JULY 2016

virus BULLETIN

Covering the global threat landscape

# VBSPAM COMPARATIVE REVIEW JULY 2016

*Martijn Grooten & Ionuţ Răileanu*

## INTRODUCTION

The spam problem is mostly solved.

Most spam doesn't even get sent – it gets blocked by outbound SMTP filters, or 'suffers' from various takedown efforts – and of those spam emails that do get sent, spam filters (or, as they are commonly called these days, email security solutions) block most of them[1].

That is great news (something there isn't too much of in the world of information security). But even for the spammers, there isn't necessarily any bad news: given the large volumes of messages sent in their campaigns, even if just one per cent of the emails make it into users' inboxes, that makes their campaign a huge success.

Although further steps may need to be taken for the spam to be converted into financial gain – an attachment opened, ransomware downloaded, a ransom paid – each of which is a further hurdle that sees the success rate drop significantly, there is still enough to make the campaign worth it. Spam remains very profitable.

For the users who open those attachments, and who click through subsequent warnings, spam can be very costly. And for those users, and the IT managers of their companies, there will always be the need for email security solutions.

The VBSpam test is designed to measure the accuracy of such filters, and this month, we put 17 full email security solutions to the test, together with four DNS-based blacklists. All 17 products achieved a VBSpam award for their efforts, with no fewer than nine of them performing well enough to achieve a VBSpam+ award.

[1] Well over 99 per cent in these tests, but that number is to be taken in the context of the test. In a real-life scenario, with more hard to define 'grey' email, the number is likely to be lower, albeit still well over 95 per cent.

## THE TEST SET-UP

The VBSpam test methodology can be found at https://www.virusbulletin.com/testing/vbspam/vbspam-methodology/. As usual, emails were sent to the products in parallel and in real time, and products were given the option to block email pre-DATA (that is, based on the SMTP envelope and before the actual email was sent). However, on this occasion no products chose to make use of this option.

For those products running on our equipment, we use *Dell PowerEdge* machines. 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.

To compare the products, we calculate a 'final score', which 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)

**Final score** = SC - (5 x WFP)

Products earn VBSpam certification if the value of the final score is at least 98.

Meanwhile, products that combine a spam catch rate of 99.5% or higher with a lack of false positives and no more than 2.5% false positives among the newsletters earn a VBSpam+ award.

ISSN 1749-7027

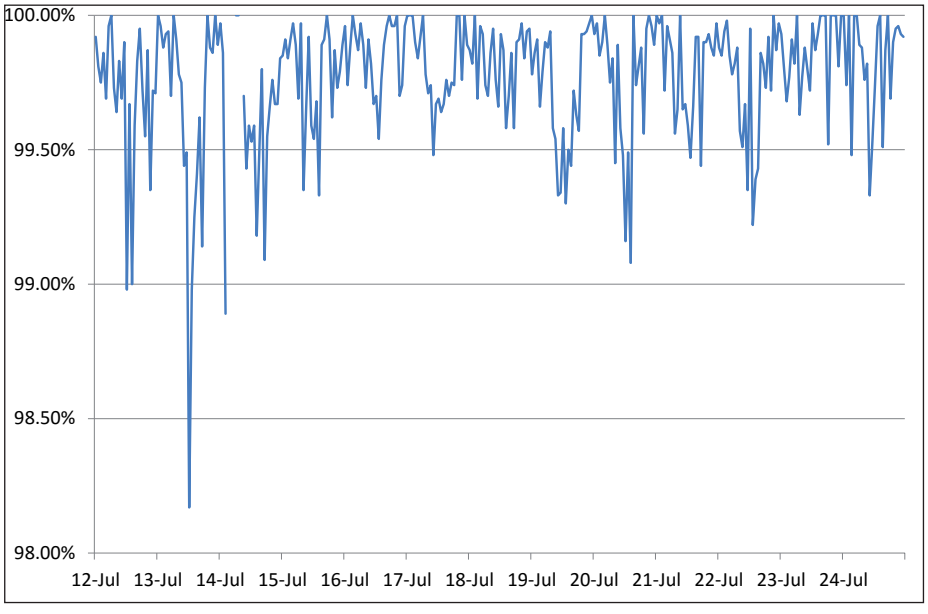



*Figure 1: Spam catch rate of all full solutions throughout the test period.*

Extra criteria based on the speed of delivery of emails in the ham corpus were not included on this occasion, as (like last time) we could not be 100 per cent confident about the accuracy of the speed measurements. However, we are confident that the awards achieved would have been unchanged had speed data been included. Moreover, we have now resolved these issues and the speed criteria will return in the next report.

## THE EMAIL CORPUS

In our tests, we measure the accuracy of email security products. We do so by hosting them in our lab[2] and sending emails from servers hosted in the same lab. As we take our role as a vendor-neutral tester seriously, we want to be as open as possible about this – and this is why, in the past, we have always made it clear when we have taken the decision to exclude a few hours' worth of emails from the test, for example because DNS issues led to sub-optimal network conditions.

A few issues plagued this test. First, it started a week later than planned as, having moved into a new lab in May/June, we weren't confident that the new lab was completely ready at the time the test was originally scheduled to start. Secondly, a number of issues with parsing the feeds from our spam providers led to a smaller than usual spam corpus. In particular, very few emails from *Abusix* made it to the final corpus, and very few emails from either provider were included for the first three days of the test; in these cases, we couldn't be absolutely certain that the emails sent through the products were exactly as they would have been received in the wild.

It should be noted that we have set up our lab in such a way that we can make the decision to exclude emails from the test without knowing what products will be affected. It should also be noted that the small size of the *Abusix* corpus in this test means that it is less easy to compare products' performance directly with those in previous tests – a fact that should be kept in mind.

With all these caveats, the test ran for 16 days, from 12am on 9 July until 12am on 25 July 2016.

The test corpus consisted of 65,679 emails. 58,054 of these were spam, 57,291 of which were provided by *Project Honey Pot*, with the remaining 763 spam emails provided by *spamfeed.me*, a product from *Abusix*. They were all relayed in real time, as were the 7,322 legitimate emails ('ham') and 303 newsletters.

Figure 1 shows the catch rate of all full solutions throughout the test, with the first three days excluded for reasons explained above. To avoid the average being skewed by poorly performing products, the highest and lowest catch rates have been excluded for each hour.

Looking at the spam corpus, we spotted four emails that had been blocked by six or fewer of the 17 full solutions in

[2] With the exception of hosted solutions.

the test. Two of these contained a religious message, while the other two were almost empty except for a request to contact the sender via email, or phone, respectively. Having observed spam messages for many years, this didn't come as a surprise: both unusual spam (often sent in smaller volumes) and spam that consists of very short emails, are notoriously hard to block.

The trough seen in the graph on 13 July was caused by a number of medical spam emails.

As for the erroneously blocked legitimate emails, no email was blocked by more than two solutions.

## RESULTS

On the whole, spam catch rates were a little poorer than they were in May – something which can only partially be explained by the special circumstances described earlier. Nevertheless, all but three products blocked more than 99.5% of all spam, and four products blocked more than 99.95% – meaning they missed fewer than one in 2,000 spam emails.

*ESET Mail Security* achieved the highest final score, closely followed by *OnlyMyEmail* and *Fortinet*'s *FortiMail* appliance. *OnlyMyEmail* once again achieved the highest spam catch rate, while *Bitdefender*, *ESET*, *Libra Esva*, both *Kaspersky* products and *SpamTitan* all achieved fully clean sheets, with no false positives even in the newsletter corpus.

There were VBSpam+ awards for *Bitdefender*, *ESET*, *Fortinet*, *GFI, IBM*, *Libra Esva, OnlyMyEmail* and both *Kaspersky* products.

## FULL SOLUTIONS

### Axway MailGate 5.3.1


**SC rate:** 99.58%
**FP rate:** 0.01%
**Final score:** 99.49
**Project Honey Pot SC rate:** 99.58%
**Abusix SC rate:** 99.7%
**Newsletters FP rate:** 0.7%

### Bitdefender Security for Mail Servers 3.1.2


**SC rate:** 99.79%
**FP rate:** 0.00%
**Final score:** 99.79
**Project Honey Pot SC rate:** 99.79%
**Abusix SC rate:** 99.9%
**Newsletters FP rate:** 0.0%

### Egedian Mail Security


**SC rate:** 99.02%
**FP rate:** 0.00%
**Final score:** 99.01
**Project Honey Pot SC rate:** 99.01%
**Abusix SC rate:** 99.6%
**Newsletters FP rate:** 0.3%

### ESET Mail Security for Microsoft Exchange Server


**SC rate:** 99.99%
**FP rate:** 0.00%
**Final score:** 99.99
**Project Honey Pot SC rate:** 99.99%
**Abusix SC rate:** 100.0%
**Newsletters FP rate:** 0.0%

### Fortinet FortiMail


**SC rate:** 99.98%
**FP rate:** 0.00%
**Final score:** 99.97
**Project Honey Pot SC rate:** 99.98%
**Abusix SC rate:** 100.0%
**Newsletters FP rate:** 0.3%

### GFI MailEssentials


**SC rate:** 99.68%
**FP rate:** 0.08%
**Final score:** 99.19
**Project Honey Pot SC rate:** 99.72%
**Abusix SC rate:** 96.5%
**Newsletters FP rate:** 2.0%

### IBM Lotus Protector for Mail Security


**SC rate:** 99.84%
**FP rate:** 0.00%
**Final score:** 99.82
**Project Honey Pot SC rate:** 99.86%
**Abusix SC rate:** 98.6%
**Newsletters FP rate:** 0.7%

### Kaspersky Linux Mail Security 8.0

**SC rate:** 99.84%
**FP rate:** 0.00%
**Final score:** 99.84
**Project Honey Pot SC rate:** 99.85%
**Abusix SC rate:** 99.0%
**Newsletters FP rate:** 0.0%


### Kaspersky Secure Mail Gateway

**SC rate:** 99.78%
**FP rate:** 0.00%
**Final score:** 99.78
**Project Honey Pot SC rate:** 99.79%
**Abusix SC rate:** 99.0%
**Newsletters FP rate:** 0.0%


### Libra Esva 3.7.0.0

**SC rate:** 99.95%
**FP rate:** 0.00%
**Final score:** 99.95
**Project Honey Pot SC rate:** 99.95%
**Abusix SC rate:** 100.0%
**Newsletters FP rate:** 0.0%


### OnlyMyEmail's Corporate MX-Defender

**SC rate:** 99.998%
**FP rate:** 0.00%
**Final score:** 99.97
**Project Honey Pot SC rate:** 100.00%
**Abusix SC rate:** 100.0%
**Newsletters FP rate:** 0.7%


### ScrollOut F1

**SC rate:** 99.87%
**FP rate:** 0.22%
**Final score:** 99.36
**Project Honey Pot SC rate:** 99.88%
**Abusix SC rate:** 99.7%
**Newsletters FP rate:** 1.0%


### Sophos Email Appliance

**SC rate:** 99.47%
**FP rate:** 0.01%
**Final score:** 99.38
**Project Honey Pot SC rate:** 99.49%
**Abusix SC rate:** 98.0%
**Newsletters FP rate:** 0.3%


### SpamTitan 6.00

**SC rate:** 98.13%
**FP rate:** 0.00%
**Final score:** 98.13
**Project Honey Pot SC rate:** 98.26%
**Abusix SC rate:** 88.5%
**Newsletters FP rate:** 0.0%


### Trustwave Secure Email Gateway

**SC rate:** 99.82%
**FP rate:** 0.05%
**Final score:** 99.47
**Project Honey Pot SC rate:** 99.83%
**Abusix SC rate:** 99.5%
**Newsletters FP rate:** 2.0%


### Vade Retro MailCube

**SC rate:** 99.50%
**FP rate:** 0.01%
**Final score:** 99.40
**Project Honey Pot SC rate:** 99.51%
**Abusix SC rate:** 99.3%
**Newsletters FP rate:** 1.0%


### ZEROSPAM

**SC rate:** 99.82%
**FP rate:** 0.03%
**Final score:** 99.67
**Project Honey Pot SC rate:** 99.82%
**Abusix SC rate:** 100.0%
**Newsletters FP rate:** 0.3%

## PARTIAL SOLUTIONS

The products listed below are 'partial solutions', which means they only have access to part of the emails and/or SMTP transaction, and are intended to be used as part of a full spam solution. As such, their performance should neither be compared with those of the full solutions listed previously, nor necessarily with each other's.

### IBM XForce API

**SC rate:** 92.83%
**FP rate:** 0.00%
**Final score:** 92.83
**Project Honey Pot SC rate:** 93.02%
**Abusix SC rate:** 78.6%
**Newsletters FP rate:** 0.0%

### Spamhaus DBL

**SC rate:** 49.69%
**FP rate:** 0.00%
**Final score:** 49.69
**Project Honey Pot SC rate:** 50.34%
**Abusix SC rate:** 0.5%
**Newsletters FP rate:** 0.0%

### Spamhaus ZEN

**SC rate:** 89.46%
**FP rate:** 0.00%
**Final score:** 89.46
**Project Honey Pot SC rate:** 89.36%
**Abusix SC rate:** 97.6%
**Newsletters FP rate:** 0.0%

### Spamhaus ZEN+DBL

**SC rate:** 92.70%
**FP rate:** 0.00%
**Final score:** 92.70
**Project Honey Pot SC rate:** 92.63%
**Abusix SC rate:** 97.6%
**Newsletters FP rate:** 0.0%

## CONCLUSION

Running the 45th VBSpam test certainly wasn't as easy as most of the other tests have been, but at the time of writing, we have put the issues that plagued this test behind us, and the 46th VBSpam test is already smoothly underway. We are working on some further improvements for the tests beyond that, although the core of the test will remain the same: measuring the accuracy of email security solutions and sharing the results both with the product developers and with the wider security community.

As always, for those interested in submitting their solutions, please contact martijn.grooten@virusbulletin.com.

**Editor:** Martijn Grooten
**Chief of Operations:** John Hawes
**Security Test Engineers:** Scott James, Tony Oliveira, Adrian Luca, Ionuț Răileanu, Chris Stock
**Sales Executive:** Allison Sketchley
**Editorial Assistant:** Helen Martin
**Developer:** Lian Sebe
**Consultant Technical Editor:** Dr Morton Swimmer

**Tel: +44 (0)1235 555139 Fax: +44 (0)1865 543153**
**Email: editorial@virusbtn.com Web: https://www.virusbulletin.com/**

| | True negatives | False positives | FP rate | False negatives | True positives | SC rate | VBSpam | Final score |
|---|---|---|---|---|---|---|---|---|
| Axway | 7321 | 1 | 0.01% | 242 | 57812 | 99.58% | SPAM Verified | 99.49 |
| Bitdefender | 7322 | 0 | 0.00% | 121 | 57933 | 99.79% | SPAM + Verified | 99.79 |
| Egedian | 7322 | 0 | 0.00% | 568 | 57486 | 99.02% | SPAM Verified | 99.01 |
| ESET | 7322 | 0 | 0.00% | 5 | 58049 | 99.99% | SPAM + Verified | 99.99 |
| FortiMail | 7322 | 0 | 0.00% | 9 | 58045 | 99.98% | SPAM + Verified | 99.97 |
| GFI | 7316 | 6 | 0.08% | 188 | 57866 | 99.68% | SPAM + Verified | 99.19 |
| IBM | 7322 | 0 | 0.00% | 90 | 57964 | 99.84% | SPAM + Verified | 99.82 |
| Kaspersky LMS | 7322 | 0 | 0.00% | 93 | 57961 | 99.84% | SPAM + Verified | 99.84 |
| Kaspersky SMG | 7322 | 0 | 0.00% | 126 | 57928 | 99.78% | SPAM + Verified | 99.78 |
| Libra Esva | 7322 | 0 | 0.00% | 29 | 58025 | 99.95% | SPAM + Verified | 99.95 |
| OnlyMyEmail | 7322 | 0 | 0.00% | 1 | 58053 | 99.998% | SPAM + Verified | 99.97 |
| Scrollout | 7306 | 16 | 0.22% | 73 | 57981 | 99.87% | SPAM Verified | 99.36 |
| Sophos | 7321 | 1 | 0.01% | 310 | 57744 | 99.47% | SPAM Verified | 99.38 |
| SpamTitan | 7322 | 0 | 0.00% | 1087 | 56967 | 98.13% | SPAM Verified | 98.13 |
| Trustwave | 7318 | 4 | 0.05% | 102 | 57952 | 99.82% | SPAM Verified | 99.47 |
| Vade Retro MailCube | 7321 | 1 | 0.01% | 288 | 57766 | 99.50% | SPAM Verified | 99.40 |
| ZEROSPAM | 7320 | 2 | 0.03% | 103 | 57951 | 99.82% | SPAM Verified | 99.67 |
| IBM X-Force* | 7322 | 0 | 0.00% | 4162 | 53892 | 92.83% | N/A | 92.83 |
| Spamhaus DBL* | 7322 | 0 | 0.00% | 29209 | 28845 | 49.69% | N/A | 49.69 |
| Spamhaus ZEN* | 7322 | 0 | 0.00% | 6116 | 51938 | 89.46% | N/A | 89.46 |
| Spamhaus ZEN+DBL* | 7322 | 0 | 0.00% | 4238 | 53816 | 92.70% | N/A | 92.70 |

**The Spamhaus products and IBM X-Force are partial solutions and their performance should not be compared with that of other products.*

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

| | Newsletters | | Project Honey Pot | | Abusix | | STDev† |
|---|---|---|---|---|---|---|---|
| | False positives | FP rate | False negatives | SC rate | False negatives | SC rate | |
| Axway | 2 | 0.7% | 240 | 99.58% | 2 | 99.7% | 0.78 |
| Bitdefender | 0 | 0.0% | 120 | 99.79% | 1 | 99.9% | 0.38 |
| Egedian | 1 | 0.3% | 565 | 99.01% | 3 | 99.6% | 1.47 |
| ESET | 0 | 0.0% | 5 | 99.99% | 0 | 100.0% | 0.06 |
| FortiMail | 1 | 0.3% | 9 | 99.98% | 0 | 100.0% | 0.09 |
| GFI | 6 | 2.0% | 161 | 99.72% | 27 | 96.5% | 0.85 |
| IBM | 2 | 0.7% | 79 | 99.86% | 11 | 98.6% | 0.37 |
| Kaspersky LMS | 0 | 0.0% | 85 | 99.85% | 8 | 99.0% | 0.4 |
| Kaspersky SMG | 0 | 0.0% | 118 | 99.79% | 8 | 99.0% | 0.61 |
| Libra Esva | 0 | 0.0% | 29 | 99.95% | 0 | 100.0% | 0.19 |
| OnlyMyEmail | 2 | 0.7% | 1 | 100.00% | 0 | 100.0% | 0.04 |
| Scrollout | 3 | 1.0% | 71 | 99.88% | 2 | 99.7% | 0.39 |
| Sophos | 1 | 0.3% | 295 | 99.49% | 15 | 98.0% | 0.78 |
| SpamTitan | 0 | 0.0% | 999 | 98.26% | 88 | 88.5% | 3.14 |
| Trustwave | 6 | 2.0% | 98 | 99.83% | 4 | 99.5% | 0.32 |
| Vade Retro MailCube | 3 | 1.0% | 283 | 99.51% | 5 | 99.3% | 0.82 |
| ZEROSPAM | 1 | 0.3% | 103 | 99.82% | 0 | 100.0% | 0.58 |
| IBM X-Force* | 0 | 0.0% | 3999 | 93.02% | 163 | 78.6% | 3.41 |
| Spamhaus DBL* | 0 | 0.0% | 28450 | 50.34% | 759 | 0.5% | 11.5 |
| Spamhaus ZEN* | 0 | 0.0% | 6098 | 89.36% | 18 | 97.6% | 4.6 |
| Spamhaus ZEN+DBL* | 0 | 0.0% | 4220 | 92.63% | 18 | 97.6% | 3.8 |

** The Spamhaus products and IBM X-Force are partial solutions and their performance should not be compared with that of other products.*

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

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

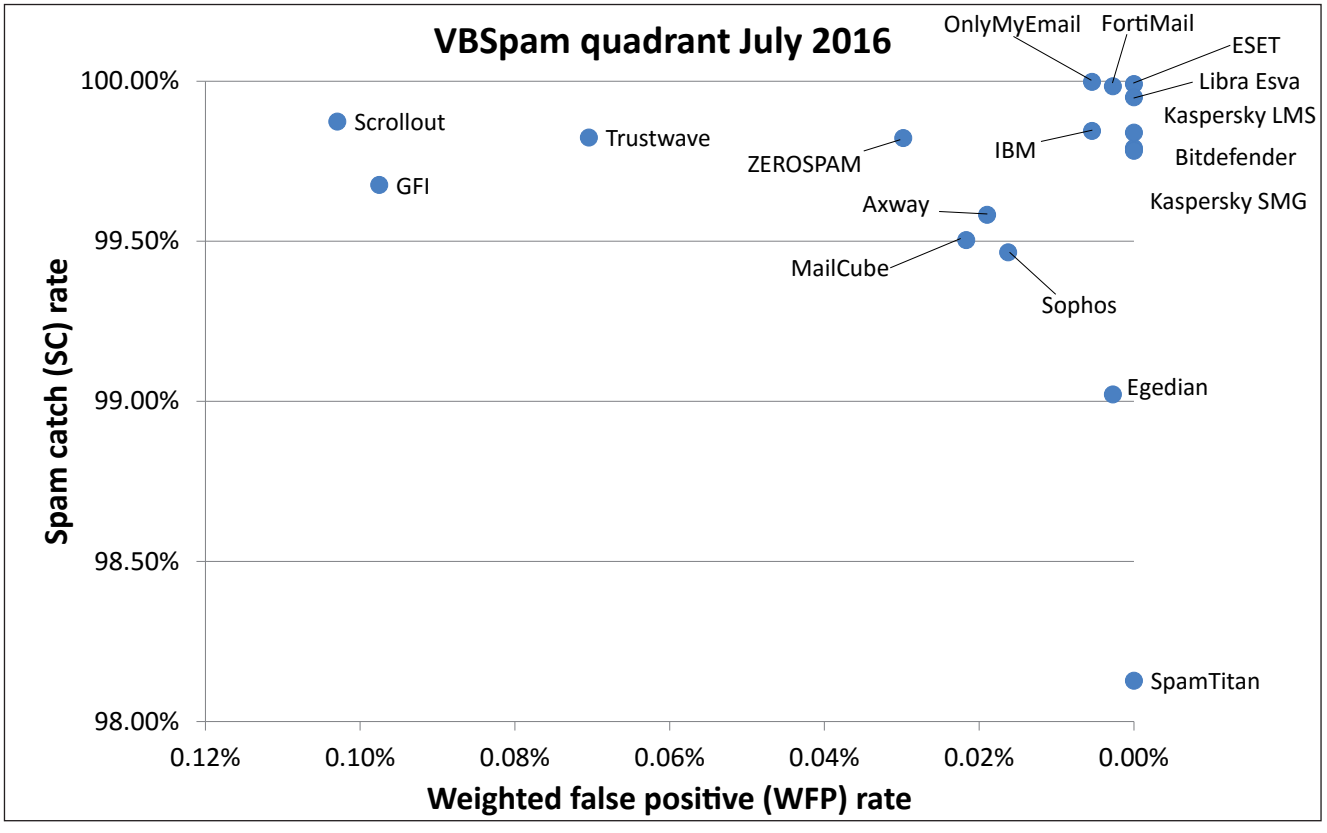
| Hosted solutions | Anti-malware | IPv6 | DKIM | SPF | DMARC | Multiple MX-records | Multiple locations |
|---|---|---|---|---|---|---|---|
| OnlyMyEmail | Proprietary (optional) | | √ | √ | * | √ | √ |
| Vade Retro MailCube | DrWeb; proprietary | √ | √ | √ | | √ | √ |
| ZEROSPAM | ClamAV | | | √ | | √ | √ |

* OnlyMyEmail verifies DMARC status but doesn't provide feedback at the moment.

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

| Local solutions | Anti-malware | IPv6 | DKIM | SPF | DMARC | Interface | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | CLI | GUI | Web GUI | API |
| Axway MailGate | Kaspersky, McAfee | √ | √ | √ | | | | √ | |
| Bitdefender | Bitdefender | √ | | | | √ | | √ | √ |
| Egedian | Bitdefender, ClamAV | √ | | | | √ | | √ | √ |
| ESET | ESET Threatsense | √ | √ | √ | √ | √ | √ | | |
| FortiMail | Fortinet | √ | √ | √ | | √ | | √ | |
| GFI | Five anti-virus engines | √ | | √ | | | | √ | |
| IBM | Sophos; IBM Remote Malware Detection | | | √ | | √ | | √ | |
| Kaspersky LMS | Kaspersky Lab | √ | | √ | | √ | | √ | |
| Kaspersky SMG | Kaspersky Lab | √ | | √ | | √ | | √ | |
| Libra Esva | ClamAV; others optional | | √ | √ | | √ | | √ | |
| Scrollout | ClamAV | | | √ | | √ | | √ | √ |
| Sophos | Sophos | | √ | √ | | | | √ | |
| SpamTitan | Kaspersky; ClamAV | √ | √ | √ | | √ | | √ | √ |
| Trustwave | Support for multiple third-party engines | √ | √ | √ | | √ | √ | √ | |

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




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