MARCH 2017

virus BULLETIN

Covering the global threat landscape

VBSPAM COMPARATIVE REVIEW MARCH 2017

Martijn Grooten & Ionuţ Răileanu

While we were working on this report, one of the biggest news stories circulating was that of a ransomware attack against the Dutch parliament. Writing about the attack, *Reuters*[1] immediately made a link with a recent diplomatic row between The Netherlands and Turkey.

Much as this would have made for a fascinating story – not to mention a huge headache for both countries' diplomats – the real story was far more mundane. Someone working in Parliament received an email[2] about an invoice, thought the email looked sufficiently credible to open it, open the attachment, and then likely enable macros, after which the malware managed, somehow, to bypass locally installed security software.

There are many mistakes in this sorry tale that should not have been made, but it serves as an important reminder: spam is still an issue. For those with a good understanding of email (which presumably includes most readers of this report), this may not seem obvious. We can spot most spam emails – even the few that our spam filters miss – from a mile away and laugh at the silly mistakes made by the spammers: 'Look at the domain name!'; 'Did you notice that it wasn't even signed with DKIM?'.

But most people are not like us; nor should we expect them to be. They may notice the spam, but sometimes they don't, and if it happens to be malicious, some pretty nasty things can happen. And therefore it is important that almost all spam is blocked by email security solutions, and it matters that some of these solutions block a little bit more than others. While spam may not be the most exciting aspect of computer security, it remains a vector for some very costly attacks.

In the VBSpam comparative reviews, we report on the state of spam filtering, give our stamp of approval to those email security solutions that perform well, and highlight the differences in performance between the various solutions.

This month, 15 full solutions were put to the test, all of which performed well enough to achieve a VBSpam award, with four of them performing well enough to earn the VBSpam+ accolade. We also tested seven DNS-based blacklists of various kinds.

THE VOLATILITY OF SPAM

In January, well before this test started, the Necurs botnet – which had been notorious for spreading malicious spam, in particular the Locky ransomware – significantly decreased its activities[3], only to return in the third week of March with a massive pump-and-dump spam campaign[4].

When we looked into this latter campaign, we noticed[5] that most Necurs spam was easily blocked by every product on test in our lab. Thus the earlier temporary decline in Necurs spam, though good news, is unlikely to have precipitated sighs of relief in spam research labs around the world. This does, however, serve as a clear demonstration of the fact that spam tends to be extremely volatile, both in quantity and in quality.

It is in this context that one should view the decent overall performance of products in this test, with most products blocking more spam on this occasion than in the last test (the average performance measure was only marginally higher, but this figure was skewed by a few outliers). There is no doubt that some hard work on the part of the products' developers

[1] http://uk.reuters.com/article/uk-netherlands-cyber-parliament-idUKKBN16Z1IT
[2] https://twitter.com/markloman/status/846754303016685568
[3] http://blog.talosintelligence.com/2017/01/locky-struggles.html
[4] http://blog.talosintelligence.com/2017/03/necurs-diversifies.html
[5] https://www.virusbulletin.com/blog/2017/03/mostly-blocked-still-good-enough-necurs-sending-pump-and-dump-spam/

ISSN 1749-7027

contributed to this, but part of the boost in performance may simply be a matter of luck – perhaps the period between late February and early March, when this test was run, just wasn't a very difficult one for spam filtering.

The decrease in Necurs spam during this period is likely to have contributed to the decline in spam with malicious attachments, of which we recorded only a little over 1,000 emails in this test. The typical malicious attachment continues to be a downloader, which means that different users might receive different payloads, depending on their location. Delivery notifications and invoices continue to be a popular lure in these malicious campaigns, though we did notice one adult-themed spam campaign with a malicious JScript-based downloader attached.

Only 25 of the malicious emails were missed by any of the full solutions, and only two of these were missed by more than one solution: a sample of the Nemucod downloader and a generic downloader written in Java, both of which were missed by two products.

Among the rest of the spam, there were also very few difficult emails: the email with which products had most difficulty was missed by no more than five full solutions. This particular email was a one-line 419 scam. While such scams may not be known for their technical sophistication, the lower volumes in which such messages are often sent helps keep them under the radar.

RESULTS

Among the performance on the spam corpus, *OnlyMyEmail* and *ESET* stood out for missing just one and two emails respectively, while *Bitdefender*, *Fortinet*, *IBM*, *Kaspersky*'s *Linux Mail Security* product and *ZEROSPAM* all deserve credit for blocking least 99.95% of spam. *OnlyMyEmail*, *ESET*, *Bitdefender* and *Fortinet* did not block any legitimate emails either, earning them VBSpam+ awards. 'Clean sheets' – where the product didn't block any emails from either the ham feed or the newsletter feed – were achieved by *Bitdefender*, *ESET* and *Fortimail*.

Axway MailGate 5.5.1

SC rate: 99.89%
FP rate: 0.01%
Final score: 99.77
Project Honey Pot SC rate: 99.78%
Abusix SC rate: 99.97%
Newsletters FP rate: 1.3%
Malware SC rate: 99.52%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Bitdefender Security for Mail Servers 3.1.6

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

ESET Mail Security for Microsoft Exchange Server

SC rate: 99.999%
FP rate: 0.00%
Final score: 99.999
Project Honey Pot SC rate: 99.997%
Abusix SC rate: 100.00%
Newsletters FP rate: 0.0%
Malware SC rate: 99.90%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Fortinet FortiMail

SC rate: 99.98%
FP rate: 0.00%
Final score: 99.98
Project Honey Pot SC rate: 99.999%
Abusix SC rate: 99.96%
Newsletters FP rate: 0.0%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

GFI MailEssentials

SC rate: 98.73%
FP rate: 0.04%
Final score: 98.33
Project Honey Pot SC rate: 99.57%
Abusix SC rate: 98.07%
Newsletters FP rate: 4.7%
Malware SC rate: 99.62%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

IBM Lotus Protector for Mail Security

SC rate: 99.99%
FP rate: 0.01%
Final score: 99.91
Project Honey Pot SC rate: 99.98%
Abusix SC rate: 100.00%
Newsletters FP rate: 0.3%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Kaspersky Linux Mail Security 8.0

SC rate: 99.96%
FP rate: 0.01%
Final score: 99.89
Project Honey Pot SC rate: 99.93%
Abusix SC rate: 99.98%
Newsletters FP rate: 0.0%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Kaspersky Secure Mail Gateway

SC rate: 99.92%
FP rate: 0.01%
Final score: 99.85
Project Honey Pot SC rate: 99.86%
Abusix SC rate: 99.96%
Newsletters FP rate: 0.0%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Libra Esva 4.1.0.0

SC rate: 99.97%
FP rate: 0.03%
Final score: 99.81
Project Honey Pot SC rate: 99.98%
Abusix SC rate: 99.97%
Newsletters FP rate: 0.6%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

OnlyMyEmail's Corporate MX-Defender

SC rate: 99.999%
FP rate: 0.00%
Final score: 99.99
Project Honey Pot SC rate: 99.999%
Abusix SC rate: 100.00%
Newsletters FP rate: 0.3%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Scrollout F1

SC rate: 99.17%
FP rate: 0.27%
Final score: 97.57
Project Honey Pot SC rate: 99.93%
Abusix SC rate: 98.57%
Newsletters FP rate: 6.6%
Malware SC rate: 99.81%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Sophos Email Appliance

SC rate: 99.68%
FP rate: 0.04%
Final score: 99.48
Project Honey Pot SC rate: 99.38%
Abusix SC rate: 99.92%
Newsletters FP rate: 0.0%
Malware SC rate: 99.90%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

SpamTitan 6.00

SC rate: 99.85%
FP rate: 0.00%
Final score: 99.81
Project Honey Pot SC rate: 99.83%
Abusix SC rate: 99.87%
Newsletters FP rate: 0.9%
Malware SC rate: 99.62%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Vade Secure MailCube

SC rate: 99.73%
FP rate: 0.05%
Final score: 99.46
Project Honey Pot SC rate: 99.39%
Abusix SC rate: 99.99%
Newsletters FP rate: 0.0%
Malware SC rate: 99.04%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

ZEROSPAM

SC rate: 99.95%
FP rate: 0.01%
Final score: 99.77
Project Honey Pot SC rate: 99.93%
Abusix SC rate: 99.97%
Newsletters FP rate: 2.8%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

IBM XForce API

SC rate: 87.93%
FP rate: 0.03%
Final score: 87.77
Project Honey Pot SC rate: 90.78%
Abusix SC rate: 85.69%
Newsletters FP rate: 0.6%
Malware SC rate: 88.72%

IBM XForce API – domains

SC rate: 41.49%
FP rate: 0.00%
Final score: 41.49
Project Honey Pot SC rate: 83.96%
Abusix SC rate: 8.34%
Newsletters FP rate: 0.0%
Malware SC rate: 0.96%

IBM XForce API – combined

SC rate: 91.11%
FP rate: 0.03%
Final score: 90.96
Project Honey Pot SC rate: 97.91%
Abusix SC rate: 85.81%
Newsletters FP rate: 0.6%
Malware SC rate: 88.91%

Spamhaus DBL

SC rate: 14.74%
FP rate: 0.05%
Final score: 14.47
Project Honey Pot SC rate: 19.71%
Abusix SC rate: 10.85%
Newsletters FP rate: 0.0%
Malware SC rate: 0.00%

Spamhaus ZEN

SC rate: 93.36%
FP rate: 0.00%
Final score: 93.36
Project Honey Pot SC rate: 87.66%
Abusix SC rate: 97.81%
Newsletters FP rate: 0.0%
Malware SC rate: 84.80%

Spamhaus ZEN+DBL

SC rate: 95.00%
FP rate: 0.05%
Final score: 94.74
Project Honey Pot SC rate: 91.25%
Abusix SC rate: 97.93%
Newsletters FP rate: 0.0%
Malware SC rate: 84.80%

URIBL (MX Tools)

SC rate: 38.79%
FP rate: 0.49%
Final score: 35.50
Project Honey Pot SC rate: 77.29%
Abusix SC rate: 8.72%
Newsletters FP rate: 27.2%
Malware SC rate: 0.00%

CONCLUSION

This was an easy test for filtering spam – for most products, anyway. However, as new spam botnets come and go, the situation may quickly change. We are looking forward to seeing how products perform in a no doubt much changed threat landscape in May.

The next test report, to be published in June 2017, will continue to look at all aspects of spam. Those interested in submitting a product are asked to contact martijn.grooten@virusbulletin.com.

APPENDIX: SET-UP, METHODOLOGY AND EMAIL CORPORA

The full VBSpam test methodology can be found at https://www.virusbulletin.com/testing/vbspam/vbspam-methodology/.

The test ran for 69 days, from 12am on 18 February to 12am on 5 March 2017.

The test corpus consisted of 166,873 emails. 159,058 of these were spam, 69,743 of which were provided by *Project Honey Pot*, with the remaining 89,315 spam emails provided by *spamfeed.me*, a product from *Abusix*. There were 7,499 legitimate emails ('ham') and 316 newsletters.

Moreover, 1,046 emails from the spam corpus were found to contain a malicious attachment; though we report separate performance metrics on this corpus, 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[6]. Consequently, products were able to filter email in an environment that was very close to one in which they would be deployed in the real world.

For those products running in our lab, we 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)

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.

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

Editor: Martijn Grooten

Head of Testing: Peter Karsai

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 Email: editor@virusbulletin.com

Web: https://www.virusbulletin.com/

	True negatives	False positives	FP rate	False negatives	True positives	SC rate	VBSpam	Final score
Axway	7498	1	0.01%	180	158878	99.89%	SPAM Verified	99.77
Bitdefender	7499	0	0.00%	27	159031	99.98%	SPAM + Verified	99.98
ESET	7499	0	0.00%	2	159056	99.999%	SPAM + Verified	99.999
FortiMail	7499	0	0.00%	37	159021	99.98%	SPAM + Verified	99.98
GFI MailEssentials	7496	3	0.04%	2023	157035	98.73%	SPAM Verified	98.33
IBM	7498	1	0.01%	14	159044	99.99%	SPAM Verified	99.91
Kaspersky LMS	7498	1	0.01%	64	158994	99.96%	SPAM Verified	99.89
Kaspersky SMG	7498	1	0.01%	133	158925	99.92%	SPAM Verified	99.85
Libra Esva	7497	2	0.03%	42	159016	99.97%	SPAM Verified	99.81
OnlyMyEmail	7499	0	0.00%	1	159057	99.999%	SPAM + Verified	99.99
Scrollout	7479	20	0.27%	1328	157730	99.17%	SPAM Verified	97.57
Sophos	7496	3	0.04%	504	158554	99.68%	SPAM Verified	99.48
SpamTitan	7499	0	0.00%	236	158822	99.85%	SPAM Verified	99.81
Vade Secure MailCube	7495	4	0.05%	434	158624	99.73%	SPAM Verified	99.46
ZEROSPAM	7498	1	0.01%	75	158983	99.95%	SPAM Verified	99.77
IBM X-Force IP*	7497	2	0.03%	19205	139853	87.93%	N/A	87.77
IBM X-Force URL*	7499	0	0.00%	93057	66001	41.49%	N/A	41.49
IBM X-Force combined*	7497	2	0.03%	14133	144925	91.11%	N/A	90.96
Spamhaus DBL*	7495	4	0.05%	135620	23438	14.74%	N/A	14.47
Spamhaus ZEN*	7499	0	0.00%	10561	148497	93.36%	N/A	93.36
Spamhaus ZEN+DBL*	7495	4	0.05%	7949	151109	95.00%	N/A	94.74
URIBL*	7462	37	0.49%	97366	61692	38.79%	N/A	35.50

**The Spamhaus, IBM X-Force and URIBL products 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		Malware		Project Honey Pot		Abusix		STDev†	Speed			
	False positives	FP rate	False negatives	SC rate	False negatives	SC rate	False negatives	SC rate		10%	50%	95%	98%
Axway	4	1.3%	5	99.52%	152	99.78%	28	99.97%	0.22	●	●	●	●
Bitdefender	0	0.0%	0	100.00%	11	99.98%	16	99.98%	0.09	●	●	●	●
ESET	0	0.0%	1	99.90%	2	99.997%	0	100.00%	0.02	●	●	●	●
FortiMail	0	0.0%	0	100.00%	1	99.999%	36	99.96%	0.13	●	●	●	●
GFI MailEssentials	15	4.7%	4	99.62%	297	99.57%	1726	98.07%	0.90	●	●	●	●
IBM	1	0.3%	0	100.00%	14	99.98%	0	100.00%	0.05	●	●	●	●
Kaspersky LMS	0	0.0%	0	100.00%	47	99.93%	17	99.98%	0.13	●	●	●	●
Kaspersky SMG	0	0.0%	0	100.00%	98	99.86%	35	99.96%	0.18	●	●	●	●
Libra Esva	2	0.6%	0	100.00%	15	99.98%	27	99.97%	0.08	●	●	●	●
OnlyMyEmail	1	0.3%	0	100.00%	1	99.999%	0	100.00%	0.01	●	●	●	●
Scrollout	21	6.6%	2	99.81%	48	99.93%	1280	98.57%	1.70	●	●	●	●
Sophos	0	0.0%	1	99.90%	431	99.38%	73	99.92%	0.43	●	●	●	●
SpamTitan	3	0.9%	4	99.62%	116	99.83%	120	99.87%	0.28	●	●	●	●
Vade Secure MailCube	0	0.0%	10	99.04%	427	99.39%	7	99.99%	0.38	●	●	●	●
ZEROSPAM	9	2.8%	0	100.00%	49	99.93%	26	99.97%	0.16	●	●	●	●
IBM X-Force IP*	2	0.6%	118	88.72%	6427	90.78%	12778	85.69%	3.61	N/A	N/A	N/A	N/A
IBM X-Force URL*	0	0.0%	1036	0.96%	11189	83.96%	81868	8.34%	17.05	N/A	N/A	N/A	N/A
IBM X-Force combined*	2	0.6%	116	88.91%	1461	97.91%	12672	85.81%	3.70	N/A	N/A	N/A	N/A
Spamhaus DBL*	0	0.0%	1046	0.00%	55999	19.71%	79621	10.85%	6.20	N/A	N/A	N/A	N/A
Spamhaus ZEN*	0	0.0%	159	84.80%	8609	87.66%	1952	97.81%	3.06	N/A	N/A	N/A	N/A
Spamhaus ZEN+DBL*	0	0.0%	159	84.80%	6102	91.25%	1847	97.93%	2.43	N/A	N/A	N/A	N/A
URIBL*	86	27.2%	1046	0.00%	15842	77.29%	81524	8.72%	15.66	N/A	N/A	N/A	N/A

** The Spamhaus products, IBM X-Force and URIBL are partial solutions and their performance should not be compared with that of other products. None of the queries to the IP blacklists included any information on the attachments; hence their performance on the malware corpus is added purely for information.*

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

● *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.)

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

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

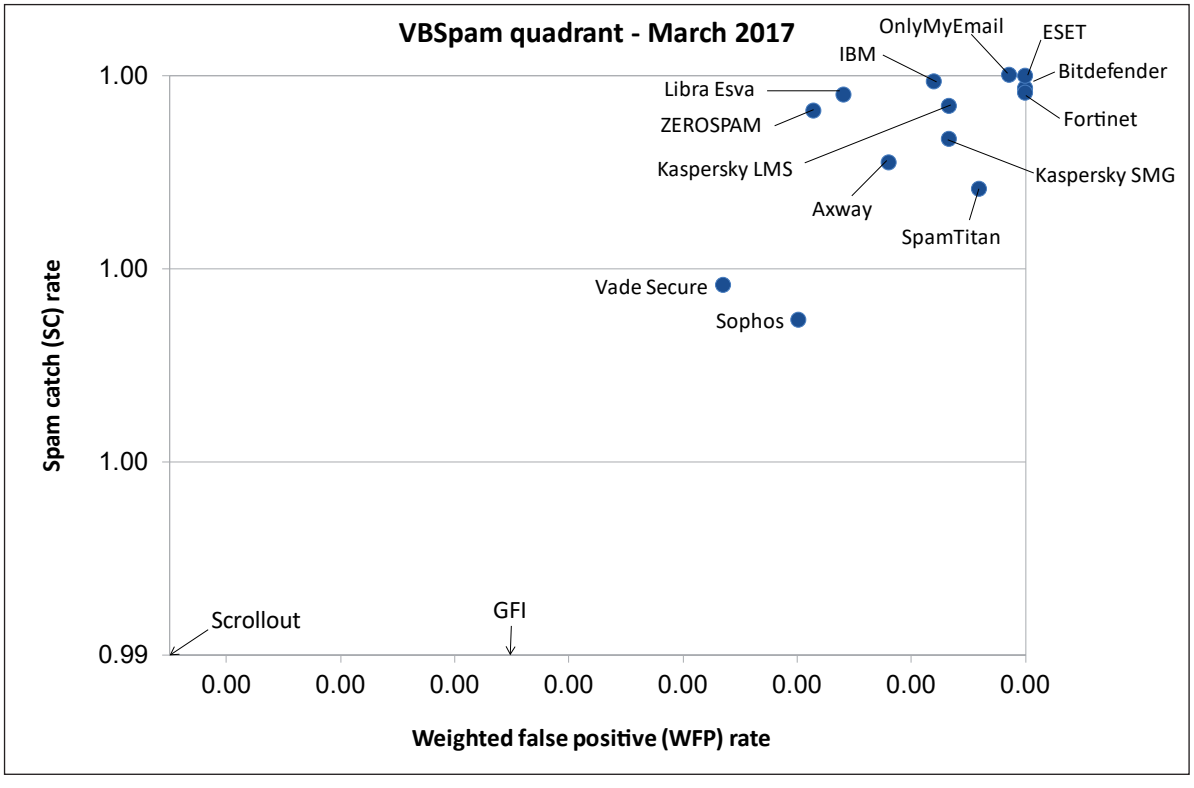
(Please refer to the text for full product names.)

Local solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Interface			
						CLI	GUI	Web GUI	API
Axway MailGate	Kaspersky, McAfee	√	√	√				√	
Bitdefender	Bitdefender	√				√		√	√
ESET	ESET Threatsense	√	√	√	√	√	√		
FortiMail	Fortinet	√	√	√	√	√		√	√
GFI MailEssentials	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	√	√	√		√		√	√

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

Product	Final score
ESET	99.999
OnlyMyEmail	99.99
Bitdefender	99.98
FortiMail	99.98
IBM	99.91
Kaspersky LMS	99.89
Kaspersky SMG	99.85
Libra Esva	99.81
SpamTitan	99.81
Axway	99.77
ZEROSPAM	99.77
Sophos	99.48
Vade Secure MailCube	99.46
GFI MailEssentials	98.33
Scrollout	97.57

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



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