



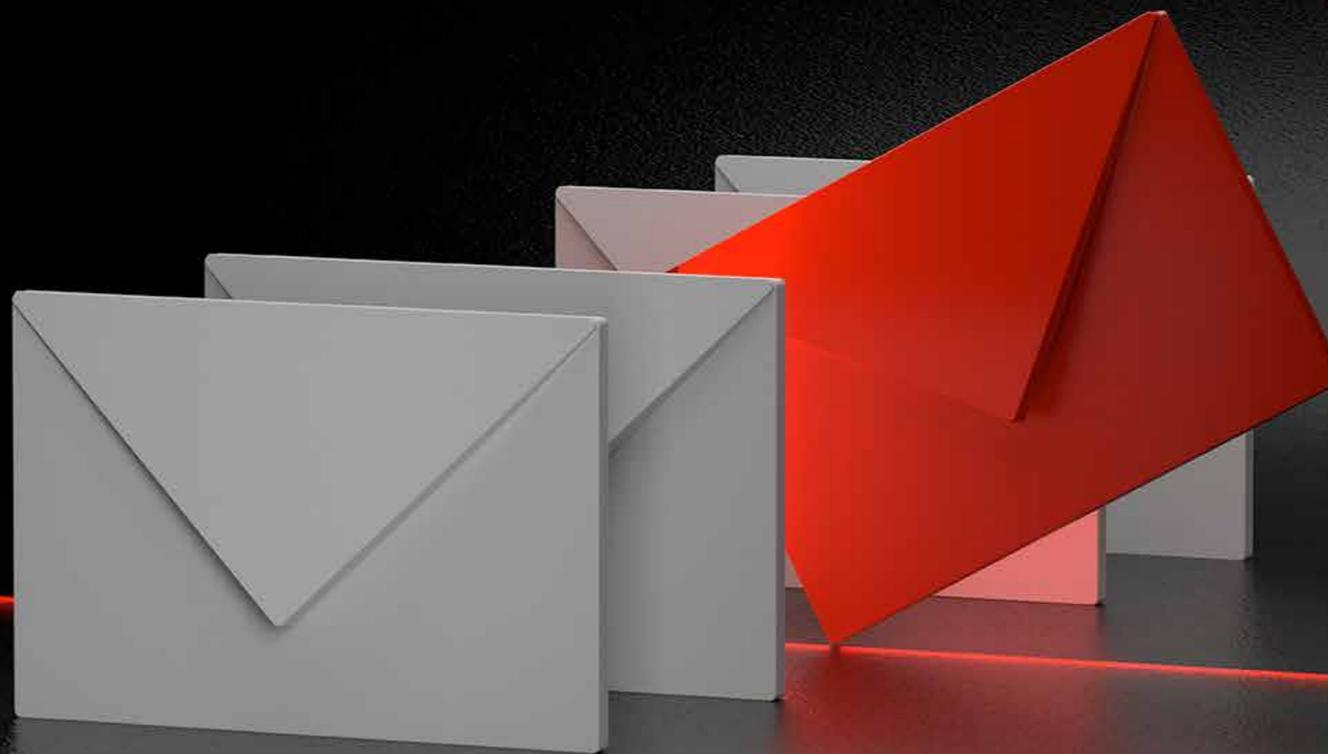
INTELLIGENCE-LED TESTING

Email Security Services

Enterprise and Small Business

June 2022

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
 Rory Brown
 Gia Gorbald
 Anila Johny
 Erica Marotta
 Jeremiah Morgan
 Joseph Pike
 Georgios Sakatzidis
 Dimitrios Tsarouchas
 Stephen Withey

IT SUPPORT

Danny King-Smith
 Chris Short

PUBLICATION

Sara Claridge
 Colin Mackleworth

Website selabs.uk

Twitter [@SELabsUK](https://twitter.com/SELabsUK)

Email info@SELabs.uk

LinkedIn linkedin.com/company/se-labs/

Blog blog.selabs.uk

Phone +44 (0)203 875 5000

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 Information
 Alliance (VIA); the Anti-Malware Testing Standards
 Organization (AMTSO); and NetSecOPEN.

© 2022 SE Labs Ltd

CONTENTS

Introduction	04
Executive Summary	05
Email Security Services Protection Awards	06
Attackers vs. Targets	07
1. Threat Detection Results	08
2. Total Accuracy Ratings	09
3. Protection and Legitimate Handling Accuracy	10
4. Conclusion	13
Appendix A: Attack Details	14
Targeted Attack Types	14
Appendix B: Detailed Results	15
Targeted Attack Details	15
Legitimate Message Details	18
Appendix C: Terms Used	19
Appendix D: FAQs	20
Appendix E: Services Tested	20

Document version 1.0 Written 6th June 2022;

1.1 Updated 13th June 2022 Corrected Legitimate Message Details



INTRODUCTION

Scoring Email Security Services

How seriously do you take the email threat?

Cyber criminals often use email as a way to start an attack. According to many sources email is by far the most common way that attackers try to gain access to your business and personal systems. The UK government's [Cyber Security Breaches Survey 2022](#) reported that email phishing alone accounts for 83% of attacks.

But we all know that, don't we? Because organisations, large and small, receive thousands of general and more targeted email threats every year. We don't see them all because our email services throw some messages away as they arrive. Others end up in a quarantine system that only network administrators can access. But you may notice a pile of messages in your Junk folder, with or without phishing links, malware attachments and documents.

Email security services don't handle all threats in the same way. Some will be stopped dead, while others can infiltrate fully. Somewhere in the middle we see email quarantine systems, Junk folders and edited messages – emails that have their links, attachments and even the words in the message tampered with. This tampering may effectively remove a threat, or it may not. There is a lot to assessing an email security solution!

The approach that we take is to measure everything and then judge how important each result is. Our view is that keeping threats as far away from the user as possible is best. But sometimes security personnel need to see what's coming in, so quarantines can be useful investigation tools. We have devised a scoring method that credits or penalises services according to our view on best outcomes. See [Protection and Legitimate Handling Accuracy](#) on page 10 for more. We also have a beginner's guide to email security on our [website](#).

We provide you with all of the results in this report so you can create your own personalised score using our data. If you prefer users to find threats in their Junk folder (yikes!) you can adjust the scoring accordingly. If you have a zero tolerance on false positives you can adjust the scores to take this into account too.

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

Executive Summary

This test examined the effectiveness of four email security solutions. Two were built into the **Microsoft** and **Google** email platforms, the other two being third-party 'add-on' services designed to provide additional security.

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.

Perception-Point achieved a remarkable 100% Total Accuracy rating, meaning that it allowed all legitimate

messages through to the user, while detecting and protecting against all of the threats.

Microsoft Defender for Office 365 had strong protection but misclassified some of the legitimate messages, to the degree that it dropped to third place. **Fortinet FortiMail** occupies second place with its well-balanced approach to handling unwanted and wanted email.

Google Workspace Enterprise was strong at allowing legitimate messages through but detected less than half of the threats. This pushed its Protection rating very low.

Executive Summary					
Product Tested	Protection Accuracy Rating	Legitimate Accuracy Rating	Total Accuracy Rating	Total Accuracy Rating (%)	Award
Perception-Point	2,310	1,100	3,410	100%	AAA
Fortinet FortiMail Cloud Email Security	2,165	1,060	3,225	95%	AAA
Microsoft Defender for Office 365	2,230	800	3,030	89%	AAA
Google Workspace Enterprise	-180	1,100	920	27%	C

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:

- **Perception-Point**
- **Fortinet FortiMail Cloud Email Security**
- **Microsoft Defender for Office 365**



- **Google Workspace Enterprise**



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 14.

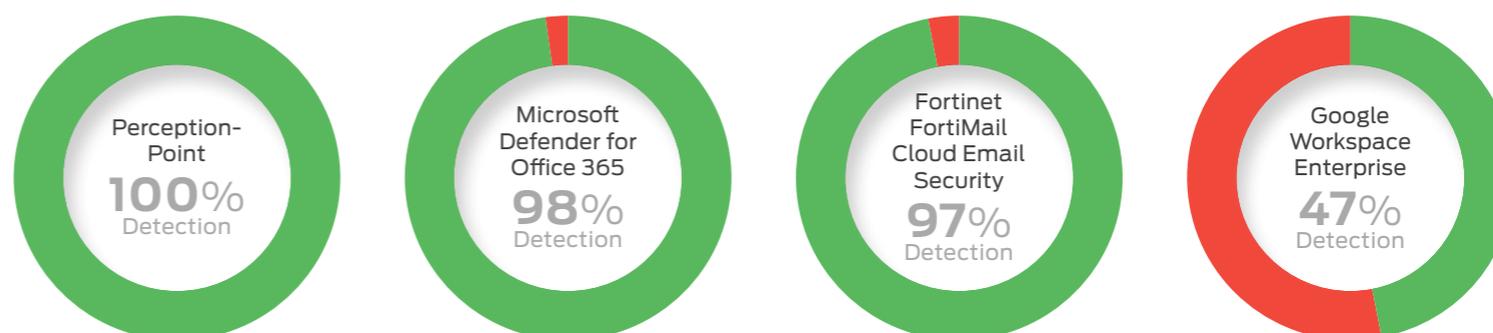
Attackers vs. Targets			
Attacker/APT Group	Method	Target	Details
Sandworm			Windows vulnerabilities via Office documents
APT28			Microsoft Office macros
FIN4			Man-in-the-middle spear phishing
FIN7 & Carbanak			Documents containing scripts combined with public tools
Dragonfly & Dragonfly 2.0			Phishing & 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. Threats that the Microsoft services moved to the Junk folder are counted as detections.

Threat Detection Results			
Product	Detection Rate	Misses	Detection Rate (%)
Perception-Point	231	0	100%
Microsoft Defender for Office 365	227	4	98%
Fortinet FortiMail Cloud Email Security	225	6	97%
Google Workspace Enterprise	109	122	47%



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.

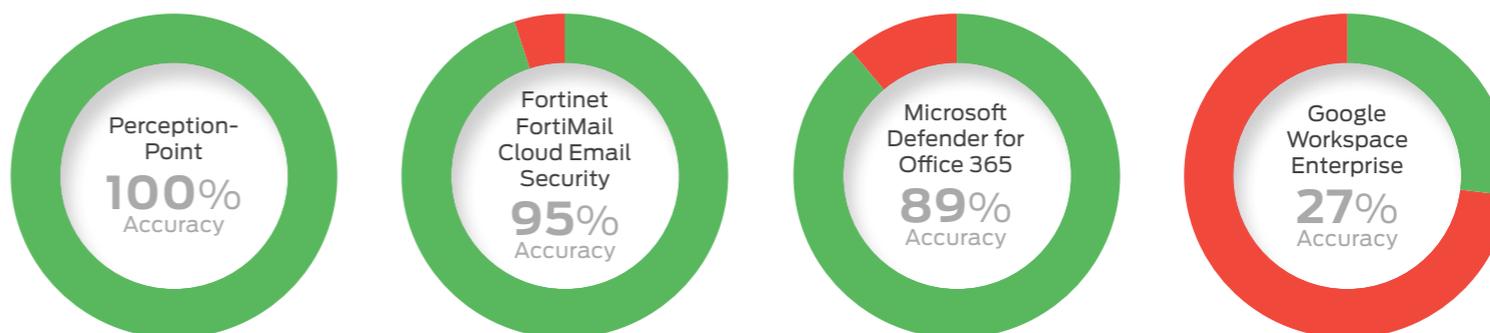
The graphic below takes into account not only each service's ability to detect and protect against threats, but also its handling of non-malicious messages and components of those messages, such as attachments and links to websites.

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

Total Accuracy Ratings		
Product	Total Accuracy Rating	Total Accuracy Rating (%)
Perception-Point	3,410	100%
Fortinet FortiMail Cloud Email Security	3,225	95%
Microsoft Defender for Office 365	3,030	89%
Google Workspace Enterprise	920	27%



Total Accuracy Ratings combine protection and false positives.

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.

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

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

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.

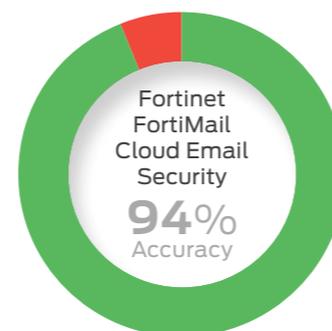
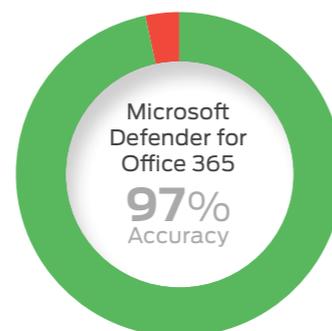
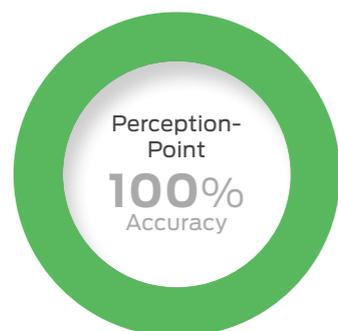
These ratings are based on our opinion of how important these different outcomes are. You may have a different view on how serious it is for a legitimate email to end up in quarantine, or for a malware threat to end up in the inbox. You can use the raw data from this report (See **Appendix B: Detailed Results** on page 15) to roll your own set of personalised ratings.

Annual Report 2021

Our 3rd Annual Report
is now available

- Annual Awards Winners
- Ransomware in advanced security tests
- Security Testing DataBase
- Review: 6 years of endpoint protection

Protection Accuracy Ratings		
Product	Protection Accuracy Rating	Protection Accuracy Rating (%)
Perception-Point	2,310	100%
Microsoft Defender for Office 365	2,230	97%
Fortinet FortiMail Cloud Email Security	2,165	94%
Google Workspace Enterprise	-180	-8%



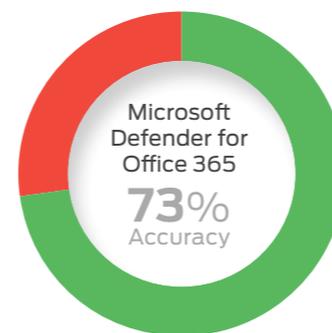
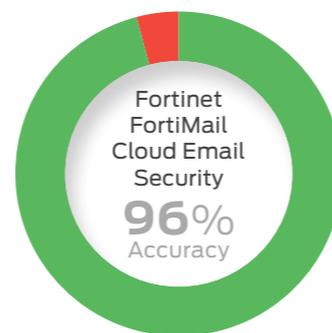
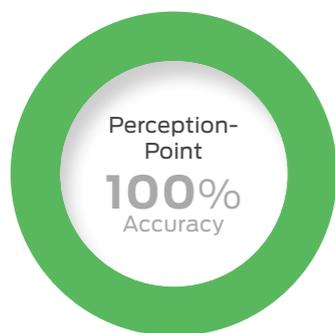
**DOWNLOAD
THE REPORT NOW!**

(free – no registration)

selabs.uk/ar2021

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 (%)
Perception-Point	1,100	100%
Google Workspace Enterprise	1,070	97%
Fortinet FortiMail Cloud Email Security	1,060	96%
Microsoft Defender for Office 365	800	73%



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



4. Conclusion

This test exposed well-known email platforms 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 14. 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 like **Fortinet FortiMail** and **Perception-Point** 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.

Perception-Point displayed the strongest performance in this test, achieving a remarkable 100% Total Accuracy rating, which takes into account handling both threats and legitimate messages. **Microsoft's Defender for Office 365** followed close behind, in terms of protection, but its legitimate message handling pushed it into third place.

Microsoft says that, "the majority of these cases involved messages sent to business accounts configured with enhanced protection. We believe that customers who use enhanced protection would prefer their email security solutions not to allow such messages."

Fortinet FortiMail came second, with a 95% Total Accuracy rating. **Google Workspace Enterprise** was the second most accurate when handling legitimate messages but failed to detect less than half of the threats, which slammed its protection rating down into a negative rating.

Full details of how each product handled different types of threats are available in **Appendix B: Detailed Results** on page 15.

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!



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: 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: 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/>

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: 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/>

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

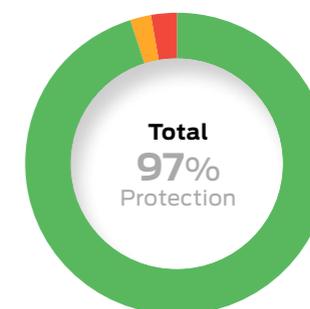
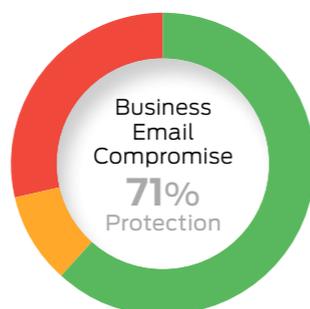
Each service has a number of options when handling such threats. The tables show how each service handled each category.

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

Fortinet FortiMail Cloud Email Security											
	Stopped	Blocked	Quarantined (admin)	Rejected	Edited (deny)	Quarantined (user)	Junk (deny)	Junk Folder	Junk (allow)	Edited (allow)	Inbox
Business Email Compromise	5	8	0	0	0	0	0	2	0	0	6
Phishing	52	35	0	3	0	0	0	0	0	0	0
Social Engineering	0	26	0	31	0	0	0	3	0	0	0
Malware	0	24	0	36	0	0	0	0	0	0	0
Total	57	93	0	70	0	0	0	5	0	0	6



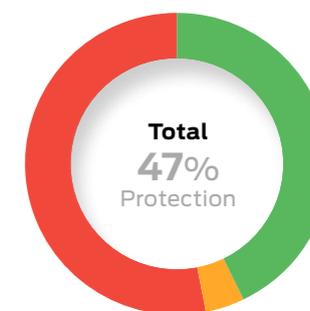
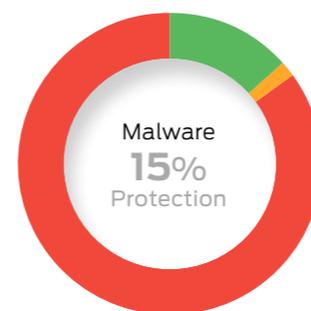
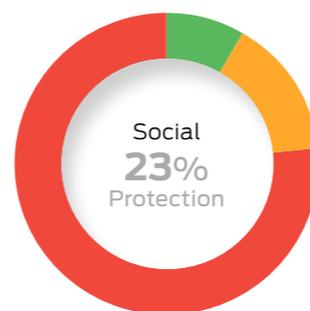
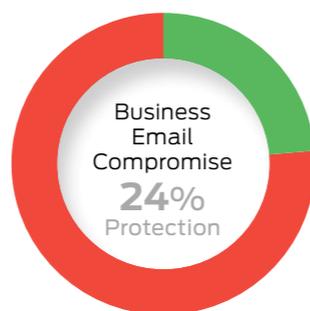
Perception-Point											
	Stopped	Blocked	Quarantined (admin)	Rejected	Edited (deny)	Quarantined (user)	Junk (deny)	Junk Folder	Junk (allow)	Edited (allow)	Inbox
Business Email Compromise	1	0	20	0	0	0	0	0	0	0	0
Phishing	61	0	29	0	0	0	0	0	0	0	0
Social Engineering	0	0	60	0	0	0	0	0	0	0	0
Malware	0	0	60	0	0	0	0	0	0	0	0
Total	62	0	169	0	0	0	0	0	0	0	0



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	1	0	16	0	0	0	0	0	0	0	4
Phishing	48	0	41	0	1	0	0	0	0	0	0
Social Engineering	0	0	60	0	0	0	0	0	0	0	0
Malware	0	0	60	0	0	0	0	0	0	0	0
Total	49	0	177	0	1	0	0	0	0	0	4



Google Workspace Enterprise											
	Stopped	Blocked	Quarantined (admin)	Rejected	Edited (deny)	Quarantined (user)	Junk (deny)	Junk Folder	Junk (allow)	Edited (allow)	Inbox
Business Email Compromise	3	0	0	2	0	0	0	0	0	0	16
Phishing	49	0	0	0	1	0	31	0	0	0	9
Social Engineering	4	0	0	0	0	0	1	9	0	0	46
Malware	0	0	0	0	0	0	8	1	0	0	51
Total	56	0	0	2	1	0	40	10	0	0	122



Legitimate Message Details

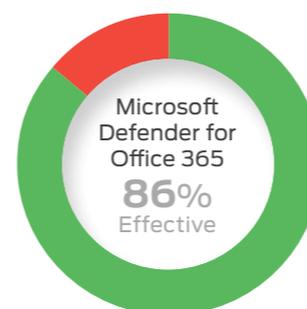
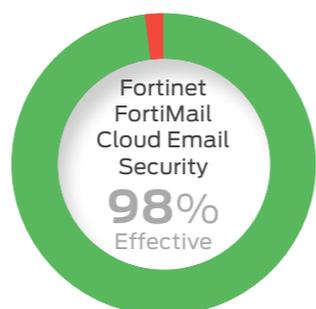
These results show how effectively each service managed messages that posed no threat. In an ideal world all legitimate messages would arrive in the inbox. When they are categorised as being a threat then a 'false positive' result is recorded.

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
Fortinet FortiMail Cloud Email Security	108	0	0	0	2
Perception-Point	110	0	0	0	0
Microsoft Defender for Office 365	95	0	0	15	0
Google Workspace Enterprise	108	0	2	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.

 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

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 7th March and 20th April 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.
- SE Labs conducted this email security services protection test using real email accounts running on **Microsoft Office 365** and **Google Workspace Enterprise**.

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.

Appendix E: Services Tested

The table below shows each service's name as it was being marketed at the time of the test. Each is labelled in this report using the Report Label value.

Services Tested	
Vendor	Service
Fortinet	FortiMail Cloud Email Security
Google	Workspace Enterprise
Microsoft	Defender for Office 365
Perception-Point	Perception-Point

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.