

# SELabs

INTELLIGENCE-LED TESTING


## Email Security Services

## Enterprise and Small Business



Jan - Mar 2023

**ESS**  
PROTECTION



SE Labs tested a range of email security services from well-known third-party security vendors and email platforms. This report aims to judge which were most effective.

Each service was exposed to the same threats, which were a mixture of targeted attacks using well-established techniques and public attacks that were found to be live on the internet at the time of the test.

The results indicate how effectively the services were at detecting and/ or protecting against those threats in real time and shortly after the attacks took place.

**Management****Chief Executive Officer** Simon Edwards**Chief Operations Officer** Marc Briggs**Chief Human Resources Officer** Magdalena Jurenko**Chief Technical Officer** Stefan Dumitrascu**Testing Team**

Nikki Albesa

Thomas Bean

Solandra Brewster

Gia Gorbald

Anila Johny

Erica Marotta

Luca Menegazzo

Jeremiah Morgan

Julian Owusu-Abrokwa

Joseph Pike

Georgios Sakatzidi

Dimitrios Tsarouchas

Stephen Withey

**Marketing**

Sara Claridge

Janice Sheridan

**Publication**

Colin Mackleworth

**IT Support**

Danny King-Smith

Chris Short

Website [selabs.uk](https://selabs.uk)Email [info@SELabs.uk](mailto:info@SELabs.uk)LinkedIn [www.linkedin.com/company/se-labs/](https://www.linkedin.com/company/se-labs/)Blog [blog.selabs.uk](https://blog.selabs.uk)

Post SE Labs Ltd,

55A High Street, Wimbledon, SW19 5BA, UK

SE Labs is ISO/IEC 27001 : 2013 certified and  
BS EN ISO 9001 : 2015 certified for The Provision  
of IT Security Product Testing.

SE Labs is a member of the Microsoft Virus Initiative (MVI);  
the Anti-Malware Testing Standards Organization (AMTSO);  
the Association of anti Virus Asia Researchers (AVAR);  
and NetSecOPEN.



© 2023 SE Labs Ltd

# Contents

<b>Introduction</b>	<b>04</b>
<b>Executive Summary</b>	<b>05</b>
<b>Email Security Services Protection Award</b>	<b>06</b>
<b>Attackers vs. Targets</b>	<b>07</b>
<b>1. Threat Detection Results</b>	<b>08</b>
<b>2. Total Accuracy Ratings</b>	<b>09</b>
<b>3. Protection and Legitimate Handling Accuracy</b>	<b>10</b>
<b>4. Conclusion</b>	<b>12</b>
<b>Appendices</b>	<b>13</b>
<b>Appendix A: Attack Details</b>	<b>13</b>
Targeted Attack Types	<b>13</b>
<b>Appendix B: Detailed Results</b>	<b>14</b>
Targeted Attack Details	<b>14</b>
Legitimate Message Details	<b>17</b>
<b>Appendix C: Terms Used</b>	<b>18</b>
<b>Appendix D: FAQs</b>	<b>19</b>

Document version 1.0 Written 21st June 2023



## Introduction

# Does it matter if your company is hacked?

And why are some businesses overconfident that they are secure?

A true story: There was a team manager, a head of IT and a chief financial officer. I asked each if they considered their network to be secure, hacked or in some other state. The ex-military team manager was supremely confident that the secure network was, as its optimistic name suggested, secure. The IT manager said, “I don’t know,” and the CFO said, “I don’t know, and does it matter?”

There are a couple of common reasons why people don’t think that their organisations will be hacked. One is that their security is the best. Another is that they don’t think they are a worthy target. But all businesses are targets because they are designed to make money. And if they cannot operate then they can’t perform their main function – making money.

Hackers know this and extort money from victims by stealing their data and threatening to release it to the public, exposing victims to large regulatory fines and litigation. And, of course, there’s the embarrassment factor of looking amateur. Hackers can also encrypt data on business systems, paralysing companies until they pay up (or restore from backups).

Hackers discriminate, so not everyone faces the same level of risk. But, as we can see from the groups of attackers that we emulate in this test, they search widely for targets. APT32 has attacked a wide range of companies, although it focusses on Asian targets. Exotic Lily likes to target IT companies with ransomware. APT38 goes straight for the money, picking on banks and other financial institutions (including cryptocurrency exchanges), while APT41 engages in espionage against healthcare organisations in specific territories.

In this report we emulate the behaviour of each of these attack groups to see how well-known email security solutions protect against these significant threats. For more details about the attack groups see **Attackers vs. Targets** on page 7 and **Appendix A: Attack Details** on page 13.

As with all of our reports, if you have any questions please contact us via our [website](#) and [LinkedIn](#). Our [newsletter](#) is an excellent source of updates, too.

# Executive Summary

This test examined the effectiveness of five email security solutions. **Microsoft Defender for Office 365** and **Google Workspace Enterprise** are commercial email platforms. **Trellix Email Security**, **WithSecure Email Security** and **Mailcow Open Source solution** are third-party 'add-on' services designed to provide additional security. Of the 'add-ons', the services from **Trellix** and **WithSecure** are commercial, while **Mailcow's** is open-source.

As a category of security services, email protection for enterprises and small businesses have improved significantly since SE Labs started testing their efficacy. In previous tests, some services performed so badly that they registered negative protection ratings. The jagged highs and lows of the accuracy ratings in previous tests are more evenly distributed in a normal bell-shaped curve for this test. The total

accuracy ratings range (44% to 100%) has also improved such that all five email services in this round of testing merited awards.

A 100% Total Accuracy Rating was achieved by top performer **Trellix Email Security**. It was awarded an AAA rating, as was **Microsoft Defender for Office 365**, which achieved 84%.

**WithSecure Email Security** was awarded an A rating for its 58% Total Accuracy Rating while **Google Workspace Enterprise** and **Mailcow Open Source Solution** got B awards for respectively achieving 50% and 40%.

The overall improvements are largely due to excellent protection against phishing email (98% to 100%) and near perfect Legitimate

Accuracy Ratings. Overall protection against email with malware was slightly less effective where the lowest score was 41% and second highest score was 91%.

Protection against business email compromise techniques was more variable. AAA awardees **Trellix** and **Microsoft** provided 100% protection, while the other three services were in the 15% to 19% range.

Most of the services have to improve their protection against social engineering attacks, where lowest score was a poor 1% and the second highest score was 56%. Once again, **Trellix Email Security** was the outlier with its 100% protection rating against social engineering attacks.

Executive Summary					
Product Tested	Protection Accuracy Rating	Legitimate Accuracy Rating	Total Accuracy Rating	Total Accuracy Rating (%)	Award
Trellix Email Security	4,700	1,090	5,790	100%	AAA
Microsoft Defender for Office 365	3,800	1,100	4,900	84%	AAA
WithSecure Email Security	2,545	800	3,345	58%	A
Google Workspace Enterprise	1,800	1,090	2,890	50%	B
Mailcow Open Source Solution	1,500	1,080	2,580	44%	B

Products highlighted in green were the most accurate, scoring 40 per cent or more for Total Accuracy. Those in orange scored less than 40 but 30 or more. Products shown in red scored less than 30 per cent.

For exact percentages, see **2. Total Accuracy Ratings** on page 9.

# Email Security Services Protection Award

The following products win SE Labs awards:

- **Trellix Email Security**
- **Microsoft Defender for Office 365**



- **WithSecure Email Security**



- **Google Workspace Enterprise**
- **Mailcow Open Source Solution**



# SE Labs Monthly Newsletter

**Don't miss our security articles and reports**

- Test reports announced
- Blog posts reviewed
- Security testing analysed
- **NEW:** Podcast episodes



**SUBSCRIBE NOW!**



## Attackers vs. Targets











When testing services against targeted attacks it is important to ensure that the attacks used are relevant. Anyone can run an attack randomly against someone else. It is the security vendor's challenge to identify common attack types and to protect against them. As testers, we need to generate threats that in some way relate to the real world.

All of the attacks used in this test are valid ways to compromise an organisation. Without any security in place, all would succeed in attacking the target. Outcomes would include systems infected with ransomware, remote access to networks and data theft.

But we didn't just sit down and brainstorm how we would attack different companies. Instead we used current threat intelligence to look at what the bad guys have been doing over the last few years and copied them quite closely. This way we can test the services' abilities to handle similar threats to those faced by global governments, financial institutions and national infrastructure.

The graphic on this page shows a summary of the attack groups that inspired the targeted attacks used in this test. If a service was able to detect and protect against these then there's a good chance they are on track to blocking similar attacks in the real world. If they fail, then you might take their bold marketing claims about defeating hackers with a pinch of salt.

For more details about each APT group see **Appendix A: Attack Details** on page 13.

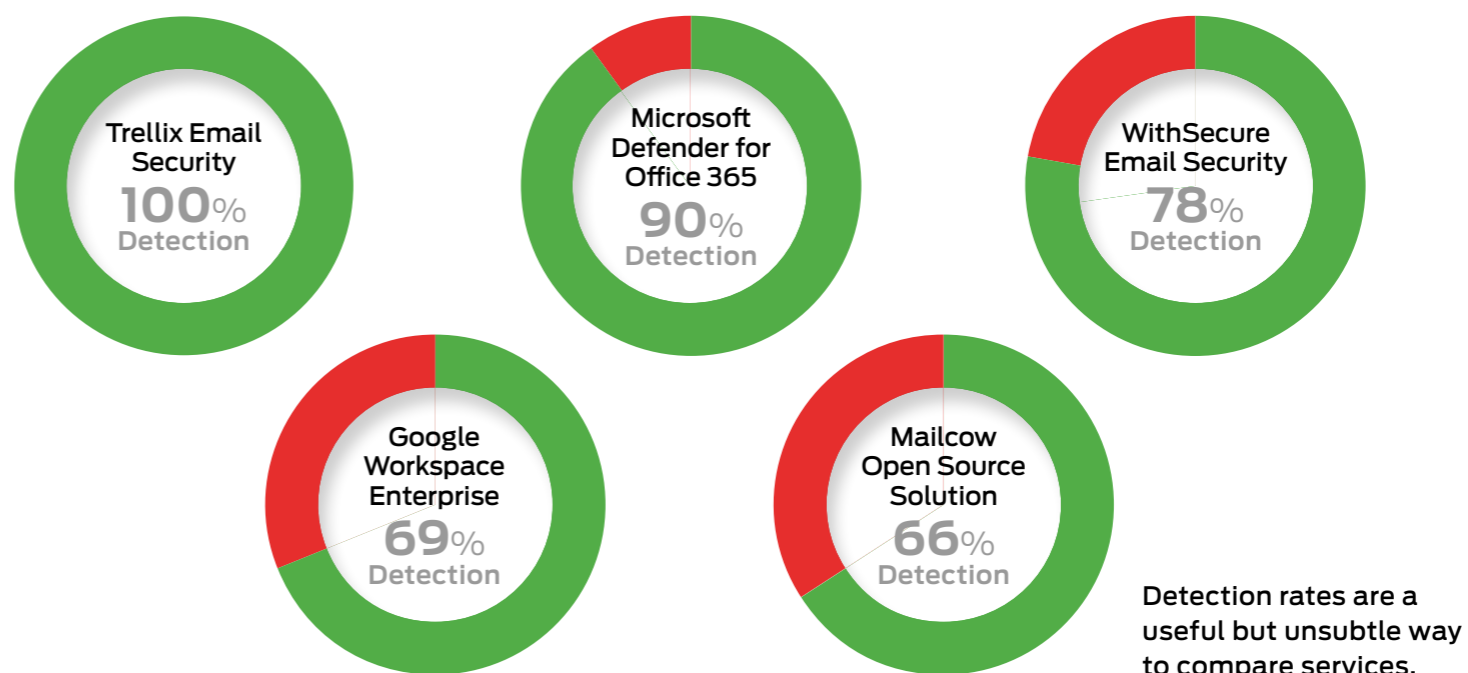
Attackers vs. Targets			
Attacker/APT Group	Method	Target	Details
APT32			Ransomware via drive-by download.
Exotic Lily			Ransomware deployed by steganography.
APT38			Ransomware deployed by steganography.
APT41			Malicious payloads using publicly available tools.
FIN7 & Carbanak			Documents containing scripts combined with public tools.

Key			
 Aviation	 Banking and ATMs	 Energy	 Entertainment
 Financial	 Gambling	 Government Espionage	 Healthcare
 IT	 Law	 Natural Resources	 US Retail, Restaurant and Hospitality

# 1. Threat Detection Results

While testing and scoring email security services is complex, it is possible to report straight-forward detection rates. The figures below summarise how each service and configuration handles threats in the most general, least detailed way.

Threat Detection Results			
Product	Detection Rate	Misses	Detection Rate (%)
Trellix Email Security	470	0	100%
Microsoft Defender for Office 365	425	45	90%
WithSecure Email Security	368	102	78%
Google Workspace Enterprise	325	145	69%
Mailcow Open Source Solution	310	160	66%





## 2. Total Accuracy Ratings

Judging the effectiveness of an email hosted protection service is a subtle art and many factors need to be considered when assessing how well it performs. To make things easier we've combined all of the different results into one easy-to-understand table.

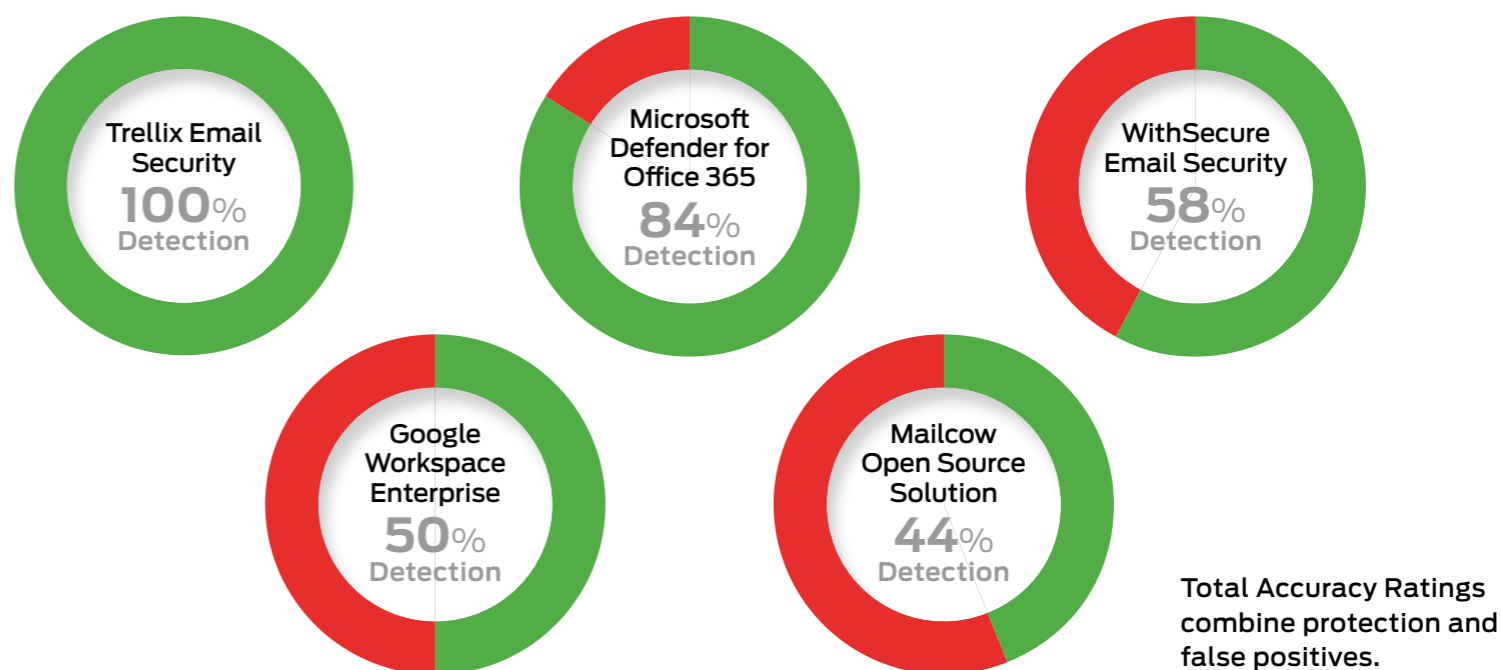
The graphic below takes into account not only each service's ability to detect and protect against threats, but also its handling of non-malicious messages and components of those messages, such as attachments and links to websites.

Not all protection measures, or detections for that matter, are equal. A service might completely delete an incoming malicious email and never allow the intended recipient to see (and subsequently interact with) it. Services may condemn suspicious messages to a 'quarantine' area if it lacks the utter conviction that the message is unwanted. This keeps threats away from recipients unless the recipient judges that the message is really safe. At the weaker end of the scale, the service might simply add a warning to the email's Subject line.

We take these different possible outcomes into account when attributing points that form final ratings.

For example, a service that completely blocks a malicious message from falling into the hands of its intended recipient is rated more highly than one that prefixes the Subject line with "Malware: " or "Phishing attempt: ", or sends the message to a 'Junk' folder.

Total Accuracy Ratings		
Product	Total Accuracy Rating	Total Accuracy Rating (%)
Trellix Email Security	5,790	100%
Microsoft Defender for Office 365	4,900	84%
WithSecure Email Security	3,345	58%
Google Workspace Enterprise	2,890	50%
Mailcow Open Source Solution	2,580	44%



Categorising how a service handles legitimate messages is similar, but in reverse. Making a small change to the Subject line is much less serious a failing than deleting the message and failing to notify the recipient.

## 3. Protection and Legitimate Handling Accuracy

The results below indicate how effectively the services dealt with threats and legitimate email. Points are earned for detecting threats and for blocking or otherwise neutralising them. Points are also earned for allowing legitimate email entry into the recipient's inbox without significant damage.

### Stopped; Rejected; Notified; Edited effectively (+10 for threats; -10 for legitimate)

If the service detects the threat and prevents any significant element of that threat from reaching the intended recipient we award it 10 points. If it miscategorises and blocks or otherwise significantly damages legitimate email then we impose a minus 10 point penalty.

### Quarantined (Between +10 for threats; -10 for legitimate)

Services that intervene and move malicious messages into a quarantine system are awarded either six or ten points depending on whether or not the user or administrator can recover the message. However, there is a six to ten point deduction for each legitimate message that is incorrectly sent to quarantine.

### Junk (+5 for threats; -5 for legitimate)

The message was delivered to the user's Junk folder.

### Inbox (-10 for threats; +10 for legitimate)

Malicious messages that arrive in the user's

Scoring Different Outcomes		
Action	Threat	Legitimate
Inbox	-10	10
Junk Folder	5	-5
Quarantined (admin)	10	-10
Quarantined (user)	6	-6
Notified	10	-10
Stopped	10	-10
Rejected	10	-10
Blocked	10	-10
Edited (Allow)	-10	10
Edited (Deny)	10	-10
Junk (Deny)	10	-10
Junk (Allow)	-7	7

inbox have evaded the security service. Each such case loses the service 10 points. All legitimate messages should appear in the inbox. For each one correctly routed there is an award of 10 points.

### Rating calculations

For threat results we calculate the protection ratings using the following formula:

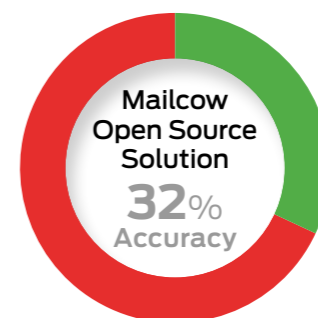
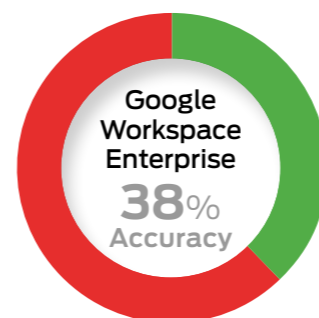
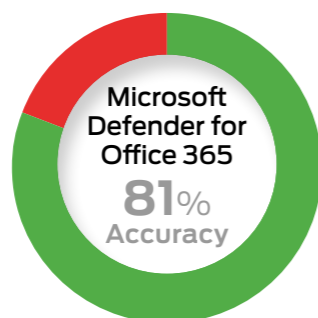
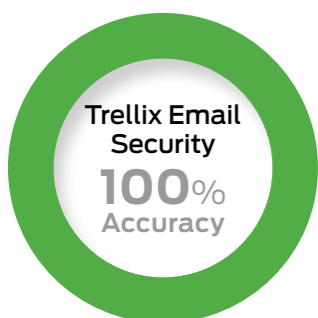
**Protection rating =**  
 (10x number of Stopped etc.) +  
 (6-8x number of Quarantined) +  
 (5x number of Junk) +  
 (-10x number of Inbox)  
 etc.

### For legitimate results the formula is:

(10x number of Inbox) +  
 (-5x number of Junk) +  
 (-6 -8x number of Quarantined) +  
 (-10x number of Stopped etc.)  
 etc.

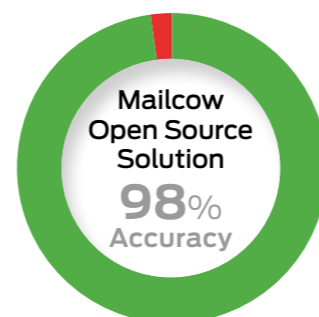
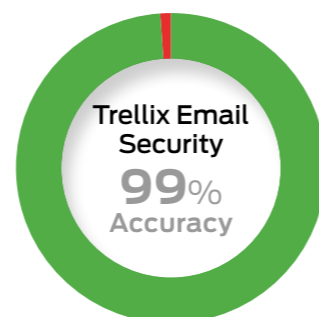
These ratings are based on our opinion of how important these different outcomes are. You may have a different view on how serious it is for a legitimate email to end up in quarantine, or for a malware threat to end up in the inbox. You can use the raw data from this report (See **Appendix B: Detailed Results** on page 14) to roll your own set of personalised ratings.

Protection Accuracy Ratings		
Product	Protection Accuracy Rating	Protection Accuracy Rating (%)
Trellix Email Security	4,700	100%
Microsoft Defender for Office 365	3,800	81%
WithSecure Email Security	2,545	54%
Google Workspace Enterprise	1,800	38%
Mailcow Open Source Solution	1,500	32%



The table below shows how accurately the services handled legitimate email. The rating system is described in detail in [3. Protection and Legitimate Handling Accuracy](#) on page 10.

Legitimacy Accuracy Rating		
Product	Legitimate Accuracy Rating	Legitimate Accuracy Rating (%)
Microsoft Defender for Office 365	1,100	100%
Google Workspace Enterprise	1,090	99%
Trellix Email Security	1,090	99%
Mailcow Open Source Solution	1,080	98%
WithSecure Email Security	800	73%



Legitimate Accuracy Ratings give a weighted value to services based on how accurately they handle legitimate messages.

## 4. Conclusion

This test exposed two email platforms and three third-party security services to a range of threats. We used documented targeted attack methods as used by real-life attackers. These included focussed phishing, custom malware, business compromise techniques and other types of social engineering.

We've listed the **attacker groups** that inspired our attacks on page 13. To make things even more realistic, we created a simulated target organisation with regular suppliers and other partners. This enabled us to create look-alike adversaries. We used techniques such as using similar domain names to send malicious emails.

You can divide the email services that we test regularly into two main groups: platforms and third-party services. Platforms include Google, Microsoft and Yahoo. Services handle email before or as it is delivered to a platform. Some act as gateways, receiving and processing messages before either deleting them or forwarding to the platform. Others integrate more directly into the platform, which is an increasingly common approach.

At SE Labs we believe that security products should keep threats as far away from end users as possible. Our scoring reflects that. With most security testing,

and email in particular, there are so many variables and possible outcomes that the results can look a little overwhelming. We've tried to provide a neat 'Total Protection' score for each product to help simplify things, while providing enough data to allow you to create your own scoring system should you wish.

The five email services tested were accurate, scoring 40 per cent or more for Total Accuracy. The standouts were **Trellix Email Security** and **Microsoft Defender for Office 365** which both achieved AAA awards for Total Accuracy Rating scores of 100% and 84% respectively.

**Trellix Email Security** earned its AAA award by not letting a single attack get through to the user's inbox. It achieved an outstanding 100% Protection Accuracy Rating either by rejecting or stopping all attacks, or placing them in administered quarantine. This hawkish vigilance against harmful email was balanced by its ability to distinguish legitimate messages, blocking only a single one.

The other AAA awardee is **Microsoft Defender for Office 365** which provided excellent protection against business email compromise techniques and phishing attacks. It was less effective against social

engineering email, scoring 56% but achieved a 91% Protection Rating against email malware attacks. It also scored a 100% Legitimacy Accuracy Rating.

**WithSecure Email Security** achieved a 58% Total Accuracy Rating for which it received an A award. It allowed all legitimate messages through to the user while disallowing phishing attacks. **WithSecure** was also effective against email malware attacks as shown in its 76% protection rating.

**Google Workspace Enterprise** and **Mailcow Open Source solution** both received B awards. Both email services were excellent at repelling phishing attacks but were less effective against compromising business and malware bearing email. They were poor at preventing social engineering threats from reaching end users but good at allowing legitimate messages.

# Appendices

## Appendix A: Attack Details

### Targeted Attack Types

#### Attack Group APT32

**Method of Attack** Link to Malicious Webpage  
**Targets** Government

Also tracked as OceanLotus Group, APT32 is based in Vietnam and has targeted a range of industries in neighbouring countries such as Laos, Cambodia and the Philippines.

It leverages both malware and commercially available tools to attack targets in the interests of the Vietnamese state.

**References:**

<https://attack.mitre.org/groups/G0050/>

#### Attack Group Exotic Lily

**Method of Attack** Spear phishing attachment/  
Spear phishing Link  
**Targets** IT sector

Operating since at least September 2021, this group targets mostly IT sector organisations. It has used a variety of phishing tactics, such as disguising threats as legitimate file-sharing email notifications. These provided links (URLs) that lead to the initial compromise and ultimately ransomware attacks using variations such as Conti and Diavol.

**References:**

<https://attack.mitre.org/groups/G1011/>

#### Attack Group APT38

**Method of Attack** Spearphishing attachment  
**Targets** Financial

Based in North Korea, APT38 focused on banks, other financial institutions and cryptocurrency exchanges in over 30 countries. The most notable targets were the Bank of Bangladesh, Bancomext and Banco de Chile. North Korea is estimated to have stolen billions of dollars from cryptocurrency organisations.

**References:**

<https://attack.mitre.org/groups/G0082/>

#### Attack Group APT41

**Method of Attack** Link to malicious webpage  
**Targets** Healthcare

This Chinese based threat actor focused on state-sponsored espionage activities. It targeted healthcare, telecoms organisations and technology sectors across 14 countries.

After infecting targets, the group is known to have deployed Encryptor RaaS ransomware.

**References:**

<https://attack.mitre.org/groups/G0096/>

#### Attack Group FIN7 & Carbanak

**Method of Attack** Spear phishing attacks  
containing scripts  
**Targets** Retail

This group used spear phishing attacks targeted at retail, restaurant and hospitality businesses. What appeared to be customer complaints, CVs (resumes) and food orders sent in Word and RTF formatted documents, were actually attacks that hid malicious (VBS) code behind hidden links.

**References:**

<https://attack.mitre.org/groups/G0046/>

## Appendix B: Detailed Results

The following tables show how each service handled different types of targeted attack. The table at the end of the series also summarises how they handled different categories of commodity threats.

There are four main categories of targeted attack used in this test:

- Business Email Compromise
- Phishing
- Social Engineering
- Malware

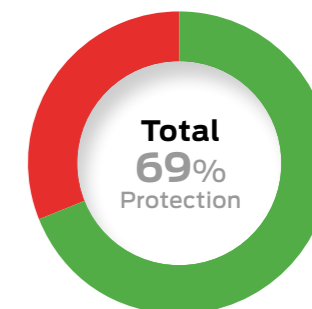
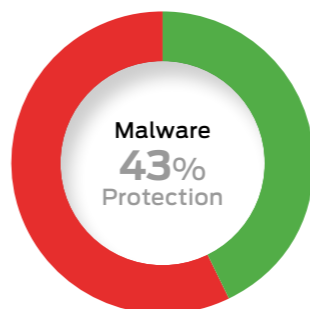
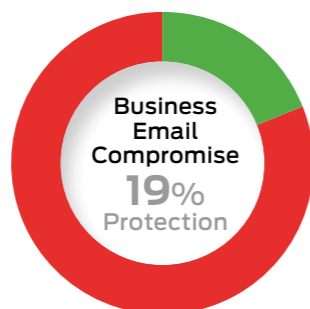
Each service has a number of options when handling such threats. The tables show how each service handled each category.

For example, you can see how many social engineering samples made it through to the inbox; how many were sent to the Junk folder; and how many were prevented from coming anywhere near the user – the Junk folder and Quarantine (admin) are common options.

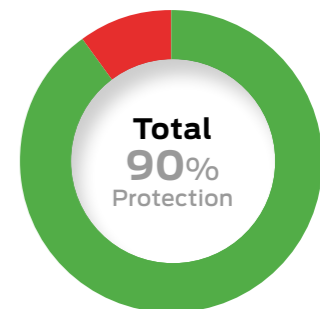
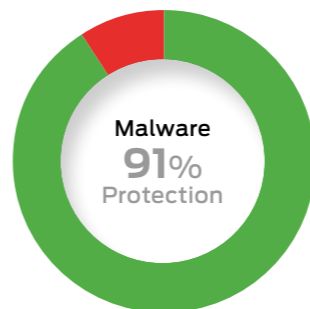
Not every possible option needs to be taken by a service under test, so the tables show only those outcomes that occurred.

### Targeted Attack Details

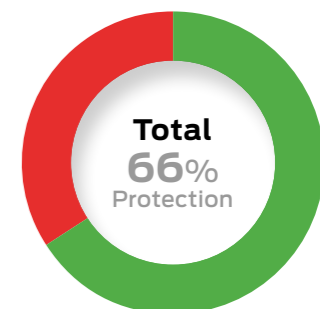
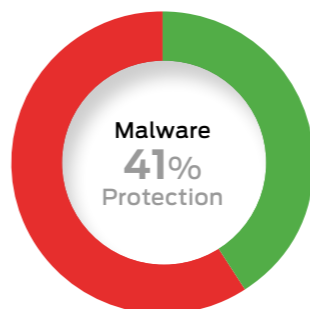
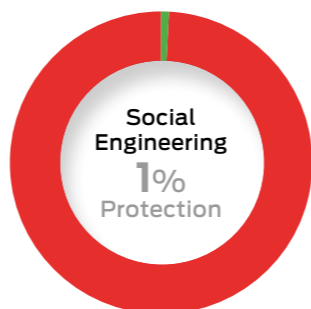
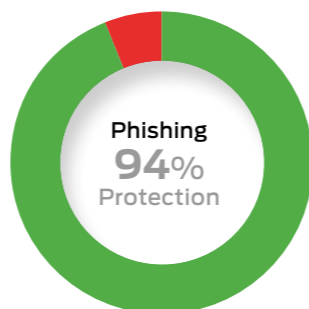
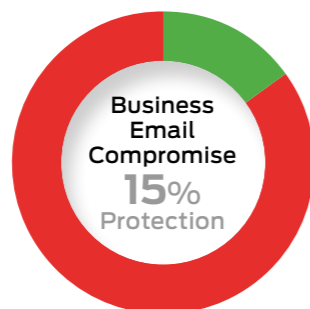
Google Workspace Enterprise											
	Stopped	Blocked	Quarantined (admin)	Rejected	Edited (deny)	Quarantined (user)	Junk (deny)	Junk Folder	Junk (allow)	Edited (allow)	Inbox
Business Email Compromise	2	0	1	2	0	0	0	0	0	0	21
Phishing	12	0	98	180	5	0	0	0	0	0	5
Social Engineering	2	0	0	0	0	0	0	0	0	0	88
Malware	23	0	0	0	0	0	0	0	0	0	31
<b>Total</b>	<b>39</b>	<b>0</b>	<b>99</b>	<b>182</b>	<b>5</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>145</b>



Microsoft Defender for Office 365											
	Stopped	Blocked	Quarantined (admin)	Rejected	Edited (deny)	Quarantined (user)	Junk (deny)	Junk Folder	Junk (allow)	Edited (allow)	Inbox
Business Email Compromise	0	0	26	0	0	0	0	0	0	0	0
Phishing	0	0	120	180	0	0	0	0	0	0	0
Social Engineering	0	0	50	0	0	0	0	0	0	0	40
Malware	10	0	39	0	0	0	0	0	0	0	5
<b>Total</b>	<b>10</b>	<b>0</b>	<b>235</b>	<b>180</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>45</b>



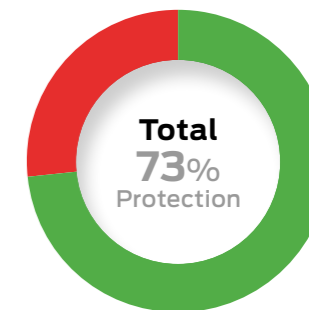
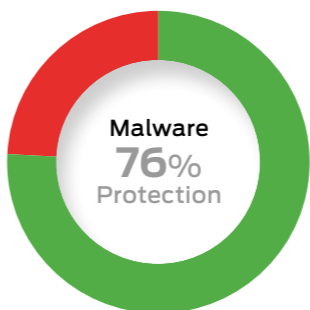
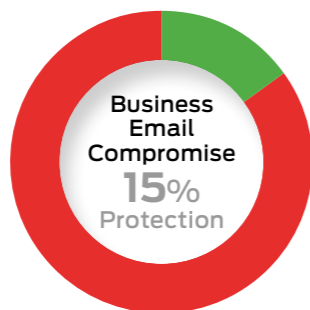
Mailcow Open Source Solution											
	Stopped	Blocked	Quarantined (admin)	Rejected	Edited (deny)	Quarantined (user)	Junk (deny)	Junk Folder	Junk (allow)	Edited (allow)	Inbox
Business Email Compromise	4	0	0	0	0	0	0	0	0	0	22
Phishing	85	0	0	179	19	0	0	0	0	0	17
Social Engineering	1	0	0	0	0	0	0	0	0	0	89
Malware	22	0	0	0	0	0	0	0	0	0	32
<b>Total</b>	<b>112</b>	<b>0</b>	<b>0</b>	<b>179</b>	<b>19</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>160</b>



Trellix Email Security											
	Stopped	Blocked	Quarantined (admin)	Rejected	Edited (deny)	Quarantined (user)	Junk (deny)	Junk Folder	Junk (allow)	Edited (allow)	Inbox
Business Email Compromise	0	0	26	0	0	0	0	0	0	0	0
Phishing	0	0	120	180	0	0	0	0	0	0	0
Social Engineering	0	0	90	0	0	0	0	0	0	0	0
Malware	21	0	33	0	0	0	0	0	0	0	0
<b>Total</b>	<b>21</b>	<b>0</b>	<b>269</b>	<b>180</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>



WithSecure Email Security											
	Stopped	Blocked	Quarantined (admin)	Rejected	Edited (deny)	Quarantined (user)	Junk (deny)	Junk Folder	Junk (allow)	Edited (allow)	Inbox
Business Email Compromise	2	0	0	0	2	0	0	0	0	0	22
Phishing	0	0	75	180	0	0	45	0	0	0	0
Social Engineering	0	0	0	0	0	0	0	0	23	0	67
Malware	40	0	0	0	0	0	1	0	0	0	13
<b>Total</b>	<b>42</b>	<b>0</b>	<b>75</b>	<b>180</b>	<b>2</b>	<b>0</b>	<b>46</b>	<b>0</b>	<b>23</b>	<b>0</b>	<b>102</b>





## Legitimate Message Details

These results show how effectively each service managed messages that posed no threat. In an ideal world all legitimate messages would arrive in the inbox. When they are categorised as being a threat then a 'false positive' result is recorded.

It is important to test for false positives because too many indicate a product that is too aggressive

and will block useful email as well as threats. It would be easy to create a product that blocked all threats if it was also allowed to block all legitimate email.

Finding the balance between allowing good and blocking bad is the key to almost every type of security system.

Legitimate Message Details					
	Inbox	Edited (allow)	Junk Folder	Quarantined (admin)	Blocked
Microsoft Defender for Office 365	110	0	0	0	0
Google Workspace Enterprise	109	0	0	1	0
Trellix Email Security	109	0	0	0	1
Mailcow Open Source Solution	108	0	0	0	2
WithSecure Email Security	95	0	15	0	0

## Appendix C: Terms Used

The results below use the following terms:

- **Notified** The service prevented the threat from being delivered and notified the user. There was no option for the user to recover the threat.
- **Stopped** The service silently prevented the threat from being delivered.
- **Rejected** The service prevented the threat from being delivered and sent a notification to the sender.
- **Edited (deny)** The service delivered the message but altered it to remove malicious content.
- **Junk (deny)** The service modified the message, which was sent to the target Junk folder. The malicious content was removed.
- **Blocked** The service prevented the threat from being delivered and logged the event.
- **Quarantined (admin)** The service prevented the threat from being delivered and kept a copy of it, which could be recovered by the administrator only.
- **Quarantine (user)** The service prevented the threat from being delivered and kept a copy of it, which could be recovered by the user.
- **Junk Folder** The message was delivered to the user's Junk folder by the email platform.
- **Junk (allow)** The service modified the message, which was sent to the target Junk folder, but didn't remove the malicious content.
- **Inbox** The service failed to detect or protect against the threat.
- **Edited (allow)** The service modified the message, which was sent to the target inbox, but didn't remove the malicious content.

# Annual Report 2023

**Our 4th Annual Report  
is now available**

- **Threat Intelligence Special**
- **Ransomware Focus**
- **Security Awards**
- **Advanced Email Testing**



**DOWNLOAD THE  
REPORT NOW!**

(free – no registration)

**[selabs.uk/ar2023](https://selabs.uk/ar2023)**

## Appendix D: FAQs

A **full methodology** for this test is available from our website.

- The products chosen for this test were selected by SE Labs.
- The test was unsponsored.
- The test was conducted between 13th March and 9th May 2023.
- All products were configured according to each vendor's recommendations, when such recommendations were provided.
- Malicious emails, URLs, attachments and legitimate messages were independently located and verified by SE Labs.
- Targeted attacks were selected and verified by SE Labs.
- Malicious and legitimate data was provided to partner organisations once the test was complete.

### **Q** What is a partner organisation? Can I become one to gain access to the threat data used in your tests?

**A** Partner organisations benefit from our consultancy services after a test has been run. Partners may gain access to low-level data that can be useful in product improvement initiatives and have permission to use award logos, where appropriate, for marketing purposes. We do not share data on one partner with other partners. We do not partner with organisations that do not engage in our testing.

### **Q** I am a security vendor and you tested my product without permission. May I access the threat data to verify that your results are accurate?

**A** We are willing to share a certain level of test data with non-partner participants for free. The intention is to provide sufficient data to demonstrate that the results are accurate. For more in-depth data suitable for product improvement purposes we recommend becoming a partner.

# SE Labs

INTELLIGENCE-LED TESTING

SE Labs helps advance the effectiveness of computer security through innovative, detailed and intelligence-led testing, run with integrity.



### Enterprises

Reports for enterprise-level products supporting businesses when researching, buying and employing security solutions.

**Download Now!**

### Small Businesses

Our product assessments help small businesses secure their assets without the purchasing budgets and manpower available to large corporations

**Download Now!**



### Consumers

Download free reports on internet security products and find out how you can secure yourself online as effectively as a large company

**Download Now!**

 [selabs.uk](https://selabs.uk)



### SE Labs Report Disclaimer

1. The information contained in this report is subject to change and revision by SE Labs without notice.
2. SE Labs is under no obligation to update this report at any time.
3. SE Labs believes that the information contained within this report is accurate and reliable at the time of its publication, which can be found at the bottom of the contents page, but SE Labs does not guarantee this in any way.
4. All use of and any reliance on this report, or any information contained within this report, is solely at your own risk. SE Labs shall not be liable or responsible for any loss of profit (whether incurred directly or indirectly), any loss of goodwill or business reputation, any loss of data suffered, pure economic loss, cost of procurement of substitute goods or services, or other intangible loss, or any indirect, incidental, special or consequential loss, costs, damages, charges or expenses or exemplary damages arising his report in any way whatsoever.
5. The contents of this report does not constitute a recommendation, guarantee, endorsement or otherwise of any of the products listed, mentioned or tested.
6. The testing and subsequent results do not guarantee that there are no errors in the products, or that you will achieve the same or similar results. SE Labs does not guarantee in any way that the products will meet your expectations, requirements, specifications or needs.
7. Any trade marks, trade names, logos or images used in this report are the trade marks, trade names, logos or images of their respective owners.
8. The contents of this report are provided on an "AS IS" basis and accordingly SE Labs does not make any express or implied warranty or representation concerning its accuracy or completeness.