DECEMBER 2017

virus BULLETIN

Covering the global threat landscape

VBSPAM COMPARATIVE REVIEW DECEMBER 2017

Martijn Grooten & Ionuţ Răileanu

Spam is making a bit of a comeback – not that it ever really went away. In fact, spam volumes have been several times higher in the past, but this year it has picked up interest from the security community again, as evidenced, for example, by a paper presented at VB2017 that looked at the technical details of five spam botnets[1], a presentation at AVAR that looked at spam botnets more generally[2], and a presentation at Botconf on perhaps the most well known spam botnet, Necurs[3].

Technically, spam botnets are not the most advanced, and there is a huge gap between them and the sophisticated malware attacks that regularly make the news.

A typical spam bot runs on a machine or device (not just *Windows* PCs; a lot of spam is sent from compromised web servers or even compromised IoT devices) with very poor security hygiene – it is quite telling that Necurs has not infected any new machines for years.

Spam is also typically sent from countries with relatively high Internet penetration but with relatively low income, which in turn contributes to poor security: more than 25 per cent of the spam messages in this test were sent from machines in either Vietnam or India.

The fact that spam botnets, especially those running on older devices, tend to be relatively easy to detect, contributes to high rates of blocking spam – whether the emails come with a malicious payload or not – although it is worth keeping in mind that the products we test are designed for use in the corporate market, not by home users, and while most ISPs perform a decent amount of spam filtering, it is likely that more bad stuff 'leaks through' to home users.

In this VBSpam test, the 50th of its kind, 14 full solutions were lined up on the *Virus Bulletin* test bench. No fewer than eight products achieved a VBSpam+ award, while five other products achieved a VBSpam award.

WHY MALICIOUS SPAM IS BOTH EASY AND HARD TO BLOCK

This test once again shows that spam messages with a malicious attachment aren't a big issue for most email security solutions. The fact that almost all of them were blocked by the participating IP blacklists (which block based purely on the sending IP address) shows that it's not just the content of the messages that products act upon: it's the fact that these emails are first and foremost spam and that they are sent from known spam botnets.

That is not to say that, in most cases, the attachments wouldn't have been blocked anyway, but it is worth looking at the attachments themselves to understand that blocking them isn't entirely trivial.

Few would disagree that these attachments are malicious, but all they do – after obfuscation and often some social engineering ('please enable macros to view the hidden content') – is download a piece of malware from a remote server.

This means that a static analysis of the file – as performed by most email security solutions – won't reveal any malicious activity (such as installing a backdoor or encrypting files) and will, at best, reveal similarities with previously seen attachments. Malware authors constantly change the attachments sent in these emails with the explicit intention of evading this kind of detection.

We hope soon to publish a report in which, among other things, we will look more closely at the malware attached to these emails.

[1] https://www.virusbulletin.com/blog/2017/11/vb2017-paper-peering-spam-botnets/.
[2] http://avar.skdlabs.com/index.php/speakers/the-story-of-the-botnets-behind-malicious-spam-campaigns/.
[3] https://botconf2017.sched.com/event/CtHT/malware-penny-stocks-pharma-spam-necurs-delivers.

ISSN 1749-7027

RESULTS

Amost all participating vendors have reason to be content with their results in this test, but this is especially the case for *OnlyMyEmail*, which didn't miss a single spam message among more than 150,000 emails (including thousands carrying malware). It didn't block any legitimate emails either, and with only two false positives in the newsletters corpus, the product is well deserving of a VBSpam+ award.

VBSpam+ awards were also achieved by *Bitdefender*, *ESET*, *Fortinet*, *IBM*, *Libra Esva*, and both *Kaspersky* products.

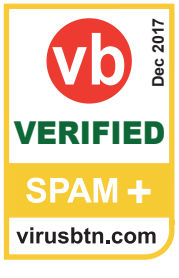
It was interesting to note that two of the three domain blacklists included in the test, both of which blocked domains in more than 50% of spam emails in the September test, saw a significant drop in their catch rate. This is often a sign of a shift in spammers' techniques towards emails that contain only links to legitimate domains that are used to host the spammy/malicious content, or to redirect to other sites, or emails that contain no links at all.

Finally, it is worth noting once again that all percentages reported here should be seen in the context of the test. In the real world, thanks to a combination of factors, catch rates as perceived by both systems administrators and end-users will be lower for all participating products.

Axway MailGate 5.5.1

SC rate: 99.76%
FP rate: 0.06%
Final score: 99.42
Project Honey Pot SC rate: 99.48%
Abusix SC rate: 99.97%
Newsletters FP rate: 1.1%
Malware SC rate: 99.98%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Bitdefender Security for Mail Servers 3.1.6



SC rate: 99.96%
FP rate: 0.00%
Final score: 99.96
Project Honey Pot SC rate: 99.93%
Abusix SC rate: 99.99%
Newsletters FP rate: 0.0%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

CYREN

SC rate: 98.89%
FP rate: 0.00%
Final score: 98.83
Project Honey Pot SC rate: 97.77%
Abusix SC rate: 99.73%
Newsletters FP rate: 1.4%
Malware SC rate: 99.48%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

ESET Mail Security for Microsoft Exchange Server

SC rate: 99.997%
FP rate: 0.00%
Final score: 99.997
Project Honey Pot SC rate: 99.995%
Abusix SC rate: 99.998%
Newsletters FP rate: 0.0%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Forcepoint Email Security Cloud

SC rate: 99.42%
FP rate: 0.10%
Final score: 98.89
Project Honey Pot SC rate: 98.71%
Abusix SC rate: 99.95%
Newsletters FP rate: 0.4%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Fortinet FortiMail

SC rate: 99.99%
FP rate: 0.00%
Final score: 99.99
Project Honey Pot SC rate: 99.998%
Abusix SC rate: 99.99%
Newsletters FP rate: 0.0%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

IBM Lotus Protector for Mail Security

SC rate: 99.98%
FP rate: 0.00%
Final score: 99.97
Project Honey Pot SC rate: 99.96%
Abusix SC rate: 99.99%
Newsletters FP rate: 0.4%
Malware SC rate: 99.98%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Kaspersky for Exchange

SC rate: 99.97%
FP rate: 0.00%
Final score: 99.97
Project Honey Pot SC rate: 99.94%
Abusix SC rate: 99.99%
Newsletters FP rate: 0.0%
Malware SC rate: 99.88%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Kaspersky Linux Mail Security 8.0

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

Libra Esva 4.1.0.0

SC rate: 99.95%
FP rate: 0.00%
Final score: 99.92
Project Honey Pot SC rate: 99.91%
Abusix SC rate: 99.98%
Newsletters FP rate: 0.7%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

OnlyMyEmail's Corporate MX-Defender

SC rate: 100.00%
FP rate: 0.00%
Final score: 99.97
Project Honey Pot SC rate: 100.00%
Abusix SC rate: 100.00%
Newsletters FP rate: 0.7%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Scrollout F1

SC rate: 99.97%
FP rate: 0.31%
Final score: 98.20
Project Honey Pot SC rate: 99.93%
Abusix SC rate: 99.99%
Newsletters FP rate: 4.9%
Malware SC rate: 99.98%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

Vade Secure Cloud

SC rate: 99.66%
FP rate: 0.42%
Final score: 97.55
Project Honey Pot SC rate: 99.37%
Abusix SC rate: 99.87%
Newsletters FP rate: 0.7%
Malware SC rate: 99.95%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

ZEROSPAM

SC rate: 99.96%
FP rate: 0.00%
Final score: 99.81
Project Honey Pot SC rate: 99.92%
Abusix SC rate: 99.98%
Newsletters FP rate: 3.5%
Malware SC rate: 100.00%
Speed: 10%: ●; 50%: ●; 95%: ●; 98%: ●

IBM X-Force Combined

SC rate: 95.33%
FP rate: 0.01%
Final score: 95.26
Project Honey Pot SC rate: 95.36%
Abusix SC rate: 95.31%
Newsletters FP rate: 0.0%
Malware SC rate: 97.78%

IBM X-Force IP

SC rate: 92.89%
FP rate: 0.01%
Final score: 92.81
Project Honey Pot SC rate: 90.55%
Abusix SC rate: 94.62%
Newsletters FP rate: 0.0%
Malware SC rate: 97.78%

IBM X-Force URL

SC rate: 19.98%
FP rate: 0.00%
Final score: 19.98
Project Honey Pot SC rate: 42.92%
Abusix SC rate: 2.93%
Newsletters FP rate: 0.0%
Malware SC rate: 0.13%

Spamhaus DBL

SC rate: 12.89%
FP rate: 0.00%
Final score: 12.89
Project Honey Pot SC rate: 26.62%
Abusix SC rate: 2.69%
Newsletters FP rate: 0.0%
Malware SC rate: 0.55%

Spamhaus ZEN

SC rate: 96.54%
FP rate: 0.00%
Final score: 96.54
Project Honey Pot SC rate: 94.09%
Abusix SC rate: 98.37%
Newsletters FP rate: 0.0%
Malware SC rate: 99.87%

Spamhaus ZEN+DBL

SC rate: 97.44%
FP rate: 0.00%
Final score: 97.44
Project Honey Pot SC rate: 95.52%
Abusix SC rate: 98.86%
Newsletters FP rate: 0.0%
Malware SC rate: 99.87%

URIBL (MX Tools)

SC rate: 12.02%
FP rate: 0.01%
Final score: 11.94
Project Honey Pot SC rate: 25.03%
Abusix SC rate: 2.34%
Newsletters FP rate: 0.0%
Malware SC rate: 0.03%

CONCLUSION

The message throughout the last 50 VBSpam tests has been a fairly positive one: despite the fact that the spam landscape changes constantly (and the product market with it: the 'spam filters' we started testing in 2009 are now sold as 'email security solutions'), the overwhelming majority of spam is blocked by a wide range of solutions. While we continue to be critical when looking at individual product performance, we are happy to be the deliverers of this good news.

The next test report, which is to be published in March 2018, will once again report on 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 16 days, from 12am on 11 November to 12am on 27 November 2017. The test corpus consisted of 161,649 emails. 154,687 of these were spam, 65,964 of which were provided by *Project Honey Pot*, with the remaining 88,723 spam emails provided by *spamfeed.me*, a product from *Abusix*. There were 6,675 legitimate emails ('ham') and 287 newsletters.

Moreover, 5,989 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[4]. 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 positives 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.

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

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.

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

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	6671	4	0.06%	371	154316	99.76%	SPAM Verified	99.42
Bitdefender	6675	0	0.00%	55	154632	99.96%	SPAM + Verified	99.96
CYREN	6675	0	0.00%	1711	152976	98.89%	SPAM Verified	98.83
ESET	6675	0	0.00%	5	154682	99.997%	SPAM + Verified	99.997
Forcepoint	6668	7	0.10%	894	153793	99.42%	SPAM Verified	98.89
FortiMail	6675	0	0.00%	10	154677	99.99%	SPAM + Verified	99.99
IBM	6675	0	0.00%	29	154658	99.98%	SPAM + Verified	99.97
Kaspersky for Exchange	6675	0	0.00%	21	154666	99.99%	SPAM + Verified	99.99
Kaspersky LMS	6675	0	0.00%	14	154673	99.99%	SPAM + Verified	99.99
Libra Esva	6675	0	0.00%	74	154613	99.95%	SPAM + Verified	99.92
OnlyMyEmail	6675	0	0.00%	0	154687	100.00%	SPAM + Verified	99.97
Scrollout	6654	21	0.31%	54	154633	99.97%	SPAM Verified	98.20
Vade Secure Cloud	6647	28	0.42%	533	154154	99.66%	X	97.55
ZEROSPAM	6675	0	0.00%	67	154620	99.96%	SPAM Verified	99.81
IBM X-Force Combined*	6674	1	0.01%	7224	147463	95.33%	N/A	95.26
IBM X-Force IP*	6674	1	0.01%	11004	143683	92.89%	N/A	92.81
IBM X-Force URL*	6675	0	0.00%	123778	30909	19.98%	N/A	19.98
Spamhaus DBL*	6675	0	0.00%	134744	19943	12.89%	N/A	12.89
Spamhaus ZEN*	6675	0	0.00%	5345	149342	96.54%	N/A	96.54
Spamhaus ZEN+DBL*	6675	0	0.00%	3967	150720	97.44%	N/A	97.44
URIBL*	6674	1	0.01%	136100	18587	12.02%	N/A	11.94

**The IBM X-Force, Spamhaus 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	3	1.1%	1	99.98%	340	99.48%	31	99.97%	0.70	●	●	●	●
Bitdefender	0	0.0%	0	100.00%	48	99.93%	7	99.99%	1.26	●	●	●	●
CYREN	4	1.4%	31	99.48%	1471	97.77%	240	99.73%	3.00	●	●	●	●
ESET	0	0.0%	0	100.00%	3	99.995%	2	99.998%	0.05	●	●	●	●
Forcepoint	1	0.4%	0	100.00%	849	98.71%	45	99.95%	1.26	●	●	●	●
FortiMail	0	0.0%	0	100.00%	1	99.998%	9	99.99%	0.04	●	●	●	●
IBM	1	0.4%	1	99.98%	24	99.96%	5	99.99%	0.12	●	●	●	●
Kaspersky for Exchange	0	0.0%	7	99.88%	8	99.99%	13	99.99%	0.64	●	●	●	●
Kaspersky LMS	0	0.0%	0	100.00%	6	99.99%	8	99.99%	0.09	●	●	●	●
Libra Esva	2	0.7%	0	100.00%	59	99.91%	15	99.98%	0.36	●	●	●	●
OnlyMyEmail	2	0.7%	0	100.00%	0	100.00%	0	100.00%	0.00	●	●	●	●
Scrollout	14	4.9%	1	99.98%	44	99.93%	10	99.99%	0.26	●	●	●	●
Vade Secure Cloud	2	0.7%	3	99.95%	418	99.37%	115	99.87%	0.99	●	●	●	●
ZEROSPAM	10	3.5%	0	100.00%	50	99.92%	17	99.98%	0.31	●	●	●	●
IBM X-Force Combined*	0	0.0%	133	97.78%	3062	95.36%	4162	95.31%	5.51	N/A	N/A	N/A	N/A
IBM X-Force IP*	0	0.0%	133	97.78%	6231	90.55%	4773	94.62%	7.01	N/A	N/A	N/A	N/A
IBM X-Force URL*	0	0.0%	5981	0.13%	37654	42.92%	86125	2.93%	19.15	N/A	N/A	N/A	N/A
Spamhaus DBL*	0	0.0%	5956	0.55%	48407	26.62%	86337	2.69%	12.96	N/A	N/A	N/A	N/A
Spamhaus ZEN*	0	0.0%	8	99.87%	3896	94.09%	1449	98.37%	4.51	N/A	N/A	N/A	N/A
Spamhaus ZEN+DBL*	0	0.0%	8	99.87%	2956	95.52%	1011	98.86%	3.64	N/A	N/A	N/A	N/A
URIBL*	0	0.0%	5987	0.03%	49455	25.03%	86645	2.34%	12.61	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
Forcepoint	Forcepoint Advanced Malware Detection		√	√	√	√	√
OnlyMyEmail	Proprietary (optional)		√	√	*	√	√
Vade Secure Cloud	DrWeb; proprietary	√	√	√		√	√
ZEROSPAM	ClamAV			√		√	√

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

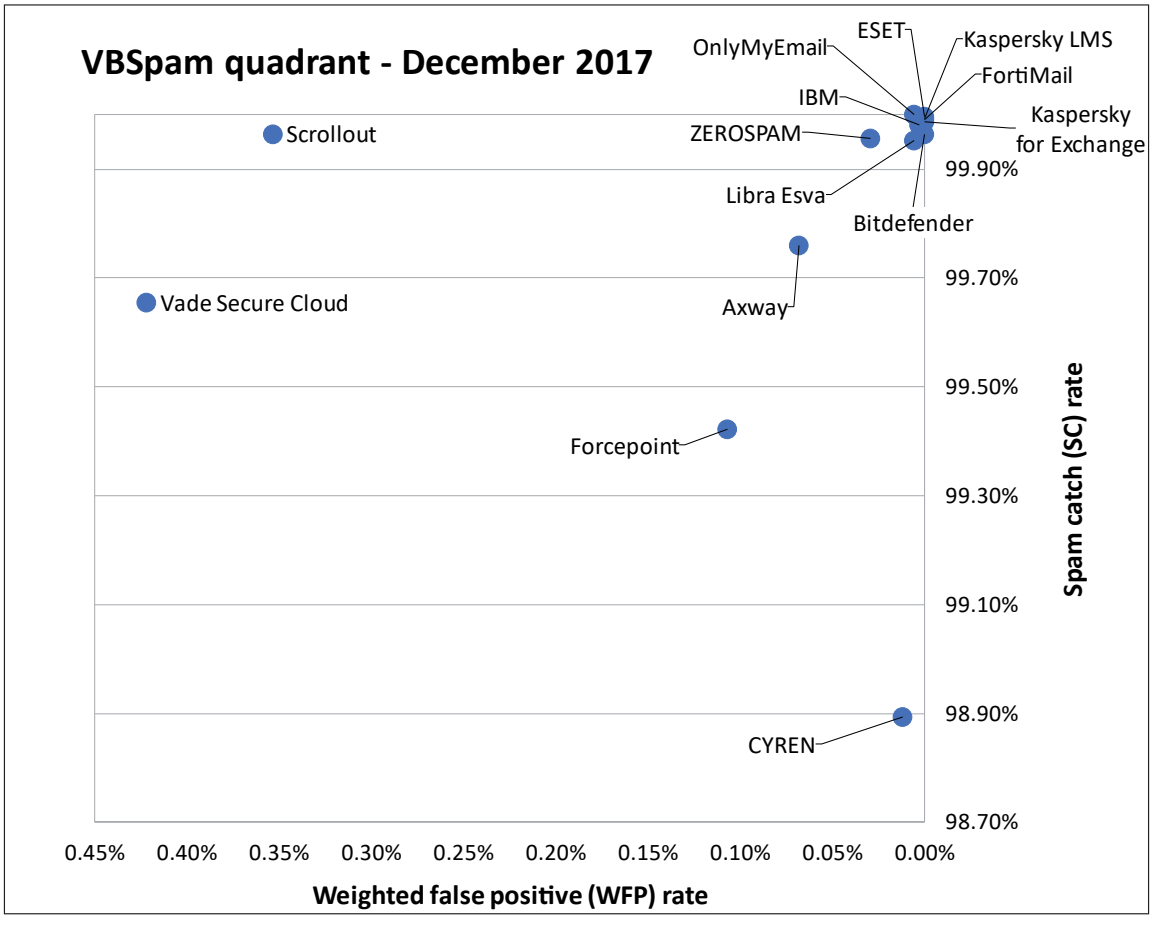
(Please refer to the text for full product names.)

Local solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Interface			
						CLI	GUI	Web GUI	API
Axway MailGate	Kaspersky, McAfee	√	√	√				√	
Bitdefender	Bitdefender	√				√		√	√
CYREN	CYREN			√			√		√
ESET	ESET Threatsense	√	√	√	√	√	√		
FortiMail	Fortinet	√	√	√	√	√		√	√
IBM	Sophos; IBM Remote Malware Detection			√		√		√	
Kaspersky for Exchange	Kaspersky Lab	√		√		√		√	
Kaspersky LMS	Kaspersky Lab	√		√	√	√		√	
Libra Esva	ClamAV; others optional		√	√		√		√	
Scrollout	ClamAV			√		√		√	√

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

Products ranked by final score	
ESET	99.997
FortiMail	99.99
Kaspersky LMS	99.99
Kaspersky for Exchange	99.99
OnlyMyEmail	99.97
IBM	99.97
Bitdefender	99.96
Libra Esva	99.92
ZEROSPAM	99.81
Axway	99.42
Forcepoint	98.89
CYREN	98.83
Scrollout	98.20
Vade Secure Cloud	97.55

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



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