●	●	●
FortiMail	●	●	●	●
Mimecast	●	●	●	●
N-able Mail Assure	●	●	●	●
N-able SpamExperts	●	●	●	●
Net At Work NoSpamProxy	●	●	●	●
Rspamd	●	●	●	●
Rspamd Premium	●	●	●	●
SEPPmail.cloudfilter	●	●	●	●
Sophos Email	●	●	●	●
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	
Bitdefender GravityZone Premium	99.998
SpamTitan	99.997
Sophos Email	99.993
Net At Work NoSpamProxy	99.992
FortiMail	99.962
N-able Mail Assure	99.929
N-able SpamExperts	99.925
Mimecast	99.719
SEPPmail.cloudfilter	99.714
Zoho Mail	99.299
Rspamd Premium	95.601
Rspamd	88.524

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		√	√	√	√	√
Rspamd Premium	ClamAV		√	√	√	√	√
SEPPmail.cloudfilter	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					√