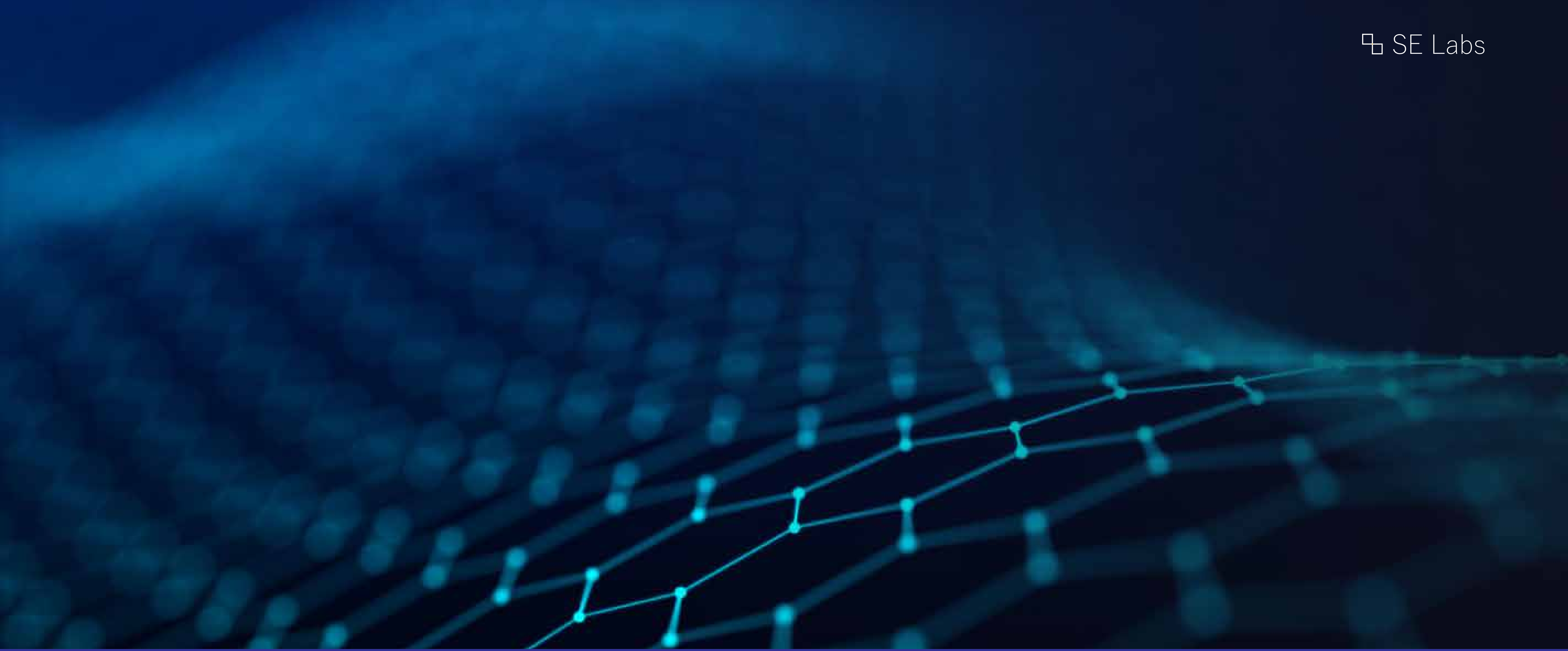
SE Labs
INTELLIGENCE-LED TESTING

Email Security Services

Enterprise and Small Business

April 2023



SE Labs tested a two email security services, one that is commercial, the other open-source. We also tested a commercial email platform.

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 Gorbold
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
Email info@SELabs.uk
LinkedIn www.linkedin.com/company/se-labs/
Blog 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.

Contents

Introduction 04
Executive Summary 05
Attackers vs. Targets 06
1. Threat Detection Results 07
2. Total Accuracy Ratings 08
3. Protection and Legitimate Handling Accuracy 09
4. Conclusion 11
Appendicies 12
Appendix A: Attack Details 12
Targeted Attack Types 12
Appendix B: Detailed Results 13
Targeted Attack Details 13
Legitimate Message Details 15
Appendix C: Terms Used 16
Appendix D: FAQs 17

Document version 1.0 Written 3rd April 2023

Introduction

DIY email security

Can you defend against email threats better than the security companies?

How well do the main email platforms handle threats? Is it worth paying for additional email security from a third-party specialist? Or could you create your own secure email server and get top grade protection for free?

In this special, one-of-a-kind report we investigate how well one of the world's largest email providers performs when trying to filter out harmful security threats from your email. We also assess the benefits of a well-known email security service that you can bolt onto any other email solution. And finally, we built an open-source email server running a combination of security and management tools to see how well it compared.

Criminals Target Email

All but the smallest of businesses use email. This is why criminals use email as a way to reach their victims. It's cheap and easy for them to send malware, links to fake login pages and many other social engineering and technical tricks to break into business networks. So how can a large or small business protect itself?

Large email platforms such as Microsoft and Google claim to defend their users from threats like phishing and viruses. Third-party email security services like Proofpoint and Mimecast offer additional protection. For the ultimate in control businesses can create their own secure email platforms using free, open-source software.

We wanted to answer the questions:

- **Is there value to be had from specialist email security services?**
- **Should you run your own server?**
- **Can you combine your own server with a specialist service?**

What Does Protection Mean?

Where email security is concerned you need to be sure that the system you use is safe against criminals who want to access your email messages. You also need to be sure that criminals have a hard time sending malicious emails to you, with the intention of gaining access to your computer systems through trickery or technical hacking. In other words, your main communication system with the world needs to stop threats and be resilient against intruders too.

It's not a stretch to imagine that the major platforms (Google, Microsoft and Apple) are better equipped at keeping hackers out of your email archives than most other options. As long as you use good passwords and multi-factor authentication, it's probably safe to trust them to keep your emails private. But what about stopping phishing emails, viruses and other fraudulent messages?

Anonymous

In this report we compare a major platform with a third-party email security service to see if it's worth spending extra on security. We worked with both companies but neither wished to be identified in this report. We reported back to them all of the threats that they identified (and missed) and provided them with an opportunity to dispute any mistakes that they identified. This report is the result of that engagement.

We also used an off-the-shelf open source solution that combines the free ClamAV anti-virus software with the Rspamd anti-spam filtering system plus a host of other tools. We hope you find this report useful and food for thought when considering your email security strategy. We have other, non-anonymised email security reports on our website.

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 three email security solutions. One is a well-known commercial email platform, the other two being third-party 'add-on' services designed to provide additional security. Of the 'add-ons', one is a commercial service and the other is a free, open-source software.

SE Labs used advanced targeted attack techniques, as seen in devastating real-world attacks, to assess how well these services handle email cyber threats. Legitimate messages were also sent through the services to ensure that security settings were balanced with reasonable usability.

The Commercial Email Security Service achieved a high Total Accuracy rating of 71%. It was particularly effective against malware attacks so that none were dropped in the end-user's Inbox. It let through a few phishing and social engineering attacks and allowed some business email to be compromised. All legitimate messages reached the Inbox, so that it scored a 100% Legitimate Accuracy rating.

The Open Source Email Security Service likewise allowed all legitimate messages through to the user but poor protection against targeted attacks dragged its Total Accuracy rating down to 3%.

The Commercial Email Platform performed poorly with a Total Accuracy rating of -5%. It provided better protection against business email compromise attacks and some protection against phishing emails but let almost all social engineering and malware attacks through. Its misclassification of some legitimate messages, placing them in quarantine, contributed to its negative overall score.

Executive Summary

Product Tested	Protection Accuracy Rating	Legitimate Accuracy Rating	Total Accuracy Rating	Total Accuracy Rating (%)	Award
Commercial Email Security Service	2,065	1,100	3,165	71%	AAA
Open Source Email Security Service	-974	1100	126	3%	-
Commercial Email Platform	-1068	860	-208	-5%	-

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 8.

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 12.

Attackers vs. Targets

Attacker/APT Group	Method	Target	Details
Sandworm	X	🏭	Windows vulnerabilities via Office documents
APT28	X	🏛	Microsoft Office macros
FIN4	X W X W	$	Man-in-the-middle spear phishing
FIN7 & Carbanak	W	🛒	Documents containing scripts combined with public tools
Dragonfly & Dragonfly 2.0	W	🏭	Phishing & supply chain methods used to gain access

Key

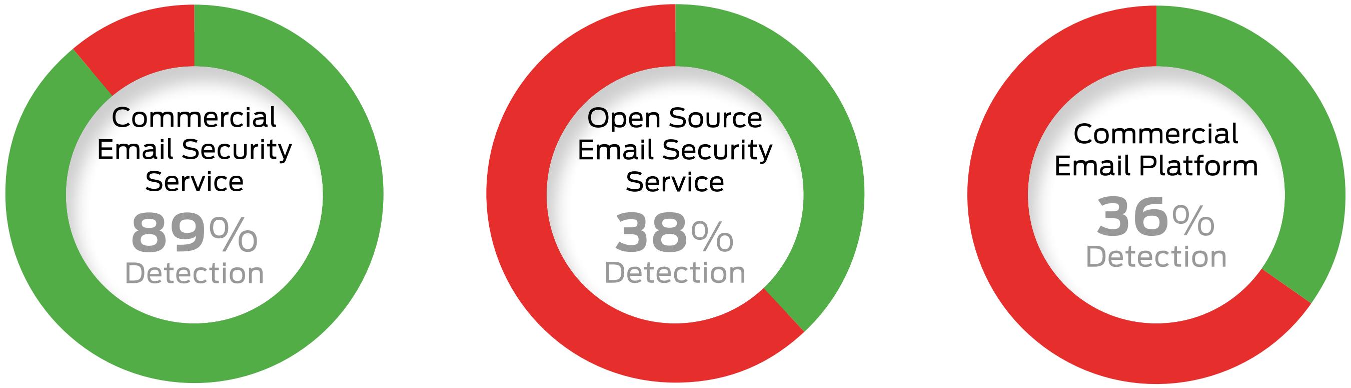
✈	Aviation	🏛	Banking and ATMs	🏭	Energy	$	Financial
🂡	Gambling	🏛	Government Espionage	✚	Healthcare	⚖	Law
🛢	Natural Resources	🛒	US Retail, Restaurant and Hospitality				

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 (%)
Commercial Email Security Service	299	37	89%
Open Source Email Security Service	128	208	38%
Commercial Email Platform	120	219	36%



Detection rates are a useful but unsubtle way to compare services.

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.

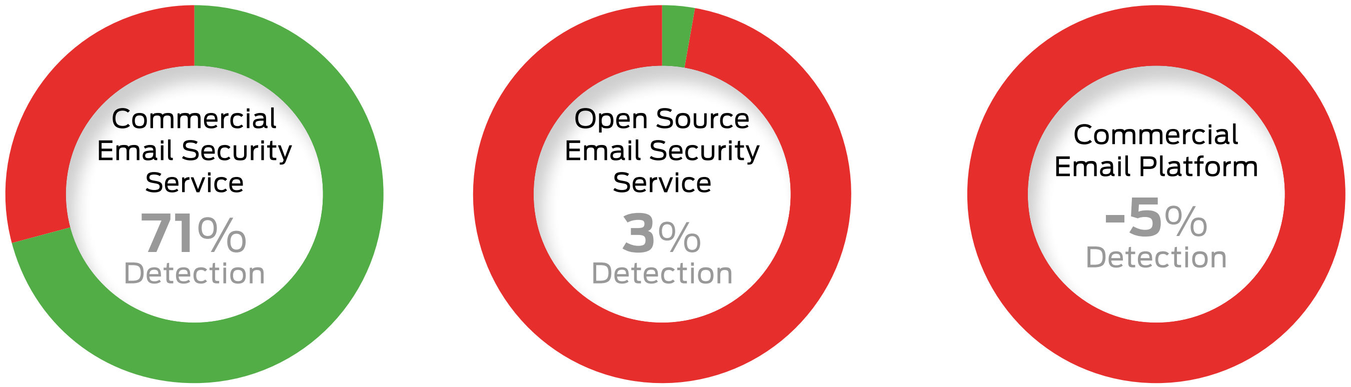
Not all protection measures, or detections for that matter, are equal. A service might completely delete an incoming malicious email and never allow the intended recipient to see (and subsequently interact with) it. Services may condemn suspicious messages to a 'quarantine' area if it lacks the utter 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 (%)
Commercial Email Security Service	3,165	71%
Open Source Email Security Service	126	3%
Commercial Email Platform	-208	-5%



Total Accuracy Ratings combine protection and false positives.

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 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.

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

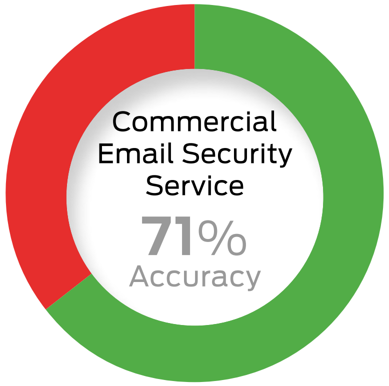
Rating calculations
For threat results we calculate the protection ratings using the following formula:
Protection rating =
(10x number of Stopped etc.) +
(6-8x number of Quarantined) +
(5x number of Junk) +
(-10x number of Inbox)
etc.

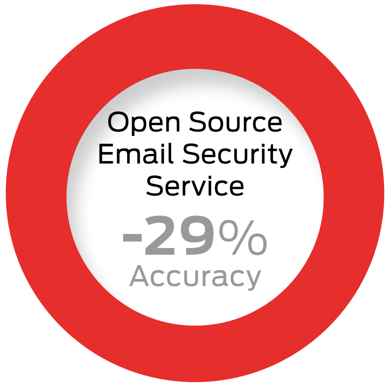
For legitimate results the formula is:
(10x number of Inbox) +
(-5x number of Junk) +
(-6 -8x number of Quarantined) +
(-10x number of Stopped etc.)
etc.

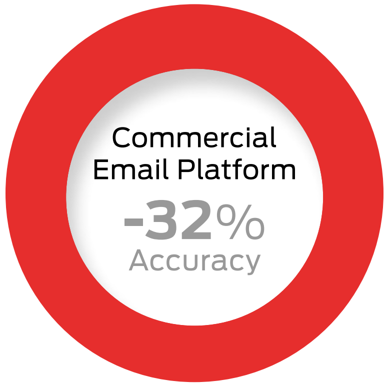
These ratings are based on our opinion of how important these different outcomes are. You may have a different view on how serious it is for a legitimate email to end up in quarantine, or for a malware threat to end up in the inbox. You can use the raw data from this report (See **Appendix B: Detailed Results** on page 13) to roll your own set of personalised ratings.

Protection Accuracy Ratings

Product	Protection Accuracy Rating	Protection Accuracy Rating (%)
Commercial Email Security Service	2,065	71%
Open Source Email Security Service	-974	-29%
Commercial Email Platform	-1,068	-32%



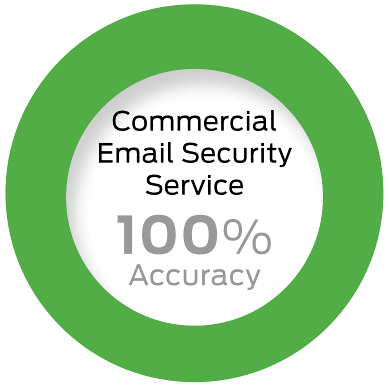


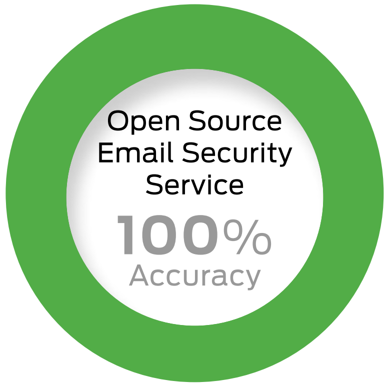


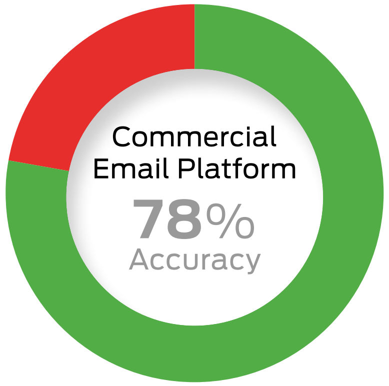
The table below shows how accurately the services handled legitimate email. The rating system is described in detail in **3. Protection and Legitimate Handling Accuracy** on page 9.

Legitimacy Accuracy Rating

Product	Legitimate Accuracy Rating	Legitimate Accuracy Rating (%)
Commercial Email Security Service	1,100	100%
Open Source Email Security Service	1,100	100%
Commercial Email Platform	860	78%







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

4. Conclusion

This test exposed a well-known email platform and 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 email compromise techniques and other types of social engineering.

We've listed the attacker groups that inspired our attacks on page 12. To make things even more realistic, we created a simulated target organisation with regular suppliers and other partners. This enabled us to also 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.

For this report, we anonymised the products to broadly answer whether it's worth investing in a specialist email security service.

Despite missing a few threats, the Commercial Email Security Service scored such a high Total Accuracy rating of 71% that it garnered an AAA award. When this score is compared to those achieved by the Open Source Email Security Service and that of the Commercial Email Platform, the drop is so precipitous that it's tempting to conclude that there is value in paying for specialist email protection.

The paid-for service's clear advantage lies in the huge gap between its Protection Accuracy rating of 71% and the negative ratings of the Open Source Email Security Service (-29%) and the Commercial Email Platform (-32%). The Commercial Email Security Service was superior at preventing phising, social engineering and malware threats from landing in the user's Inbox.

This makes investing in a commercial specialist emails security service a no-brainer for an enterprise, especially given the potentially catastrophic risks to real-world targets in banking, finance, aviation, energy, healthcare, law and government.

The cost of such a specialist security service, however, will likely give the owner of a small- or medium-sized business pause. For them, it might be more economical to run their own server or combine this server with an open source specialist service. Do the risks outweigh the costs?

The specialist security services and the commercial email platform that we tested were good at allowing end-users to view access legitimate email. The Commercial Email Platform quarantined some of the legitimate messages but its Legitimate Accuracy rating of 78% was within the range of those of the Commercial and the Open Source Email Security Services which classified all of them correctly. Also, the Commercial Email Security Service was slightly less effective against business email compromise attacks.

The Open Source Email Security Service had a 3% advantage in its Protection Accuracy rating over that of the Commercial Email Platform. This slight advantage might be enough for some to consider creating their own email platform using free, open-source software.

Appendices

Appendix A: Attack Details

Targeted Attack Types

Attack Group Sandworm

Method of Attack Windows vulnerabilities via Office documents
Targets Energy industries

In late 2015 a group known as the Sandworm Team made use of a zero-day vulnerability to cause a widespread power outage in Ukraine. This threat actor is also known as Voodoo Bear and BlackEnergy APT Group.

References:
https://attack.mitre.org/groups/G0034/

Attack Group APT28

Method of Attack Microsoft Office macros
Targets Government

Macro-based attacks are a popular choice as a starting point of a targeted attack. There is a low barrier to entry and a wide distribution of vulnerable targets. Infamous campaigns conducted by APT28, and associated groups Fancy Bear and Sednit, usually start with spear phishing email messages designed to convince users to open specially crafted, attached Microsoft Office documents that lead to further compromise of their systems.

References:
https://attack.mitre.org/groups/G0007/

Attack Group FIN4

Method of Attack Man-in-the-middle spear phishing
Targets Financial markets

This group stole clean Office documents from the target and edited them, embedding malicious macros. By using correctly formatted documents containing real information, stolen from compromised accounts, the attackers increased the likelihood that recipients would be tricked into opening the documents and allowing their own systems to be compromised.

References:
https://attack.mitre.org/groups/G0085/

Attack Group FIN7

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/

Attack Group Dragonfly & Dragonfly 2.0

Method of Attack Phishing and supply chain methods
Targets Energy sector

These two groups are sometimes tracked separately. Dragonfly has been active for approximately 10 years, with its targets shifting from defense and aviation companies to the energy sector after 2013. Dragonfly 2.0 has kept focus on the energy sector in its operations.

References:
https://attack.mitre.org/groups/G0035/
https://attack.mitre.org/groups/G0074/

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.

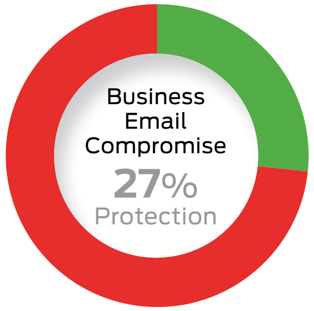
For example, you can see how many social engineering samples made it through to the inbox; how many were sent to the Junk folder; and how many were prevented from coming anywhere near the user – the Junk folder and Quarantine (admin) are common options.

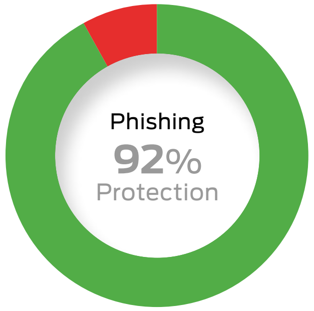
Not every possible option needs to be taken by a service under test, so the tables show only those outcomes that occurred.

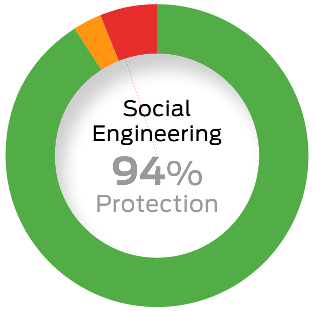
Targeted Attack Details

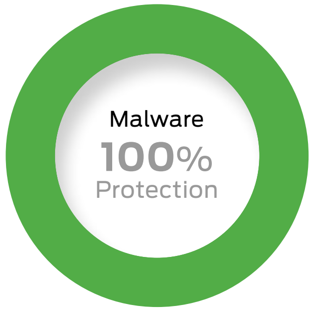
Commercial Email Security Service

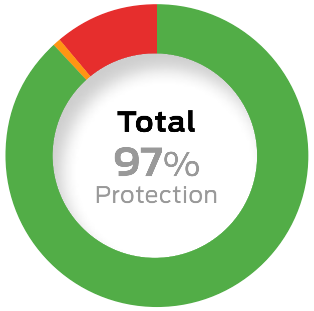
	Stopped	Blocked	Quarantined (admin)	Rejected	Edited (deny)	Quarantined (user)	Junk (deny)	Junk Folder	Junk (allow)	Edited (allow)	Inbox
Business Email Compromise	0	0	0	2	0	5	0	0	0	0	19
Phishing	0	0	0	27	46	57	8	0	0	0	12
Social Engineering	2	0	0	0	0	89	0	3	0	0	6
Malware	0	0	0	0	53	5	2	0	0	0	0
Total	**2**	**0**	**0**	**29**	**99**	**156**	**10**	**3**	**0**	**0**	**37**





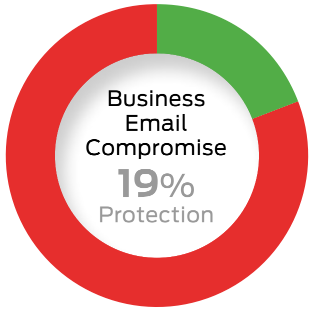


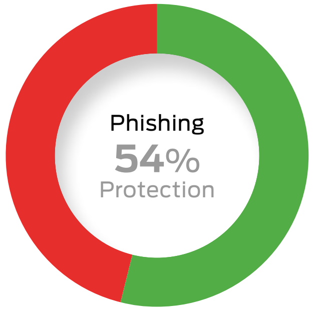


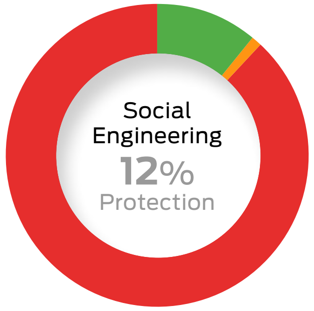


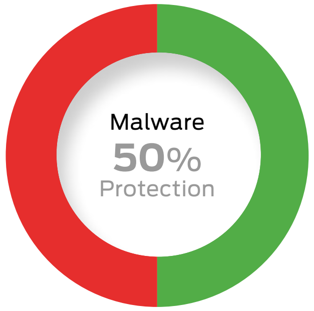
Open Source Email Security Service

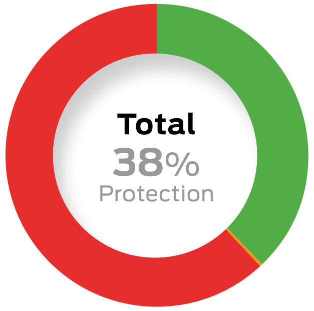
	Stopped	Blocked	Quarantined (admin)	Rejected	Edited (deny)	Quarantined (user)	Junk (deny)	Junk Folder	Junk (allow)	Edited (allow)	Inbox
Business Email Compromise	0	0	5	0	0	0	0	0	0	0	21
Phishing	30	3	0	0	48	0	0	0	0	0	69
Social Engineering	1	0	0	0	0	10	0	1	0	0	88
Malware	0	0	0	0	30	0	0	0	0	0	30
Total	**31**	**3**	**5**	**0**	**78**	**10**	**0**	**1**	**0**	**0**	**208**





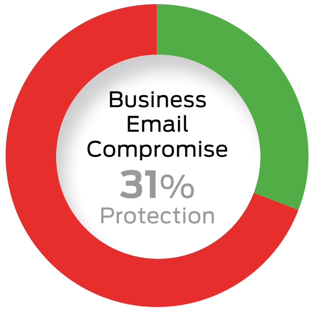


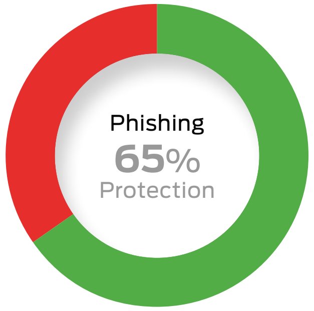


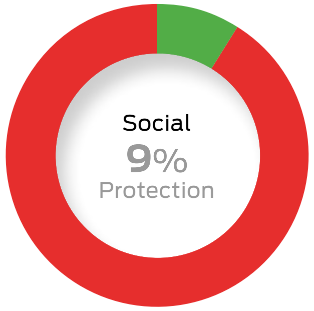


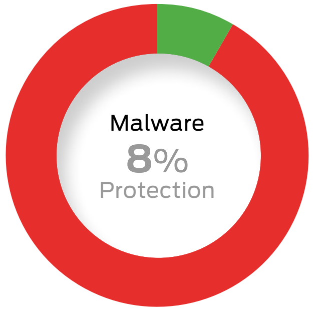
Commercial Email Platform

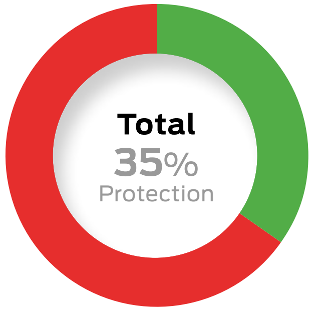
	Stopped	Blocked	Quarantined (admin)	Rejected	Edited (deny)	Quarantined (user)	Junk (deny)	Junk Folder	Junk (allow)	Edited (allow)	Inbox
Business Email Compromise	0	0	2	3	0	0	0	0	0	3	18
Phishing	3	0	54	0	29	12	0	0	0	0	52
Social Engineering	0	0	9	0	0	0	0	0	0	0	91
Malware	3	0	2	0	0	0	0	0	0	0	55
Total	**6**	**0**	**67**	**3**	**29**	**12**	**0**	**0**	**0**	**3**	**216**











Legitimate Message Details

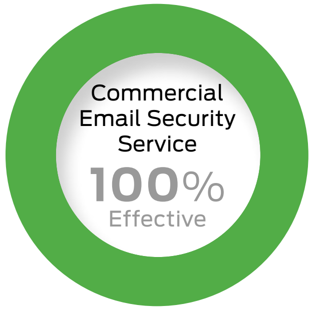
These results show how effectively each service managed messages that posed no threat. In an ideal world all legitimate messages would arrive in the inbox. When they are categorised as being a threat then a 'false positive' result is recorded.

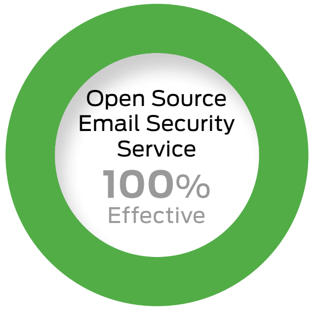
It is important to test for false positives because too many indicate a product that is too aggressive and will block useful email as well as threats. It would be easy to create a product that blocked all threats if it was also allowed to block all legitimate email.

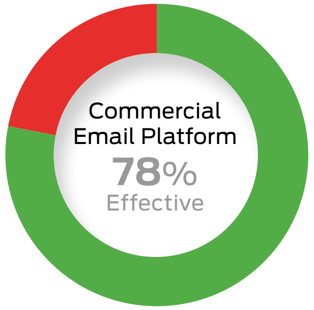
Finding the balance between allowing good and blocking bad is the key to almost every type of security system.

Legitimate Message Details

	Inbox	Edited (allow)	Junk Folder	Quarantined (admin)	Blocked
Commercial Email Security Service	110	0	0	0	0
Open Source Email Security Service	110	0	0	0	0
Commercial Email Platform	86	0	0	24	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.

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 10th October and 18th November 2022.
- 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 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.