virus BULLETIN Covering the global threat landscape

VB ESA - M365 COMPARATIVE TEST REPORT
Email Security Add-ons for Microsoft 365

Test period: 2026-08-01 to 2026-08-16

Test methodology: https://www.virusbulletin.com/testing/vb-esa-m365/vb-esa-m365-methodology/

Coro Email Security

Elpha Secure

FOREWORD

This report presents the results of the VB ESA - M365 comparative test covering the period from 1 to 16 August 2026. Whilst the test programme runs continuously, results from official test periods such as this one form the basis of public VB ESA - M365 certification.

Two products participated in this test period under public participation terms: *Coro Email Security* and *Elpha Secure*, integrated via API as integrated cloud email security (ICES) solutions. The spam corpus in this period was dominated by *Project Honey Pot* samples, which accounted for approximately 71% of total spam volume. Readers should bear this in mind when interpreting aggregate spam IDR figures, as overall scores are weighted heavily towards performance on that feed.

Elpha Secure achieved VB ESA - M365 certification; *Coro Email Security* achieved VB ESA - M365+ certification in this period. *Coro Email Security* is awarded the Top Performer badge for this period.

We intend to publish VB ESA - M365 results on a regular cadence going forward, building a longitudinal picture of how add-on products perform in the real-world *Microsoft 365* environment over time.

— *Virus Bulletin Team, September 2026*

1. EXECUTIVE SUMMARY

Two products completed the Q3 2026 VB ESA - M365 test period under public participation terms: *Coro Email Security* and *Elpha Secure*.

Both products are VB ESA - M365 certified in this period.

Results at a glance

Coro Email Security: **Spam IDR** 96% **| False positives** 0 **| ✓ VB ESA - M365+ | ✓ Malware 100 | ✓ Phishing 100**

Elpha Secure: **Spam IDR** 94% **| False positives** 0 **| ✓ VB ESA - M365 | ✓ Malware 100**

Microsoft 365 (*Exchange Online Protection* alone) passed 131 of 93,734 spam-feed messages, four of 9,725 phishing samples, and 21 of 1,013 malware samples through to the inbox in this period.

Full per-product results, the combined comparative table, and the test methodology follow in Sections 3–6 of this report.

Note on Microsoft 365: *This report does not evaluate Microsoft 365 or Exchange Online Protection. Microsoft 365 is used solely as a comparative base to isolate the incremental value each tested add-on provides on top of native filtering. Results for Microsoft 365 reflect the specific tenant configuration, licensing tier, and sample mix used in this test instance and cannot be generalized to other deployments. No conclusions about Microsoft 365's general effectiveness should be drawn from this report.*

2. THE VB ESA - M365 TEST

VB ESA - M365 is *Virus Bulletin*'s continuously running test programme for products that supplement *Microsoft 365*'s native email security – *Exchange Online Protection* (*EOP*) – with an additional detection layer. It covers integrated cloud email security (ICES) solutions, which connect via API without changing MX records.

Tested products are exposed to a continuous, live stream of real-world email: spam drawn from third-party spam feed providers including *Abusix* and *Project Honey Pot*; phishing emails containing credential-theft or malware-delivery links; malware-bearing attachments; and legitimate ham and newsletter traffic. No email is artificially constructed for the test – all test cases are in the wild.

2.1 What is actually being measured

The test is built around a *Microsoft 365* comparative base consisting of the set of samples that *Microsoft 365* itself disposed of (marking them as 'Failed' or 'FilteredAsSpam' in every test instance, or 'Quarantined' in at least one) and which therefore fall outside the scope of evaluation for the tested add-on products. Samples in this base are excluded from product scoring entirely. The samples that remain (the 'residual sample set') are what actually reached each product, and it is on this residual set alone that detection and false-positive performance is measured.

The three status values used to exclude samples are native *Microsoft 365* / *Exchange Online Protection* labels. Each exclusion rule reflects what actually happens to that message in production:

- **Failed**: The message never leaves *Microsoft 365*'s infrastructure; it is rejected or bounced before delivery. No add-on ever processes it.
- **FilteredAsSpam**: *Microsoft 365* consistently diverts the message to the Junk Email folder. In a real deployment the add-on only sees mail that *EOP* passes, not mail that it catches, so these samples are excluded. The 'every instance' threshold avoids penalizing products for occasional *EOP* inconsistency.
- **Quarantined**: *Microsoft 365* places the message under administrative hold, removing it from user reach entirely. The 'at least once' condition (versus 'every instance' for junk) reflects that quarantining a message is a strong and deliberate action, unlikely to be accidental.

In any of these cases, scoring an add-on against these samples would measure something that doesn't happen in a live environment. The residual set is therefore the most accurate proxy for what a product actually sees, and must handle, when deployed alongside *Microsoft 365*.

2.2 Incremental detection rate (IDR)

The primary detection metric is the incremental detection rate, or IDR:

IDR = (number of malicious samples detected by the add-on) ÷ (number of malicious samples that passed *Microsoft 365* filtering)

'Detected' means any add-on action that prevents delivery or places the message under administrative control (typically a block or quarantine).

2.3 Certifications and badges

The VB ESA - M365 test programme recognizes exceptional performance through a series of awards and badges.

Award	Criteria
VB ESA - M365	Spam IDR ≥ 80%; false positives ≤ 1; newsletter false positives ≤ 3
VB ESA - M365+	Spam IDR ≥ 95%; 0 false positives; 0 newsletter false positives

Badge	Criteria
Top Performer	Highest spam IDR in the test period; 0 false positives; 0 newsletter false positives
Phishing 100	0 phishing false negatives
Malware 100	0 malware false negatives

3. TEST ENVIRONMENT

Testing was conducted against a *Microsoft 365* tenant licensed on *Microsoft 365 Business Basic* / *Business Standard* – *Exchange Online Protection* only, with no *Defender for Office 365* overlay, so that measured results are attributable to the tested add-ons rather than to a richer native *Microsoft* stack. Each product received live email continuously via a dedicated *Exchange* admin centre connector for the duration of the test period. The test period ran for 16 days (2026-08-01 to 2026-08-16), with an average of 5,858 spam samples per day.

3.1 Sample volumes

The following tables show the total test-case volumes for the test period, and the number of each that passed *Microsoft 365* filtering into the residual sample set.

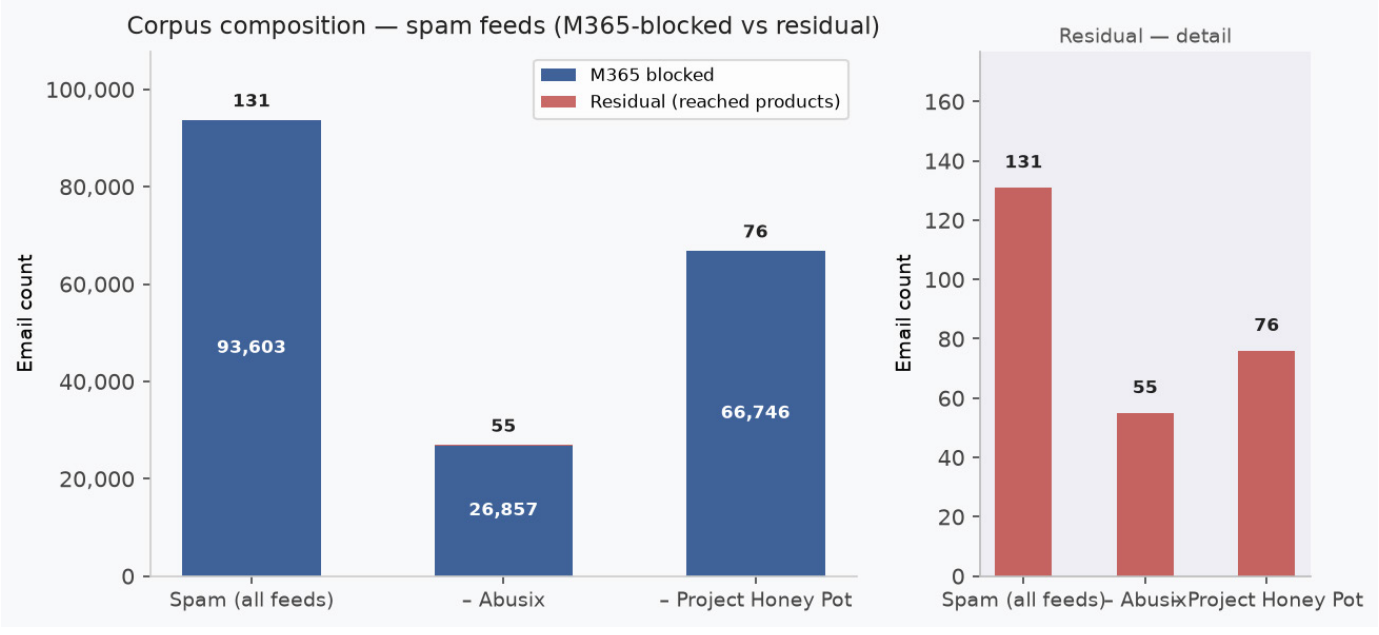
Malicious email

Category	Total	% of spam corpus	M365 blocked	Residual	Residual %
Spam (all feeds)	93,734	100%	93,603	131	0.14%
- Abusix feed	26,912	28.7%	26,857	55	0.20%
- Project Honey Pot feed	66,822	71.3%	66,746	76	0.11%
Phishing	9,725	10.4%	9,721	4	0.04%
Malware	1,013	1.1%	992	21	2.11%

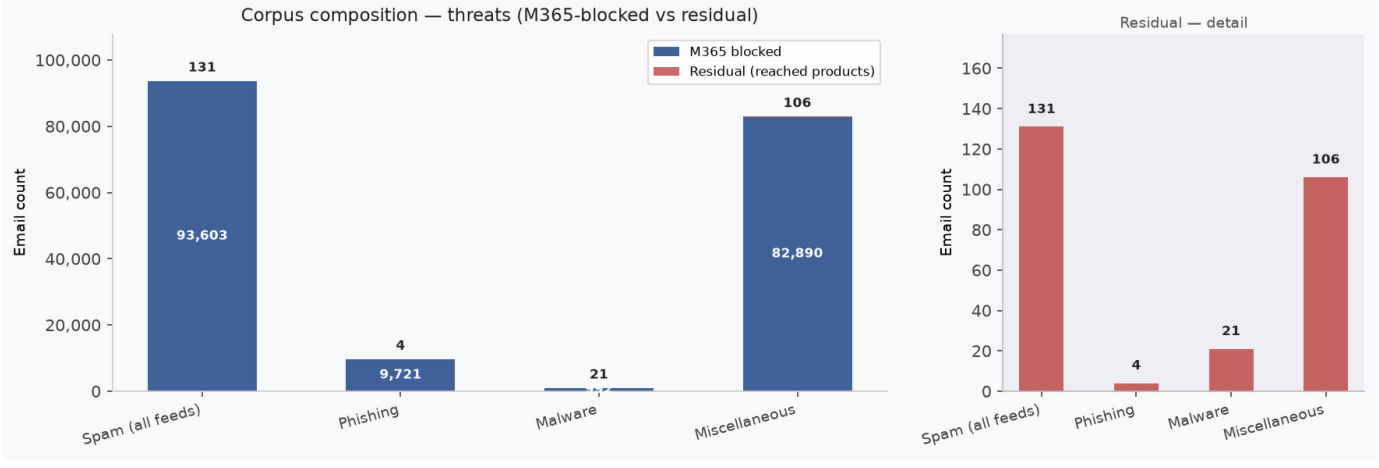
Legitimate email

Category	Total	M365 false positives	Residual (correctly passed)	Residual %
Ham	536	386	150	27.98%
Newsletters	0	N/A	N/A	N/A

Microsoft 365 itself generated 386 ham false positives this period – blocking 386 legitimate messages before the add-ons were involved. *Coro Email Security* and *Elpha Secure* each preserved all 150 ham messages correctly passed by M365, adding zero further false positives.



Spam feed corpus composition.



Threat corpus composition.

Note on the newsletter feed

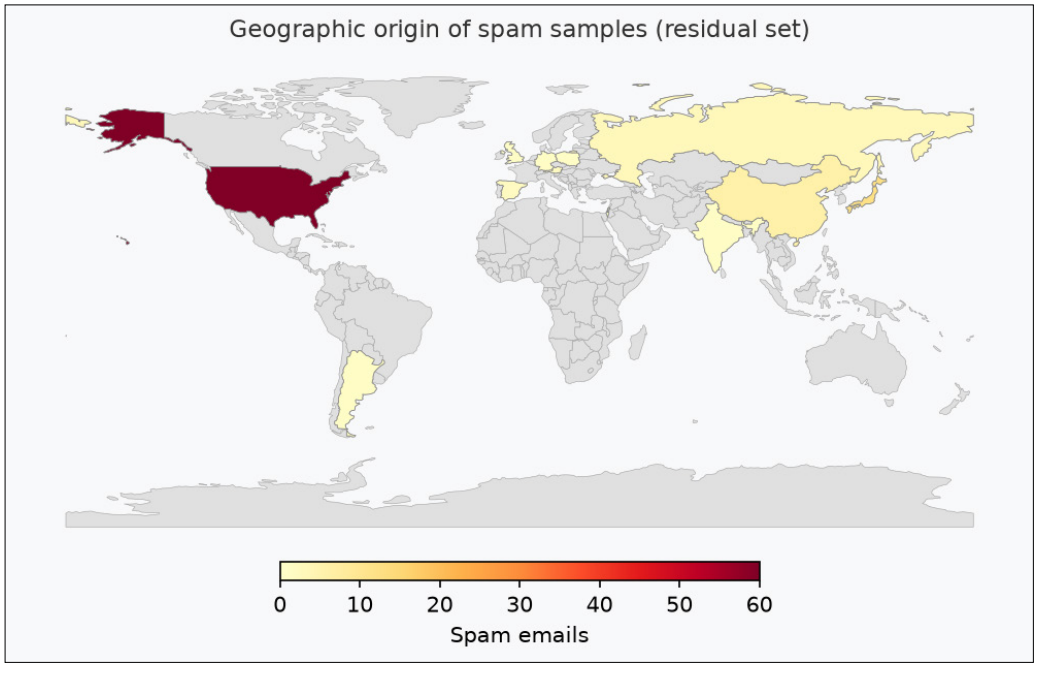
No newsletter samples were submitted during this test period. The newsletter feed is operated on a best-effort basis and may be empty in some test periods, depending on availability. False-positive scoring for newsletters is therefore not applicable for this test.

3.2 Geographic origin of spam samples

The following table shows the number of spam samples in the residual set by country of origin[1], as determined by GeoIP lookup on the sending IP address.

[1] Seven emails could not be geo-located ('IP Address not found') and are excluded from the table.

Country	Spam emails
United States	60
Hong Kong	24
Japan	12
France	9
China	6
Russian Federation	3
Austria	2
Spain	2
Argentina	1
India	1
Poland	1
United Kingdom	1
Israel	1
Germany	1



4. OVERALL RESULTS

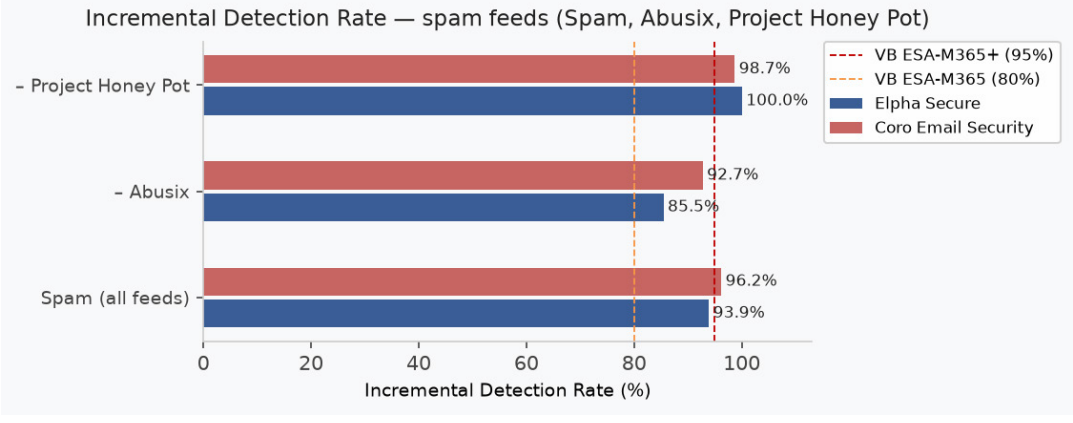
The table that follows summarizes the participating products' performance on the residual sample set for this test period.

Metric	Coro Email Security	Elpha Secure
Spam IDR	96.2%	93.9%
Residual spam caught	126 of 131	123 of 131
- Abusix feed	51 of 55	47 of 55
- Project Honey Pot feed	75 of 76	76 of 76
False positives - Ham	0	0
False positives - Newsletters	N/A	N/A
Phishing false negatives	0 of 4 residual	1 of 4 residual
Malware false negatives	0 of 21 residual	0 of 21 residual
Award	**VB ESA - M365+**	**VB ESA - M365**
Badges	**Top Performer**, **Malware 100**, **Phishing 100**	**Malware 100**

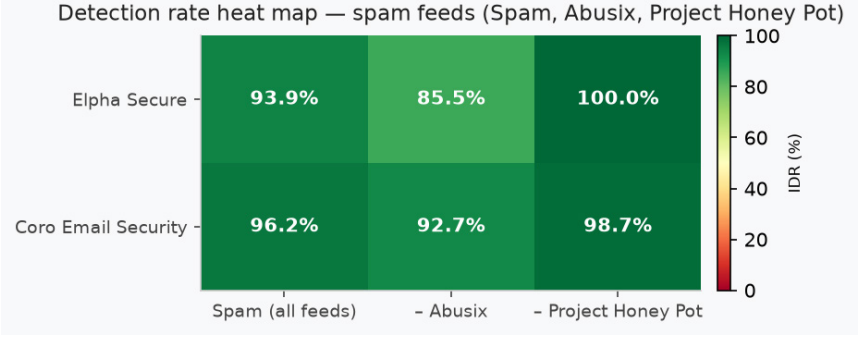
Incremental value over M365 alone – spam

The following table outlines how much each product adds on top of native *Microsoft 365* filtering.

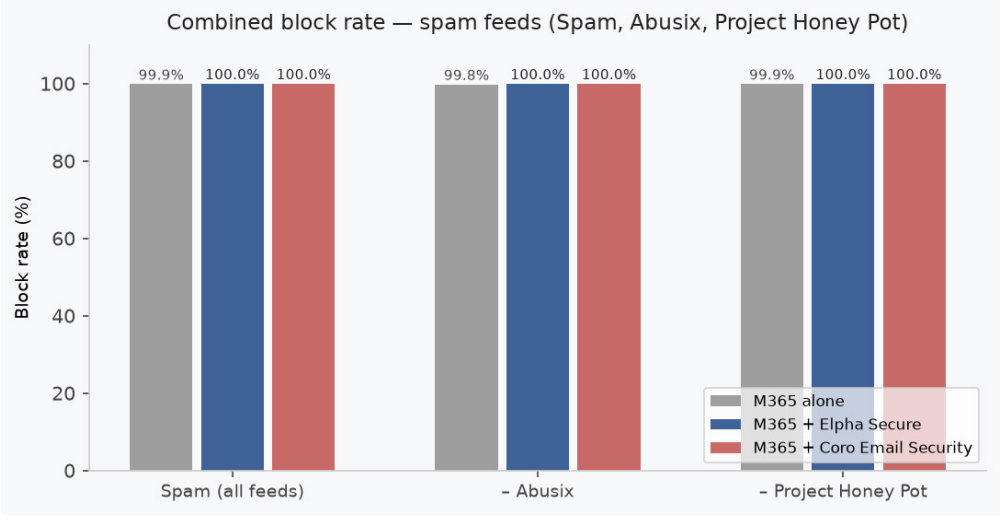
Metric	Coro Email Security	Elpha Secure
Block rate M365 alone	99.86%	99.86%
Block rate M365 + product	99.99%	99.99%
Incremental gain	**+0.13pp**	**+0.13pp**



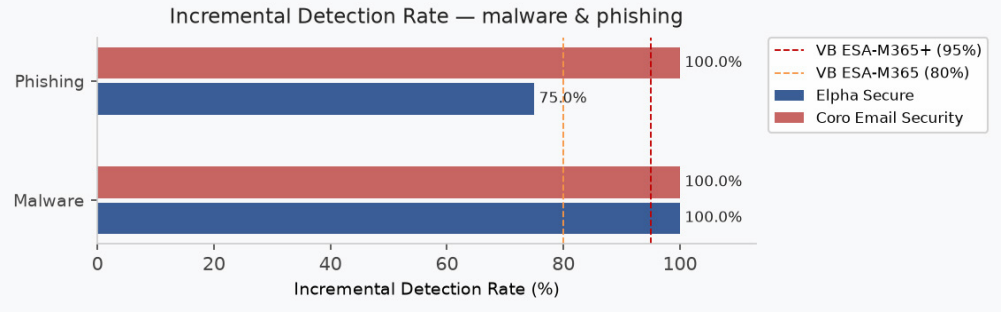
Incremental detection rates across spam feeds.



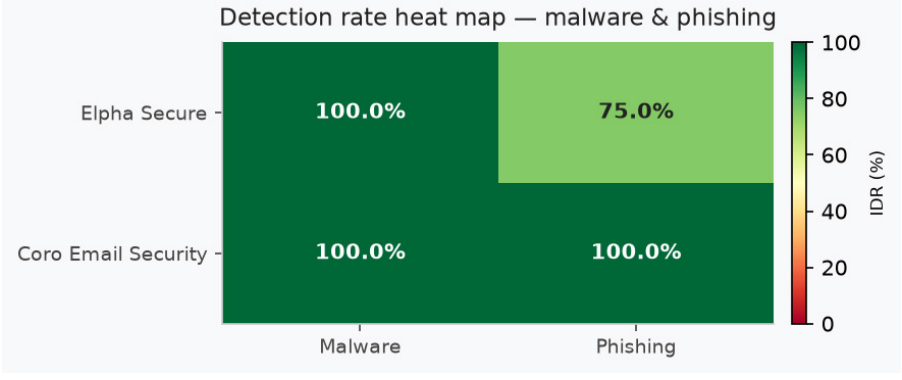
Spam detection rate heat map.



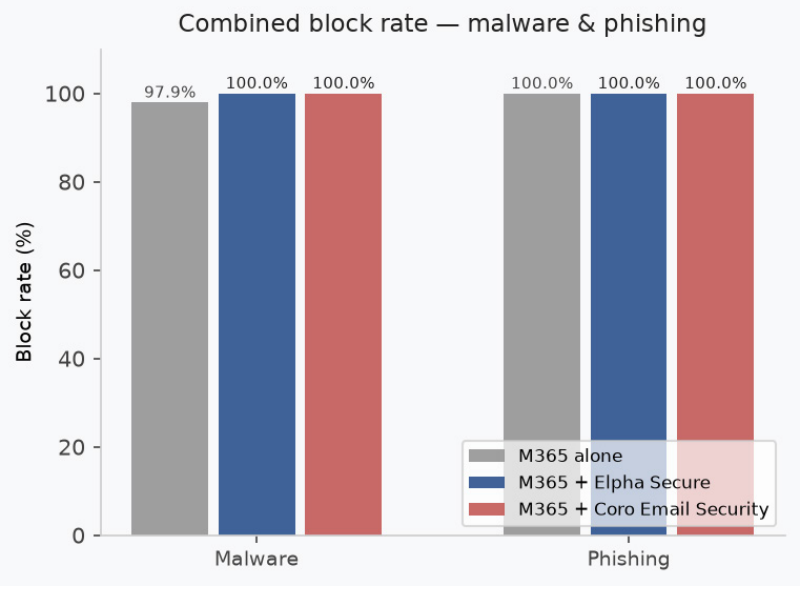
Block rate of M365 alone vs M365 + product across spam feeds.



Incremental detection rates across malware and phishing feeds.



Malware and phishing detection rate heat map.



Block rate of M365 alone vs M365 + product across malware and phishing feeds.

5. PRODUCT RESULTS

5.1 Coro Email Security

- **Website:** https://www.coro.net
- **How to integrate with Microsoft 365:** https://docs.coro.net/protection/connecting-to-m365/

✓ VB ESA - M365+ | ✓ Top Performer | ✓ Phishing 100 | ✓ Malware 100

Spam IDR 96.2% **| False positives (Ham + Newsletter)** 0

Coro Email Security detected 126 of the 131 residual spam samples submitted to it, missing five messages. It correctly allowed through all ham traffic.

- False positives against ham traffic: 0
- Phishing false negatives: 0 of 4 residual
- Malware false negatives: 0 of 21 residual

Detection performance

Feed	Residual set	Caught	Missed	IDR (caught ÷ residual)
Spam (all feeds)	131	126	5	126 ÷ 131 = 96.2%
- Abusix feed	55	51	4	51 ÷ 55 = 92.7%
- Project Honey Pot feed	76	75	1	75 ÷ 76 = 98.7%
Phishing	4	4	0	4 ÷ 4 = 100.0%
Malware	21	21	0	21 ÷ 21 = 100.0%

Note: The Abusix IDR (92.7%) and the Project Honey Pot IDR (98.7%) diverge by 6.0 percentage points. Both are third-party spam feeds of the same type, but the Abusix residual is smaller (55 samples) – each missed message on Abusix costs 1.8 percentage points, amplifying the visible gap.

Legitimate mail handling

Feed	Total	M365 correctly passed	Product FPs (blocked)	Delivered	Quarantined	Failed	Spam-foldered
Ham	536	150	0	347	0	0	189
Newsletters	0	N/A	N/A	N/A	N/A	N/A	N/A

Message disposition – all feeds

Feed	Total	Passed	Blocked	Delivered	Quarantined	Failed	Spam-foldered
Ham	536	345	191	347	0	0	189
Newsletters	0	N/A	N/A	N/A	N/A	N/A	N/A
Spam (all)	93,734	14	93,720	316	6,834	17,568	69,004
- Abusix feed	26,912	9	26,903	108	1,860	4,725	20,216
- Project Honey Pot feed	66,822	5	66,817	208	4,974	12,843	48,788
Phishing	9,725	0	9,725	9	1,026	6,572	2,117
Malware	1,013	1	1,012	23	83	830	77

Spam detection by email language

Language	Total samples	Blocked	Block rate
GB English	88	85	96.6%
JP Japanese	11	10	90.9%
ES Spanish	9	9	100.0%
FR French	9	9	100.0%
CN Chinese	6	5	83.3%
DE German	4	4	100.0%
PT Portuguese	2	2	100.0%
IL Hebrew	1	1	100.0%
BG Bulgarian	1	1	100.0%

Combined performance – M365 + Coro Email Security

The following table shows the combined effect of *Microsoft 365* native filtering and the product acting together. For malicious feeds, a higher combined block rate is better. For legitimate feeds, a lower combined block rate is better (blocked = false positive).

Feed	Total	M365 blocked	Additional blocked by product	Combined blocked	Delivered to inbox	Combined block rate
Ham	536	386	0	386	150	72.01%
Newsletters	0	N/A	N/A	N/A	N/A	N/A
Spam (all feeds)	93,734	93,603	126	93,729	5	99.99%
- Abusix feed	26,912	26,857	51	26,908	4	99.98%
- Project Honey Pot feed	66,822	66,746	75	66,821	1	99.998%
Phishing	9,725	9,721	4	9,725	0	100.00%
Malware	1,013	992	21	1,013	0	100.00%

5.2 Elpha Secure

- **Website:** https://www.elphasecure.com
- **How to integrate with Microsoft 365:** https://www.elphasecure.com/technology/how-it-works

✓ VB ESA - M365 | — Top Performer | — Phishing 100 | ✓ Malware 100

Spam IDR 93.9% **| False positives (Ham + Newsletter)** 0

Elpha Secure detected 123 of the 131 residual spam samples submitted to it, missing eight messages. It correctly allowed through all ham traffic.

- False positives against ham traffic: 0
- Phishing false negatives: 1 of 4 residual
- Malware false negatives: 0 of 21 residual

Detection performance

Feed	Residual set	Caught	Missed	IDR (caught ÷ residual)
Spam (all feeds)	131	123	8	123 ÷ 131 = 93.9%
- Abusix feed	55	47	8	47 ÷ 55 = 85.5%
- Project Honey Pot feed	76	76	0	76 ÷ 76 = 100.0%
Phishing	4	3	1	3 ÷ 4 = 75.0%
Malware	21	21	0	21 ÷ 21 = 100.0%

Note: The Abusix IDR (85.5%) and the Project Honey Pot IDR (100.0%) diverge by 14.5 percentage points. Both are third-party spam feeds of the same type, but the Abusix residual is smaller (55 samples) – each missed message on Abusix costs 1.8 percentage points, amplifying the visible gap.

Legitimate mail handling

Feed	Total	M365 correctly passed	Product FPs (blocked)	Delivered	Quarantined	Failed	Spam-foldered
Ham	536	150	0	231	0	2	303
Newsletters	0	N/A	N/A	N/A	N/A	N/A	N/A

Message disposition — all feeds

Feed	Total	Passed	Blocked	Delivered	Quarantined	Failed	Spam-foldered
Ham	536	231	298	231	0	2	303
Newsletters	0	N/A	N/A	N/A	N/A	N/A	N/A
Spam (all)	93,734	11	93,723	340	5,327	19,366	68,692
- Abusix feed	26,912	10	26,902	112	1,312	5,439	20,047
- Project Honey Pot feed	66,822	1	66,821	228	4,015	13,927	48,645
Phishing	9,725	1	9,724	11	1,093	6,510	2,110
Malware	1,013	0	1,013	23	63	850	77

Spam detection by email language

Language	Total samples	Blocked	Block rate
GB English	88	87	98.9%
JP Japanese	11	6	54.5%
ES Spanish	9	9	100.0%
FR French	9	8	88.9%
CN Chinese	6	5	83.3%
DE German	4	4	100.0%
PT Portuguese	2	2	100.0%
IL Hebrew	1	1	100.0%
BG Bulgarian	1	1	100.0%

Combined performance – M365 + Elpha Secure

The following table shows the combined effect of *Microsoft 365* native filtering and the product acting together. For malicious feeds, a higher combined block rate is better. For legitimate feeds, a lower combined block rate is better (blocked = false positive).

Feed	Total	M365 blocked	Additional blocked by product	Combined blocked	Delivered to inbox	Combined block rate
Ham	536	386	0	386	150	72.01%
Newsletters	0	N/A	N/A	N/A	N/A	N/A
Spam (all feeds)	93,734	93,603	123	93,726	8	99.99%
- Abusix feed	26,912	26,857	47	26,904	8	99.97%
- Project Honey Pot feed	66,822	66,746	76	66,822	0	100.00%
Phishing	9,725	9,721	3	9,724	1	99.99%
Malware	1,013	992	21	1,013	0	100.00%

6. METHODOLOGY SUMMARY

6.1 Full methodology and procedure

The full methodology, award criteria, and test procedure can be found at: https://www.virusbulletin.com/testing/vb-esa-m365/vb-esa-m365-methodology/.

6.2 Message trace field definitions

All per-message status values in this report are extracted from the *Microsoft 365* message trace facility. Message traces can be accessed by *Exchange* administrators at:

- https://admin.cloud.microsoft/exchange#/messagetrace

Each message submitted to the test is injected into a dedicated *Microsoft 365* tenant and its fate recorded by querying the message trace API. The fields below correspond to the status values returned and used throughout this report.

Field	M365 message trace status	Meaning in this report
Passed	Status not in {Failed, FilteredAsSpam, Quarantined}	Message was not blocked either by *Microsoft 365* or by the filter under test and reached the recipient. For malicious feeds this is a false negative; for legitimate feeds this is correct delivery.

Field	M365 message trace status	Meaning in this report
Blocked	Failed, FilteredAsSpam, or Quarantined	Message was stopped by the filter. For malicious feeds this is a true positive; for legitimate feeds this is a false positive.
Delivered	Delivered	Message was delivered to the recipient's inbox by *Microsoft 365*.
Quarantine	Quarantined	Message was held in the *Microsoft 365* quarantine store, accessible only to admins or end-users via the Quarantine portal. Not delivered to the inbox.
Failed	Failed	*Microsoft 365* rejected or permanently failed to deliver the message (e.g. NDR, connection failure, or policy rejection). The message never reached the recipient's mailbox.
Spam-foldered (FilteredAsSpam)	FilteredAsSpam	*Microsoft 365* identified the message as spam and delivered it to the recipient's Junk Email folder rather than the inbox.
Extra blocked (extra_blocked)	N/A	Messages blocked by the tested add-on that *Microsoft 365* itself passed. For malicious feeds: incremental true positives (IDR numerator). For legitimate feeds: add-on false positives.
Extra passed (extra_passed)	N/A	Messages passed by the tested add-on that *Microsoft 365* blocked. Rarely non-zero; included for completeness.

7. ABOUT VB ESA - M365

VB ESA - M365 is *Virus Bulletin*'s comparative test programme for products that supplement *Microsoft 365* email security. Products may participate publicly, with results published as in this report, or privately, receiving only non-comparative feedback. Public test participants are tested over a continuous one-year cycle, within which four periods are designated as official test periods; results from official periods form the basis of public certification.

Vendors wishing to enrol a product in VB ESA - M365 can find participation details at https://www.virusbulletin.com/testing/vb-esa-m365/vb-esa-m365-vendors/.

Head of Testing: Peter Karsai

Security Test Engineers:
Klaudia Kitti Csia, Adrian Luca, Ionuț Răileanu

Operations Manager: Bálint Tanos

Sales Executive: Allison Sketchley

Marketing Manager: David Kelemen

Editorial Assistant: Helen Martin

Telephone: +44 20 3920 6348
Email: vbtest@virusbulletin.com
Web: www.virusbulletin.com

Manor House, Howbery Business Park
Wallingford OX10 8BA
UK