virus BULLETIN Covering the global threat landscape

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

Test period: 2026-05-02 to 2026-05-18

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

Elpha Secure

Coro Email Security

FOREWORD

This report presents the results of the inaugural VB ESA - M365 comparative test, covering the period from 2 to 18 May 2026. The VB ESA - M365 programme is the result of several months of development and infrastructure work, and this first report marks the beginning of what will be a continuously running test alongside the established VBSpam test.

The VB ESA - M365 test runs in parallel with VBSpam and shares the same live email corpus. The key distinction is in scope: whereas VBSpam measures a product's performance across the full corpus, VB ESA - M365 focuses specifically on the subset of samples that qualify for the *Microsoft 365* comparative baseline – those that *Exchange Online Protection*, running without any *Defender for Office 365* overlay, passes through to the tested product. This residual set is what actually reaches each product in a real-world *Microsoft 365* deployment, making the results directly applicable to organizations that have standardized on *Microsoft 365* and are evaluating add-on security layers.

This framing is what sets VB ESA - M365 apart. The incremental detection rate measures not how good a product is in isolation, but how much it genuinely adds on top of what *Microsoft 365* already does.

Two products participated in this first public test period: *Elpha Secure* and *Coro Email Security*. Both products integrated via API as integrated cloud email security (ICES) solutions.

The spam corpus in this test period was dominated by *Project Honey Pot* samples, which accounted for approximately 84% 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. *Microsoft 365* proved unusually effective against phishing and malware during this period, intercepting all samples in the phishing category before they reached the add-ons.

Both products achieved VB ESA - M365 certification this period, with zero false positives against legitimate mail. *Elpha Secure* is awarded the Top Performer badge for this inaugural test.

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

— *Virus Bulletin Team, June 2026*

1. EXECUTIVE SUMMARY

Two products completed the 2026-05-02 to 2026-05-18 VB ESA - M365 test period under public participation terms: *Elpha Secure* and *Coro Email Security*.

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

Results at a glance

Elpha Secure: **Spam IDR** 99% **| False positives** 0 **| ✓ VB ESA - M365+ | ✓ Top Performer | ✓ Malware 100**

Coro Email Security: **Spam IDR** 92% **| False positives** 0 **| ✓ VB ESA - M365 | ✓ Malware 100**

Microsoft 365 (*Exchange Online Protection* alone) passed 108 of 25,610 spam-feed messages, 0 of 3,704 phishing samples, and 6 of 234 malware samples through to the inbox in this period.

Full per-product results, a 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 two product categories: integrated cloud email security (ICES) solutions, which connect via API without changing MX records, and secure email gateways (SEGs), which sit in front of *Microsoft 365* via MX routing.

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 email 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?

In order to measure what each product adds on top of the protection already provided by *Microsoft 365* we start by creating a comparative base, consisting of all the 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 set 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 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 thus the most accurate representation of 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; 0 false positives; 0 newsletter false positives
Malware 100	0 malware false negatives; 0 false positives; 0 newsletter false positives

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 17 days (2026-05-02 to 2026-05-18), with an average of 1,506 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.

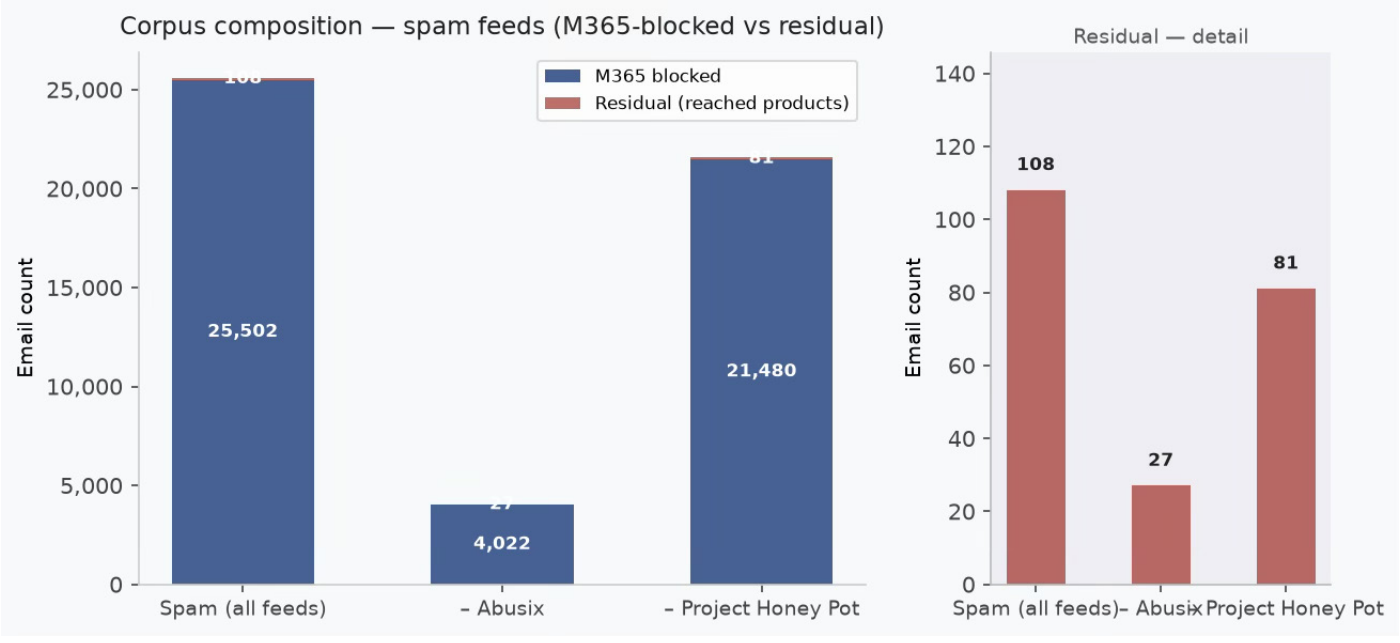
Malicious email

Category	Total	% of spam corpus	M365 blocked	Residual	Residual %
Spam (all feeds)	25,610	100.0%	25,502	108	0.4%
- Abusix feed	4,049	15.8%	4,022	27	0.7%
- Project Honey Pot feed	21,561	84.2%	21,480	81	0.4%
Phishing	3,704	14.5%	3,704	0	0.0%
Malware	234	0.9%	228	6	2.6%

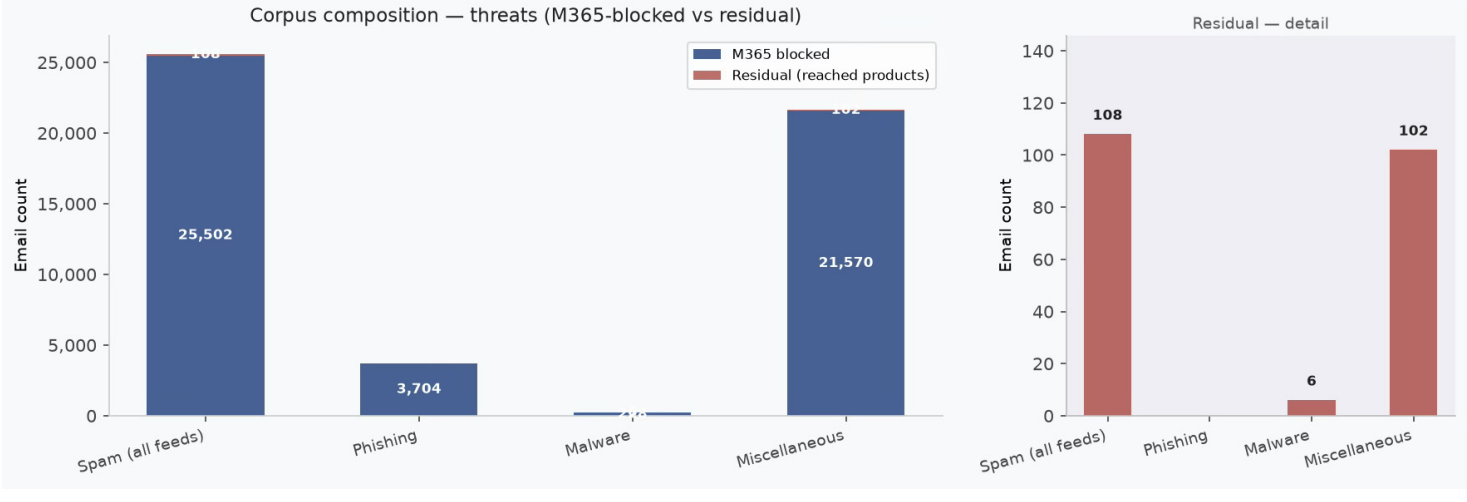
Legitimate email

Category	Total	M365 false positives	Residual (correctly passed)	Residual %
Ham	376	5	371	98.7%
Newsletters	0	0	0	N/A

Microsoft 365 itself generated five ham false positives this period – blocking five legitimate messages before the add-ons were involved. Both *Elpha Secure* and *Coro Email Security* allowed through all 371 of the ham messages correctly passed by *M365*, adding no further false positives.



Spam feed corpus composition.



Malware and phishing corpus composition.

Note on the empty phishing residual set

Microsoft 365 intercepted all submitted phishing samples in this test period, leaving no residual for the add-ons to act on. Therefore, no phishing badges are awarded on this occasion.

Note on the newsletter feed

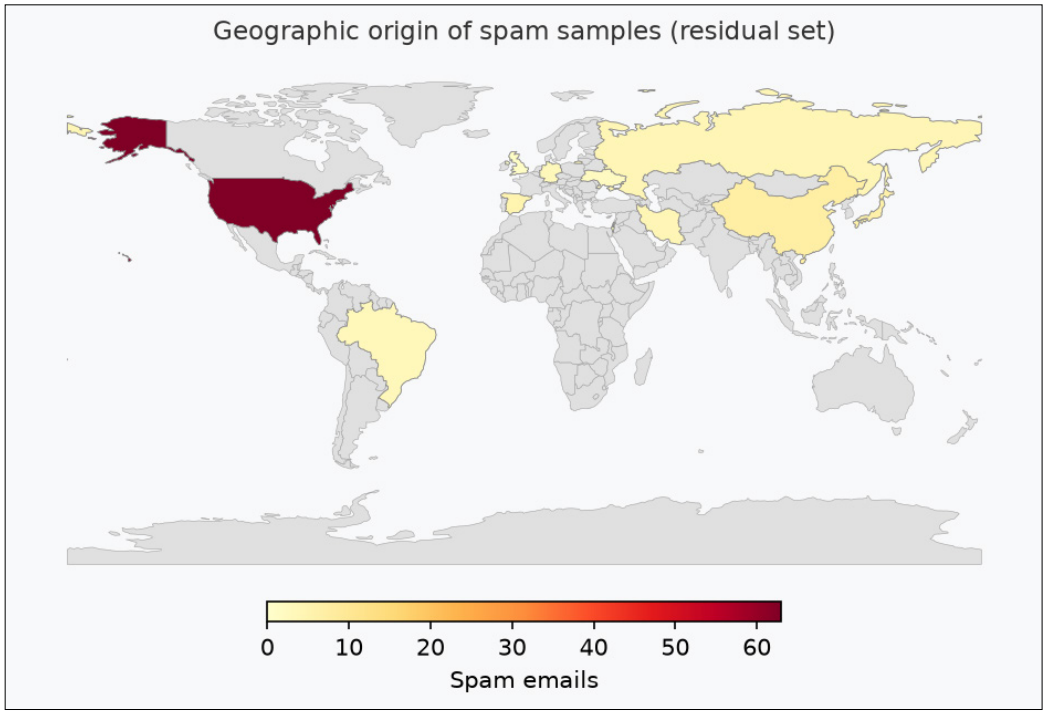
No newsletter samples were submitted during this test period. The newsletter feed is operated on a best-effort basis and may be empty in some test periods, depending on availability. False-positive scoring for newsletters is therefore not applicable for this test.

3.2 Geographic origin of spam samples

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

Country	Spam emails
United States	63
China	7
Japan	6
Spain	5
Russian Federation	4
Islamic Republic of Iran	4
Germany	3
Brazil	3
Israel	3
Ukraine	2
France	2
United Kingdom	1

** Five emails could not be geo-located ('IP Address not found') and are excluded from this table.*



Geographical distribution of spam samples in the residual set.

4. OVERALL RESULTS

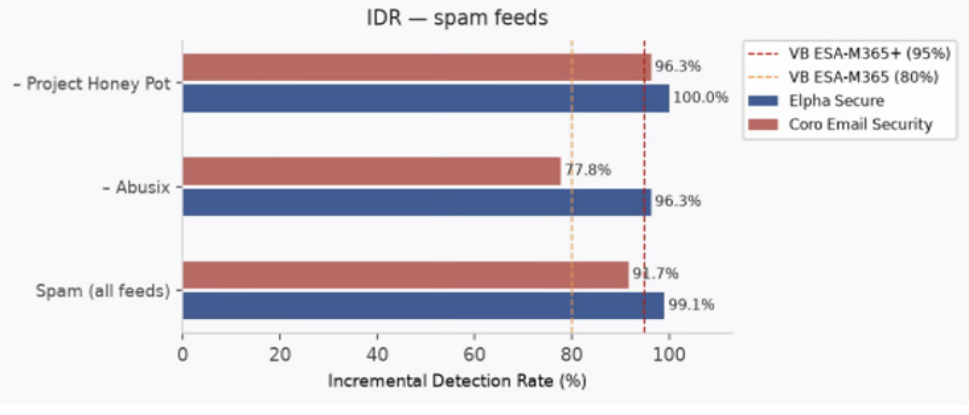
The table that follows summarizes the participating products' performance on the residual sample set for this test period.

Metric	Elpha Secure	Coro Email Security
Spam IDR	99.1%	91.7%
Residual spam caught	107 of 108	99 of 108
- Abusix feed	26 of 27	21 of 27
- Project Honey Pot feed	81 of 81	78 of 81
False positives - Ham	0	0
False positives - Newsletters	N/A	N/A
Phishing false negatives	N/A	N/A
Malware false negatives	0	0
Award	**VB ESA - M365+**	**VB ESA - M365**
Badges	**Top Performer, Malware 100**	**Malware 100**

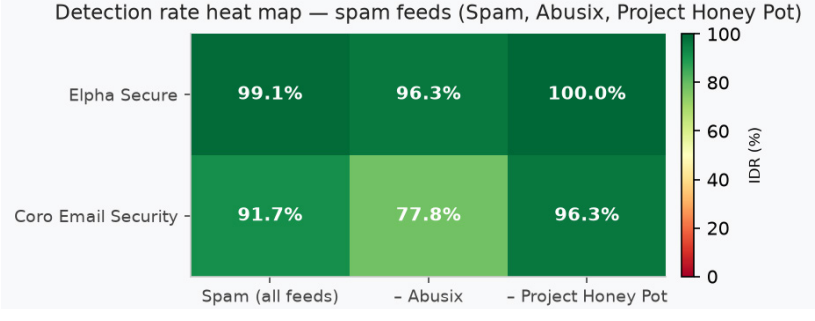
Incremental value over M365 alone – spam

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

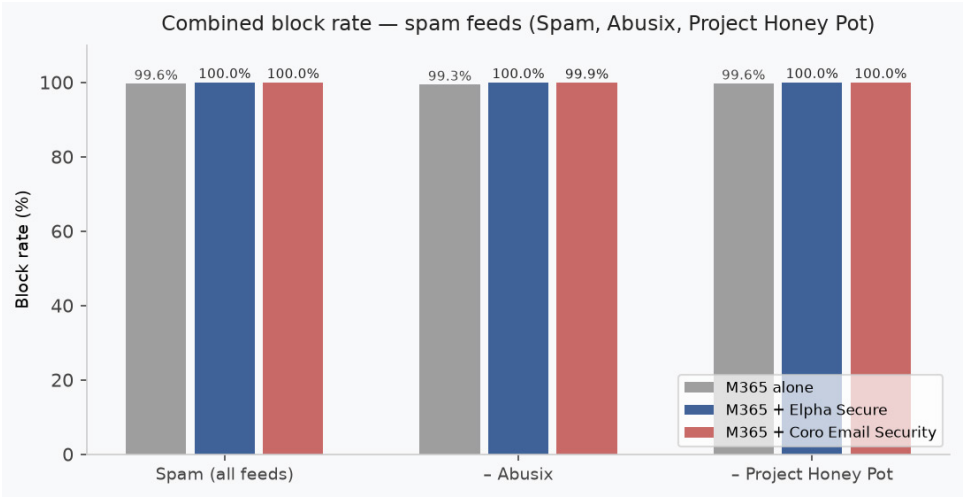
Metric	Elpha Secure	Coro Email Security
Block rate M365 alone	99.58%	99.58%
Block rate M365 + product	99.99%	99.96%
Incremental gain	**+0.41pp**	**+0.39pp**



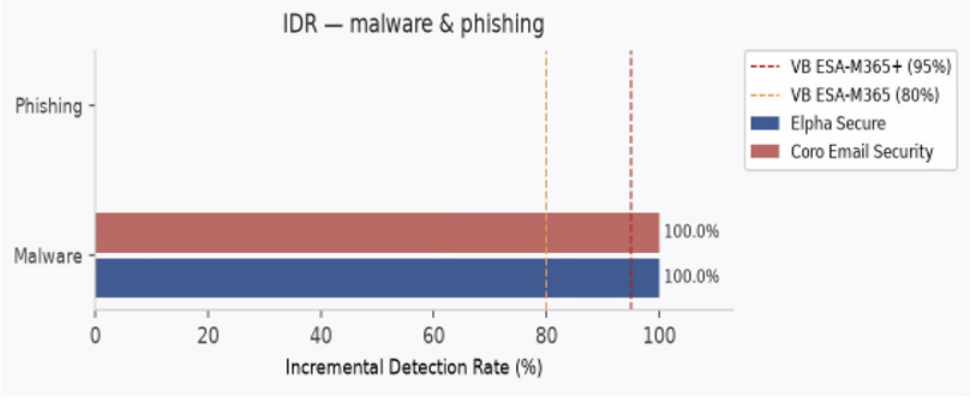
Incremental detection rates across spam feeds.



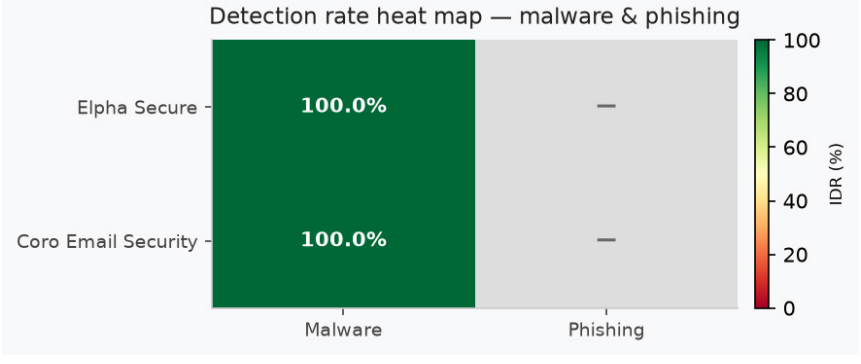
Spam detection rate heat map.



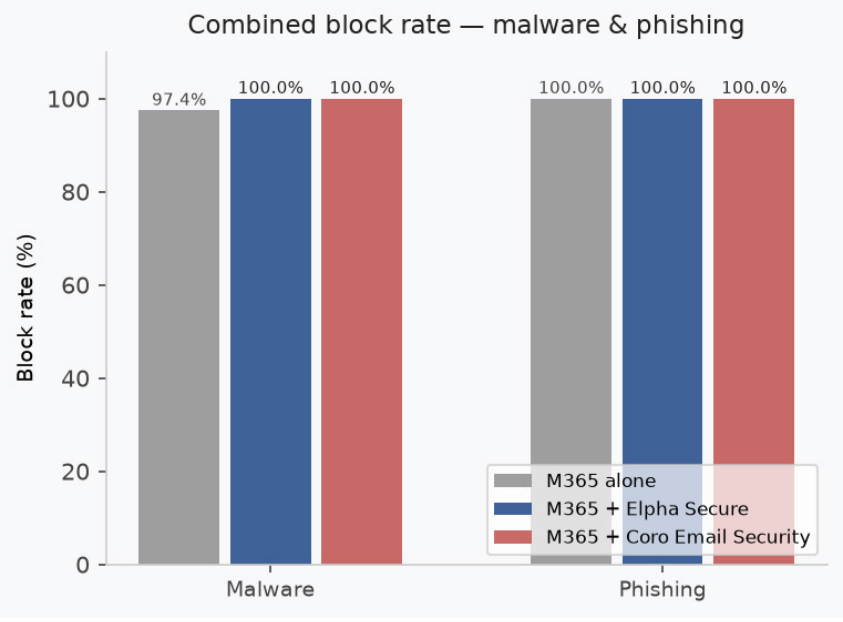
Block rate of M365 alone vs M365 + product across spam feeds.



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 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 | N/A Phishing 100 | ✓ Malware 100

Spam IDR 99.1% **| False positives (Ham + Newsletter)** 0

Elpha Secure detected 107 of the 108 residual spam samples submitted to it, missing one message. It correctly allowed through all ham and newsletter traffic.

- False positives against ham and newsletter traffic: 0
- Malware false negatives: 0 of 6 residual

Detection performance

Feed	Residual set	Caught	Missed	IDR (caught ÷ residual)
Spam (all feeds)	108	107	1	99.1%
- Abusix feed	27	26	1	96.3%
- Project Honey Pot feed	81	81	0	100.0%
Phishing	0	0	0	N/A (empty residual)
Malware	6	6	0	100.0%

Note: The Abusix IDR (96.3%) and the Project Honey Pot IDR (100.0%) diverge by 3.7 percentage points. The two are third-party spam feeds of the same type, but the Abusix residual is smaller (27 samples) and each missed message in the Abusix feed costs 3.7 percentage points, amplifying the visible gap.

Legitimate mail handling

Feed	Total	M365 correctly passed	Product FPs (blocked)	Delivered	Quarantined	Failed	Spam-foldered
Ham	376	371	0	371	0	0	5
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	376	376	0	371	0	0	5
Newsletters	0	N/A	N/A	N/A	N/A	N/A	N/A
Spam (all feeds)	25,610	1	25,609	138	5,510	12,327	7,635
- Abusix feed	4,049	1	4,048	35	1,074	1,818	1,122
- Project Honey Pot feed	21,561	0	21,561	103	4,436	10,509	6,513
Phishing	3,704	0	3,704	7	951	2,570	176
Malware	234	0	234	11	56	157	10

Spam detection by email language

Language	Total samples	Blocked	Block rate
ES Spanish	46	46	100.0%
GB English	37	37	100.0%
JP Japanese	6	6	100.0%
FR French	6	5	83.3%
RU Russian	4	4	100.0%
PT Portuguese	3	3	100.0%
IL Hebrew	3	3	100.0%
DE German	2	2	100.0%
RO Romanian	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	376	5	0	5	371	1.3%
Newsletters	0	N/A	N/A	N/A	N/A	N/A
Spam (all feeds)	25,610	25,502	107	25,609	1	99.99%
- Abusix feed	4,049	4,022	26	4,048	1	99.97%
- Project Honey Pot feed	21,561	21,480	81	21,561	0	100.0%
Phishing	3,704	3,704	0	3,704	0	100.0%
Malware	234	228	6	234	0	100.0%

5.2 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 | N/A Phishing 100 | ✓ Malware 100

Spam IDR 91.7% **| False positives (Ham + Newsletter)** 0

Coro Email Security detected 99 of the 108 residual spam samples submitted to it, missing nine messages. It correctly allowed through all ham and newsletter traffic.

- False positives against ham and newsletter traffic: 0
- Malware false negatives: 0 of 6 residual

Detection performance

Feed	Residual set	Caught	Missed	IDR (caught ÷ residual)
Spam (all feeds)	108	99	9	91.7%
- Abusix feed	27	21	6	77.8%
- Project Honey Pot feed	81	78	3	96.3%
Phishing	0	0	0	N/A (empty residual)
Malware	6	6	0	100.0%

Note: The Abusix IDR (77.8%) and the Project Honey Pot IDR (96.3%) diverge by 18.5 percentage points. The two are third-party spam feeds of the same type, but the Abusix residual is smaller (27 samples) and each missed message in the Abusix feed costs 3.7 percentage points, amplifying the visible gap.

Legitimate mail handling

Feed	Total	M365 correctly passed	Product FPs (blocked)	Delivered	Quarantined	Failed	Spam-foldered
Ham	376	371	0	371	0	0	5
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	376	376	0	371	0	0	5
Newsletters	0	N/A	N/A	N/A	N/A	N/A	N/A
Spam (all feeds)	25,610	9	25,601	110	10,323	7,973	7,204
- Abusix feed	4,049	6	4,043	28	1,892	1,106	1,023
- Project Honey Pot feed	21,561	3	21,558	82	8,431	6,867	6,181
Phishing	3,704	0	3,704	0	1,742	1,913	49
Malware	234	0	234	7	102	123	2

Spam detection by email language (residual set)

Language	Total samples	Blocked	Block rate
ES Spanish	46	45	97.8%
GB English	37	32	86.5%
JP Japanese	6	6	100.0%
FR French	6	5	83.3%
RU Russian	4	4	100.0%
PT Portuguese	3	3	100.0%
IL Hebrew	3	1	33.3%
DE German	2	2	100.0%
RO Romanian	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	376	5	0	5	371	1.3%
Newsletters	0	N/A	N/A	N/A	N/A	N/A
Spam (all feeds)	25,610	25,502	99	25,601	9	99.96%
- Abusix feed	4,049	4,022	21	4,043	6	99.85%
- Project Honey Pot feed	21,561	21,480	78	21,558	3	99.98%
Phishing	3,704	3,704	0	3,704	0	100.0%
Malware	234	228	6	234	0	100.0%

6. APPENDIX

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/.

6.1 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
Senior Threat Analyst: Norbert Biro
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